RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE BLIDA 1
Faculté de Technologie
Département d'Électronique

MEMOIRE DE MASTER
EN TÉLÉCOMMUNICATION

Spécialité : Réseaux et Télécommunications

THÈME :

Contribution du protocole IS-IS dans des réseaux IP/MPLS

Réalisé par
Mlle.ROUABAH Ikram
Mlle.SOUAB Manel

Encadré par
Mme.BOUTALEB Nassima

Année universitaire 2023/2024

Remerciements

*Après avoir rendu grâce **à Dieu** le Tout Puissant et le Miséricordieux nous tenons à remercier vivement tous ceux qui, de près ou de loin ont participé à la rédaction de ce document.*

*Tout d'abord, je tiens à remercier mon directeur de mémoire, **Mme BOUTALEB Nassima** , pour son encadrement, ses conseils avisés et son soutien constant tout au long de cette recherche.Sa rigueur scientifique et sa disponibilité ont été des atouts précieux pour mener à bien ce travail.*

J'adresse aussi mes vifs remerciements aux membres des jurys pour avoir bien voulu examiner et juger ce travail. Nous apprécions grandement letemps qu'ils nous ont accordé et les remarques constructives qu'ils nous ont faites.

Nos remerciements s'étendent également à l'ensemble des professeurs et enseignants qui ont contribué à notre formation. Leurs cours, leurs conseils et leur encadrement ont été essentiels à notre développement intellectuel et à notre progression dans cette filière.

Un grand merci à mes collègues de promotion pour leur solidarité et leur amitié. Les échanges et les discussions enrichissantes que nous avons eus ont largement contribué mon épanouissement académique et personnel.

Enfin, nous ne saurions oublier toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce projet. Nous leur exprimons notre gratitude la plus profonde pour leur soutien, leur encouragement et leur bienveillance.

Dédicaces

C'est avec une profonde gratitude et sincères mots que je dédie ce travail en premier lieu à Mes chères parents qui quel que soit l'objet qu'on essayera de leur offrir, il n'atteindra jamais ce que j'ai envie de leur dire et exprimer.

A mon cher PAPA REDHA

Celui qui est toujours là pour moi, et m'a donné un magnifique modèle de labeur et de persévérance, celui qui m'a encouragé qui m'a toujours protégé, mon model qui fait ma fierté.

Que ce travail soit l'expression des vœux que tu n'as cessé de formuler dans tes prières. Mon cher père.

A ma chère MAMAN ASSIA

La perle de mon existence, quelle brave dame que tu es, que de sacrifices consentis à mon égard afin que je progresse dans mes études. Je tombe en admiration devant la bonté de ton cœur à nulle pareille.

Quels que soient mes caprices et mes écarts tu m'as toujours soutenue, trouvant les mots justes pour me ramener sur le bon chemin.

L'évènement que nous célébrons aujourd'hui t'est entièrement dédié. Que dieu te préserve santé et longue vie

A ma chère sœur **Nour**.

A ma plus grande source de bonheur mon frère **Thabet Rahim.**

À ma grand-mère, qui m'a aidée à devenir la femme que je suis aujourd'hui. Votre sagesse, votre amour et votre soutien inconditionnel ont façonné ma vie de manière indélébile. Merci pour tout ce que vous avez fait pour moi **Lala Setti.**

A toute ma famille, mes oncles et tantes maternelles et paternelles, cousins et cousines.

A mes meilleurs amis Nourhane, Houda, Dalel, Anissa, Maroua, Samah, Awatif.

A ceux qui m'ont supportée, encouragée.

A tous les membres du CSC Club.

Et spécialement à ma très chère binôme **Manel**, merci pour tes conseils et tes encouragements, mais aussi pour les bons moments qui ont contribué à rendre ces années inoubliables.

Ikram

Dédicaces

À mes parents, pour leur amour, leur soutien inconditionnel, et leurs encouragements constants tout au long de mon parcours académique. Vous avez toujours cru en moi et m'avez donné la force de continuer même dans les moments les plus difficiles.

À mes frères REDHA et HAMZA, pour leur affection, leur compréhension et leur patience.Votre présence à mes côtés a été une source de motivation et de réconfort.

À mes amis SAMAH, IKRAM, AOUATIF, ANISSA, MAROUA, MARIA, ABDENNOUR,NOUFEL,pour leur amitié sincère et leur soutien inestimable. Vous avez su me redonner le sourire et me permettre de décompresser durant les moments de stress intense.

À mes professeurs et encadrants, pour leur guidance, leurs précieux conseils, et leur patience. Votre expertise et votre dévouement ont grandement contribué à la réussite de ce travail.

À tous ceux qui, de près ou de loin, ont cru en moi et m'ont soutenu tout au long de ce voyage académique.

Avec toute ma gratitude,

Manel

ملخص

تستكشف هذه المذكرة تكوين وتحسين شبكات الجيل الجديد، مع دمج الشبكة الخاصة الافتراضية ومقارنة بروتوكولات التوجيه بروتوكول فتح أقصر مسار أولا وبروتوكول النظام المتوسط إلى النظام المتوسط. تُظهر الأطروحة كيف يعزز بروتوكول متعدد التبديل باستخدام المؤشرات إدارة المرور وجودة الخدمة، وكيف تضمن الشبكة الخاصة الافتراضية الأمان وتجزئة المرور، وتقارن بين أداء وتعقيد بروتوكولات التوجيه الداخلية.
تساعد التوصيات المقدمة في اختيار وتكوين التقنيات المناسبة لاحتياجات الشبكات الحديثة.

الكلمات المفتاحية شبكات الجيل الجديد، بروتوكول متعدد التبديل باستخدام المؤشرات، الشبكة الخاصة الافتراضية، بروتوكول فتح أقصر مسار أولا، بروتوكول النظام المتوسط إلى النظام المتوسط، التوجيه، جودة الخدمة، الأمان.

Résume

Ce mémoire explore la configuration et l'optimisation des réseaux de nouvelle génération (NGN) basés sur IP/MPLS, en intégrant des VPN et en comparant les protocoles de routage OSPF et IS-IS. Elle démontre comment MPLS améliore la gestion du trafic et la qualité de service, comment les VPN assurent la sécurité et la segmentation du trafic, et compare les performances et la complexité des protocoles de routage internes. Les recommandations fournies aident à choisir et configurer les technologies adaptées aux besoins spécifiques des réseaux modernes.

Mots clés :
NGN, IP/MPLS, VPN, OSPF, IS-IS, routage, qualité de service, sécurité.

Abstract

This memoir investigates the configuration and optimization of next-generation networks (NGN) based on IP/MPLS, integrating VPNs, and comparing OSPF and IS-IS routing protocols. It shows how MPLS enhances traffic management and quality of service, how VPNs ensure security and traffic segmentation, and compares the performance and complexity of internal routing protocols. The provided recommendations help in selecting and configuring technologies suited to the specific needs of modern networks.

Keywords :
NGN, IP/MPLS, VPN, OSPF, IS-IS, routing,quality of service, security.

Liste des Acronymes et Abréviations

AS Autonomous System

ATM Asynchronous Transfer Mode

BDR Backup Designated Router

BGP Border Gateway Protocol

BMA Broadcast Multiple Access

CE Customer Edge

CIDR Classless Inter-Domain Routing

CLNS Connection Less Network System

CLNP Connection Less Network Protocol

CPU Central Processing Unit

CD-LDP Constraint-Based Routing Label Distribution Protocol

CS Circuit Switched

CSNP Complete Sequence Number Packet

DDB Data Base Description

DR Designated Router

EIGRP Enhanced Interior Gateway Routing Protocol

EGP Exterior Gateway Protocol

ES End System

FEC Forwarding Equivalence Class

FIB Forwarding Information Base

HDLC High-Level Data Link Control

ICMP Internet Control Message Protocol

IGP Interior Gateway Protocol

IIH IS-IS Hello

IP Internet Protocol

IS-IS Intermediate System to Intermediate System

ISP Internet Service Provider

LAN Local Area Network

LDP Label Distribution Protocol

LER Label Edge Router

LFIB Label Forwarding Information Base

LIB Label Information Base

LSA Link State Advertisement

LSR Label Switching Router

LSP Label Switched Path

LSU Link State Update

MAC Media Access Control

MGW Media Gateway

MPLS Multi Protocol Label Switching

NBMA Non-broadcast Multiple Access

NGN Next Generation Network

OSPF Open Shortest Path First

OSI Open System Interconnection

PE Provider Edge

PHP Hyper Preprocessor

POP Post Office Protocol

PPP Point-to-Point Protocol

PS Packet Switched

PSNP Partial Sequence Number Packet

QOS Quality of Service

RIP Routing Information Protocol

RPL Routing Protocol for Low-Power and Lossy Networks

RSVP Resource Reservation Protocol

RSVP-TE Resource Reservation Protocol-Traffic Engineering

SIP Session Initiation Protocol

SPF Shortest Path First

TCP Transmission Control Protocol

TDP Tag Distribution Protocol

TTL Time To Live

VLANs Virtual Local Area Network

VLSM Variable Length Subnet Mask

VoiP Voice over Internet Protocol

VPLS Virtual Private LAN Service

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Aujourd'hui, alors que les données transmises sur les réseaux connaissent une croissance exponentielle, les défis auxquels sont confrontés les opérateurs deviennent de plus en plus urgents. Le routage IP traditionnel est souvent limité par la lenteur du traitement des ressources et ne peut pas répondre efficacement à la demande croissante de bande passante et de diversité technologique. Cette évolution rapide de la demande a contraint les acteurs du secteur à réinventer leur infrastructure réseau pour garantir la fiabilité, l'évolutivité et la compatibilité avec les technologies existantes.
Dans un contexte marqué par une demande croissante de services de communication rapides et fiables, les technologies de réseaux de nouvelle génération (NGN) se sont imposées comme une solution incontournable pour répondre aux besoins modernes des entreprises et des particuliers. Ces réseaux, basés sur l'architecture IP/MPLS (Multiprotocol Label Switching), offrent une plateforme robuste et flexible permettant la convergence de divers types de services tels que la voix, les données et la vidéo sur une infrastructure commune.
Ce projet fin d'étude se propose d'explorer en profondeur la configuration d'un réseau NGN, l'intégration des VPN (Virtual Private Networks) pour la sécurité et la segmentation du trafic, ainsi que l'implémentation et la comparaison de deux protocoles de routage interne, OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System).

Contexte de travail et Problématique

Les réseaux traditionnels, souvent basés sur des architectures distinctes pour la voix, les données et la vidéo, se révèlent de plus en plus inadéquats face à la complexité et à l'ampleur des exigences actuelles. L'adoption de technologies NGN permet de surmonter ces limitations en offrant une infrastructure unifiée et évolutive. L'IP/MPLS, en particulier, a démontré sa capacité à fournir des solutions efficaces pour la gestion du trafic, la qualité de service (QoS) et la résilience du réseau.
Cependant, la mise en place d'un réseau NGN ne se limite pas à la simple adoption de nouvelles

technologies. Elle implique également une configuration précise et optimisée des éléments du réseau, ainsi qu'une intégration harmonieuse des VPN pour assurer la sécurité et l'isolation des différentes parties du réseau. En outre, le choix du protocole de routage interne est crucial pour garantir une performance optimale et une gestion efficace du réseau.

Objectifs du travail

L'objectif principal de cette thèse est d'étudier et de configurer un réseau NGN basé sur IP/MPLS, d'intégrer des VPN et de mettre en œuvre et comparer deux protocoles de routage interne, OSPF et IS-IS. Les objectifs spécifiques incluent :

1. **Configuration d'un Réseau NGN IP/MPLS :**
   •Développer une compréhension approfondie des principes et des mécanismes des réseaux NGN.
   •Concevoir et configurer une infrastructure réseau utilisant MPLS pour optimiser le routage et la gestion du trafic.
   •Explorer les fonctionnalités avancées de MPLS, telles que la QoS et la gestion du trafic.
2. **Intégration des VPN :**
   •Configurer des VPN pour assurer la sécurité, la confidentialité et la segmentation du trafic réseau.
   •Évaluer l'impact des VPN sur les performances et la gestion du réseau dans un environnement NGN.
3. **Implémentation des Protocoles de Routage Interne :**
   •Mettre en œuvre les protocoles de routage OSPF et IS-IS dans le réseau configuré.
   •Analyser les performances, la complexité de configuration et la flexibilité de chaque protocole dans différents scénarios de réseau.
4. **Comparaison des Protocoles OSPF et IS-IS :**
   •Effectuer une analyse comparative des protocoles OSPF et IS-IS en termes de convergence, scalabilité, efficacité et gestion des ressources.
   •Fournir des recommandations basées sur les résultats de l'analyse comparative pour aider les décideurs à choisir le protocole de routage le plus adapté à leurs besoins spécifiques.

Chapitre 1

Introduction aux protocoles de routage interne

1.1 Introduction

Les communications au sein d'un réseau informatique reposent principalement sur le processus de routage, et les protocoles de routage constituent le fondement de ce processus. Sans ces protocoles, aucun échange ne serait envisageable ou possible.
Toutefois, avec l'expansion d'Internet à l'échelle mondiale et l'émergence de services convergents, des problèmes liés à la performance du réseau ont surgi, menaçant ainsi sa stabilité et sa rentabilité. Cela a incité les chercheurs à explorer des solutions allant de simples améliorations à des changements radicaux dans les technologies existantes.
C'est donc sur ces protocoles de routage que les chercheurs se sont concentrés pour trouver des solutions, car ils ont un impact direct sur les performances du réseau[1].

1.2 Nouvelle génération NGN IP/ MPLS

1.2.1 Présentation

Un réseau de nouvelle génération (NGN) représente une infrastructure avancée qui combine des capacités de commutation de paquets (PS : Packet Switching) avec une architecture interopérable, évolutive et flexible, exploitant largement la fibre optique pour une bande passante élevée.
Il prend en charge une gamme étendue de services, tels que la téléphonie sur IP, l'accès à Internet et la visioconférence, tout en intégrant des fonctionnalités de commutation de circuit (CS : Circuit Switching), notamment pour la téléphonie traditionnelle. En somme, le NGN fusionne les systèmes et protocoles existants (CS et PS), offrant des possibilités avancées telles que la gestion de la qualité de service (QoS) et l'ingénierie du trafic[2].

1.2.2 Architecture NGN en couche

Les eléments essentiels de NGN dans l'architecture est en 3 couches :

- Couche transport composé de deux sous-couches[3] :
    1. La couche d'accès : englobe les fonctions et équipements nécessaires pour gérer l'accès des équipements des utilisateurs au réseau, en fonction de la technologie d'accès utilisée.
    2. La couche de transit : Elle assure le routage du trafic voix ou données à travers le cœur de réseau IP, en se basant sur le protocole approprié. Au cœur de cette architecture NGN, le « Media Gateway » (MGW) joue un rôle crucial en adaptant les protocoles de transport aux différents types de réseaux physiques disponibles, tels que le RTC, l'IP, l'ATM, etc.
- Couche contrôle : La couche de contrôle supervise toutes les fonctions de contrôle des services en général, et spécifiquement le contrôle des appels pour les services vocaux. Dans une architecture

NGN, le composant essentiel à ce niveau est le serveur d'appels, souvent désigné sous le terme de « Soft Switch ». Ce dernier, notamment pour les services vocaux, assure l'équivalent de la fonction de commutation.

- Couche service : La couche de service englobe tous les éléments nécessaires à la fourniture de services dans un réseau NGN. En termes d'équipements, cette couche comprend deux types principaux : les serveurs d'application et les "enablers" (ou éléments d'activation), qui sont des fonctionnalités telles que la gestion de l'information de présence des utilisateurs, pouvant être utilisées par plusieurs applications. Typiquement, cette couche intègre des serveurs d'application SIP (Session Initiation Protocol), qui sont cruciaux dans une architecture NGN pour la gestion des sessions multimédias en général, et des services de voix sur IP en particulier[3].

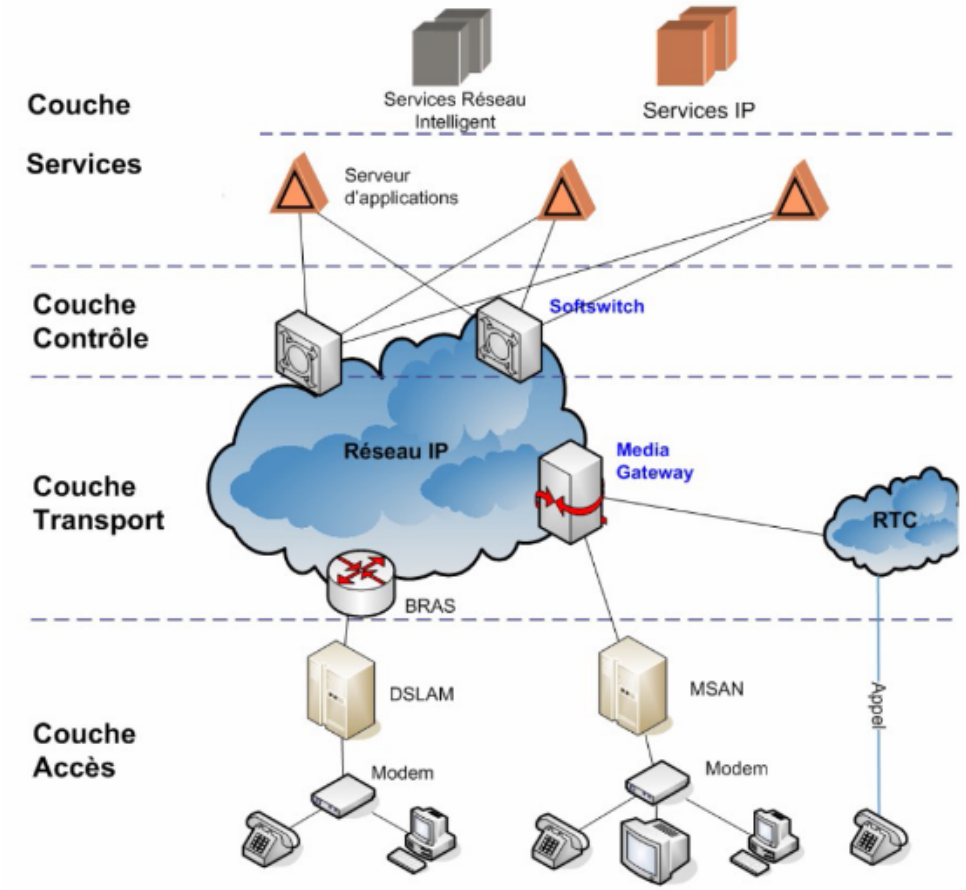

FIGURE 1.1 – Architecture en couche d'un réseau NGN[4].

1.2.3 Équipements constituants un de réseau NGN

Un réseau déploie divers équipements, comprenant notamment :

— **Soft Switch :**
Un Soft Switch est un serveur informatique doté d'un logiciel permettant le traitement des appels vocaux dans un environnement de commutation de paquets.

— **Media Gateway :**
Une passerelle multimédia effectue la conversion du trafic provenant d'un circuit TDM en paquets, permettant ainsi sa gestion par le réseau NGN. Elle peut être installée pour faire le lien entre un réseau à commutation de circuits (CS) et un réseau à commutation de paquets (PS).

— **Routeurs :**
Les routeurs IP/MPLS de backbone offrent des performances élevées et assurent la gestion efficace du trafic vers leur destination. Ils reposent sur la commutation de label (MPLS) et prennent en charge plusieurs protocoles de nouvelle génération tels que OSPF (Open Short est Path First), IS-IS (Intermediate System to Intermediate System), RSVP (Resource Reservation Protocol), LDP (Label Distribution Protocol) et BGP (Border Gateway Protocol). Ces routeurs se divisent généralement en deux catégories : les routeurs de bordure (Edge) et les routeurs principaux (Core)[5].

— **Routeur Edge :**
Les routeurs Edge (PE : Provider Edge), implantés à la périphérie du backbone IP/MPLS, jouent le rôle de passerelle entre les routeurs du cœur et les routeurs des clients (CE : Customer Edge).

— **Router core :**
Un routeur core, positionné au centre d'un réseau, représente sa pièce maîtresse. Il est reconnu pour sa puissance supérieure par rapport aux autres types de routeurs.

1.3 Communication dans un réseau IP

1.3.1 Èléments d'un réseau

Un réseau IP est principalement constitué des ces équipements suivants [6] :

- Le concentrateur : Appelé aussi hub, c'est un équipement réseau qui fonctionne au niveau1 (couche physique) du modèle OSI, utilisé dans la topologie en étoile, il permet notamment de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.
- Le commutateur : C'est un élément de niveau 2 (couche liaison de données) qui s'occupe de l'acheminement des trames au sein d'un même réseau. Contrairement au hub qui diffuse l'information sur tous les ports, le switch sait déterminer sur quel port unique il doit envoyer une trame et cela en exploitant les adresses MAC de destination assignée à chaque port du commutateur.
- Le routeur : Un routeur est un élément intermédiaire de niveau 3 du modèle OSI qui assurent l'acheminement des paquets entre réseaux distants en se basant sur des tables dites de routage construites par les routeurs.

- Le terminal : Désigne un ensemble de périphériques placés à l'extrémité des nœuds soit pour demander ou pour offrir des services via le réseau (ordinateur, serveur ou logiciel...etc.).

1.3.2 Structure du réseau d'opérateur

Pour faciliter la gestion du réseau et permettre une détection rapide des problèmes éventuels, les réseaux d'opérateurs sont généralement organisés selon une structure hiérarchique comprenant trois niveaux[7] :

1. La couche d'accès (layer Access) : constitue la périphérie du réseau, elle regroupe un ensemble de commutateurs physiquement connectés à ceux de la couche supérieure pour fournir un accès au réseau.
2. La couche distribution (layer distribution) : établit un lien entre la couche d'accès et la couche cœur, elle assure le routage des données entre les VLANs et délimite les zones de diffusion.
3. La couche cœur du réseau (layer backbone) : est la colonne vertébrale du réseau, fournissant une connexion à Internet et transférant les données le plus rapidement possible, agissant ainsi comme le centre névralgique de l'ensemble du système.

1.3.3 Commutation

La commutation est la fonctionnalité qui permet d'acheminer les données d'un point A vers un point B dans un même réseau local (un LAN Ethernet par exemple). La commutation est effectuée par le commutateur en exploitant sa table MAC, cette dernière contient la correspondance entre l'adresse MAC d'un terminal et le port sur lequel il est connecté, cette table est remplie au fur et à mesure que les trames transitent par le switch[8].

Fonctionnement :

Lorsqu'un commutateur reçoit un paquet sur l'un de ses ports :

•Il commence par désencapsuler l'entête de la trame.

•Ensuite, il vérifie si l'adresse MAC source et son port correspondant sont répertoriés dans la table MAC.

•Si cette correspondance n'existe pas, le commutateur la crée.Sinon, il passe à l'étape suivante.

•Le commutateur recherche alors l'adresse MAC de destination dans sa table MAC.

•Si l'adresse existe dans la table, la trame est envoyée via le port correspondant.Sinon, la trame est diffusée sur tous les ports à l'exception du port d'origine.

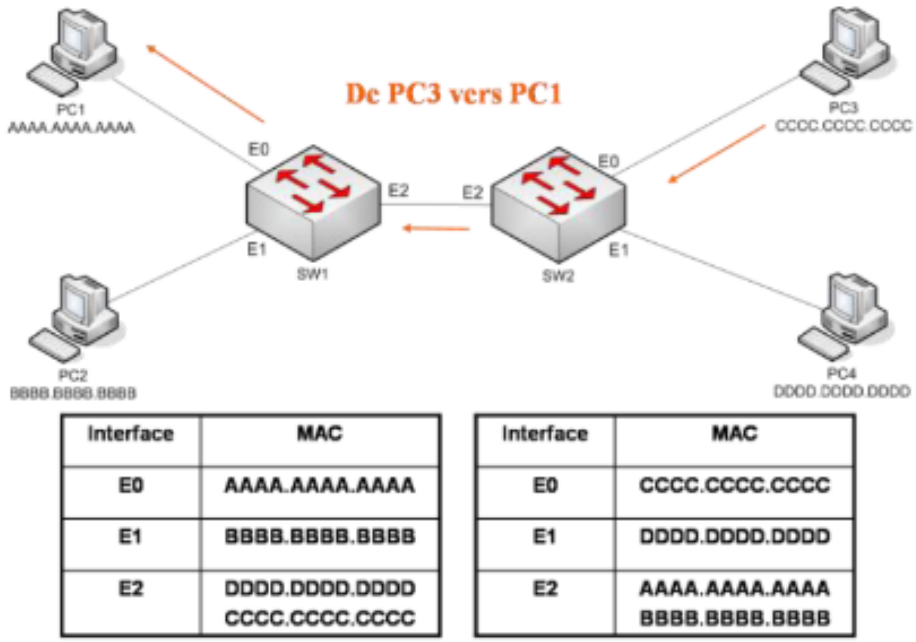

FIGURE 1.2 – Exemple de commutation[9].

1.3.4 Routage

Le routage est le mécanisme permettant d'établir des chemins entre une ou des sources vers une ou plusieurs destinations, cette fonction est remplie par le routeur, sur chaque interface du routeur un sous réseau y est connecté, cette interface représente aussi une passerelle pour les terminaux du même sous réseau, afin qu'ils puissent atteindre les destinations qui se trouvent sur d'autre sous réseaux.
Chaque routeur maintient une liste des sous réseaux avec en correspondance l'adresse IP du voisin qui permet d'atteindre le sous réseau, la liste en question est appelée la table de routage[10].

1.3.5 Table de routage

Une table de routage est un fichier de données dans la mémoire vive qui sert à stocker des informations concernant la route pour les réseaux connectés directement et les réseaux distants (tronçon suivant).
La table de routage contient des associations de réseau ou de tronçon suivant, menant à la destination finale.

FIGURE 1.3 – Tableau de routage[8].

TABLE 1.1 – Analyse d'une table de routage.

Champs	Signification
D	Décris comment la route a été découverte
10.1.1.0/24	Indique le réseau de destination
90	Indique la distance administrative (fiabilité) de la source ou de la route
2170112	Précisez la distance nécessaire pour rejoindre le réseau distant
209.165.200.226	Fournissez l'adresse IP de l'étape suivante pour accéder au réseau distant.
00 :00 :05	Précisez la durée depuis la découverte de la route
S 0/0/0	Précisez l'interface de sortie du routeur utilisée pour accéder au réseau de destination.

Fonctionnement :

Pour permettre la communication entre les machines A et B, lorsque le terminal A réalisé que son homologue B ne se trouve pas dans son domaine de diffusion, il encapsule le paquet de données. D'abord, il ajoute un en-tête de niveau 3 contenant les adresses IP source d'A et destination de B, puis un en-tête de niveau 2 avec les adresses MAC source d'A et destination de la passerelle par défaut pour B.

Le commutateur achemine ensuite le paquet vers le routeur. À réception, le routeur décapsule l'en-tête IP pour identifier l'adresse IP de B. Basé sur cette adresse, le routeur consulte sa table de routage pour déterminer le prochain saut.

Une fois le prochain saut trouvé, le paquet est à nouveau encapsulé avec un en-tête de niveau 3 contenant les adresses IP source d'A et destination de B, et un en-tête de niveau 2 avec les adresses MAC source du routeur actuel et destination du prochain routeur sur le chemin.

Ce processus se répète jusqu'à ce que le paquet atteigne le routeur connecté au terminal B, permettant ainsi la communication entre les deux machines situées dans des sous-réseaux différents.

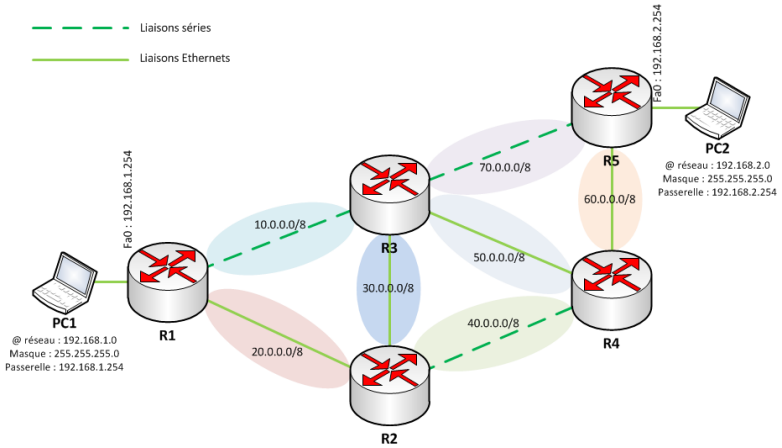

FIGURE 1.4 – Exemple de routage IP [11].

1.4 Type de routage

Un routeur peut apprendre des réseaux distants de deux manières distinctes :

1.4.1 Routage statique

Le routage statique est une méthode de configuration manuelle des routes dans un réseau informatique. Dans ce mode de routage, les chemins sont déterminés et configurés explicitement par un administrateur réseau sur chaque routeur. Les routes statiques restent constantes tant qu'elles ne sont pas modifiées manuellement, offrant ainsi stabilité et contrôle direct sur le trafic réseau. Cependant, cette méthode est moins adaptable aux changements de topologie et peut être fastidieuse à maintenir dans de grands réseaux.

TABLE 1.2 – Les avantages et les inconvénients du routage statique.

Les avantages	Les inconvénients
•Les routes statiques ne sont pas annoncées sur le réseau, pour une meilleure sécurité. •Les routes statiques utilisent moins de bande passante que les protocoles de routage dynamique, aucun cycle de processeur n'est utilisé pour calculer et communiquer des routes. • Le chemin qu'une route statique utilise pour envoyer des données est connu.	•La configuration initiale et la maintenance prennent du temps. • la configuration présente des risques d'erreurs, tout particulièrement dans les grands réseaux. • l'intervention de l'administrateur est requise pour assurer la mise à jour des informations relatives aux routes. • n'évolue pas bien avec les réseaux en expansion et la maintenance devient fastidieuse.

1.4.2 Routage dynamique

Le routage dynamique est une méthode automatisée pour déterminer les chemins de transmission des données dans un réseau. Dans ce mode de routage, les routes sont calculées et mises à jour automatiquement par des protocoles de routage dynamique, qui échangent des informations entre les routeurs pour évaluer les meilleures routes possibles. Les routes dynamiques s'adaptent aux changements de la topologie du réseau, offrant ainsi une plus grande flexibilité et une gestion simplifiée des réseaux de grande taille ou en évolution constante. Cependant, cette méthode est plus complexe à configurer et à dépanner, et peut générer un trafic de routage supplémentaire sur le réseau.

1.5 Protocoles de routage

Les protocoles de routage sont des langages ou des algorithmes utilisés par les routeurs pour déterminer les chemins les plus appropriés à travers lesquels les données doivent être envoyées dans un réseau. Les protocoles de routage peuvent être classés en protocoles de routage interne et protocoles de routage externe en fonction de la portée de leur utilisation [6] :

1.5.1 Routage interne

C'est le processus de détermination des chemins à l'intérieur d'un seul système autonome (AS). Il est utilisé pour router le trafic entre les différents réseaux et sous-réseaux qui composent cet AS. Les protocoles de routage interne sont conçus pour fonctionner efficacement à l'intérieur d'un réseau spécifique et sont utilisés pour échanger des informations de routage entre les routeurs appartenant à cet AS, Protocoles de routage interne :

- **RIP (Routing Information Protocol)** : Un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique pour déterminer le chemin optimal.
- **OSPF (Open Shortest Path First)** :Un protocole de routage à état de lien qui utilise le coût du chemin comme métrique. Il est conçu pour fonctionner efficacement sur de grands réseaux.
- **EIGRP (Enhanced Interior Gateway Routing Protocol)** :Un protocole de routage propriétaire développé par Cisco, qui combine des aspects de routage à vecteur de distance et à état de lien.
- **IS-IS (Intermediate System to Intermediate System)** : Un protocole de routage à état de lien utilisé principalement dans les réseaux IP à grande échelle, tels que les réseaux de fournisseurs de services.

1.5.2 Routage externe

Il s'agit de l'échange d'informations de routage entre différents systèmes autonomes (AS). Ce processus permet de router le trafic entre des réseaux appartenant à des entités distinctes, telles que des réseaux d'entreprise ou des fournisseurs de services Internet (ISP). Les protocoles de routage externe, notamment le Border Gateway Protocol (BGP), sont utilisés pour échanger des informations de routage entre les AS et prendre des décisions de routage basées sur des critères tels que la politique de routage et la disponibilité des chemins.

- **BGP (Border Gateway Protocol)** :Un protocole de routage de passerelle de frontière utilisé pour échanger des informations de routage entre les systèmes autonomes sur Internet.

1.6 Limites de Routage IP

Le routage IP présente des limitations en termes de traitement du trafic, principalement en raison des nombreuses opérations nécessaires qui sont très exigeantes en termes de temps CPU, telles que :
• La dés encapsulation de l'en-tête et de la queue de la trame pour isoler le paquet.
• L'examen de l'adresse IP de destination du paquet IP pour déterminer le meilleur chemin dans la table de routage.
• L'encapsulation du paquet dans une nouvelle trame, puis le transfert de cette trame à l'interface de sortie.

1.7 Définition de MPLS

MPLS, signifiant Multi Protocol Label Switching, est une technologie de réseau essentielle pour l'acheminement efficace des données. En utilisant des étiquettes, il peut créer des circuits virtuels et améliorer la gestion du trafic, la qualité de service et les performances globales des réseaux. Comprendre MPLS est donc crucial pour les professionnels des réseaux afin de rester compétitifs sur le marché du travail en évolution constante.Sa fonction principale est de combiner le concept de routage IP de couche 3 avec le mécanisme de commutation de couche 2, ainsi le MPLS est considéré comme étant un protocole de couche 2,5[2].

1.7.1 Eléments du MPLS

Dans les réseaux MPLS, le transfert des données est assuré par des équipements, tels que des routeurs ou des commutateurs, qui sont capables de lire les étiquettes et de les remplacer en fonction des informations de routage, mais qui ne sont pas en mesure d'examiner les en-têtes de la couche réseau sous-jacente[6].
Les principaux équipements utilisés dans une architecture MPLS sont :

1. **Étiquettes (Labels) :**
   Les étiquettes sont des identifiants numériques attachés aux paquets pour indiquer le chemin à suivre à travers le réseau MPLS. Chaque étiquette est associée à un FEC (Forwarding Equivalence Class) et est utilisée par les LSR pour décider comment router les paquets.
2. **Routeurs Label Edge (LER) :**
   Ces routeurs sont situés aux extrémités du réseau MPLS. Ils ajoutent, modifient ou suppriment les étiquettes des paquets entrants ou sortants, et sont responsables de l'initiation et de la terminaison des tunnels MPLS.
   Les deux types de LER qui existent sont :

•Ingress LER : Est un routeur qui gère le trafic qui entre dans un réseau MPLS.

• Egress LER : Est un routeur qui gère le trafic qui sort d'un réseau MPLS.

3. **Routeurs Label Switch (LSR)** :
   Ces routeurs sont situés à l'intérieur du réseau MPLS et sont chargés de commutation des paquets en fonction des étiquettes. Ils utilisent des tables de commutation pour déterminer comment router les paquets en fonction des étiquettes associées.
   • L'échange d'information de réseau.
   •L'échange de label.
   • L'acheminement des paquets
4. **FIB (Forwarding Information Base) :**
   La FIB est une table de routage spécifique aux routeurs MPLS, utilisée pour prendre des décisions de commutation en fonction des étiquettes MPLS associées aux paquets. Contrairement à la table de routage IP traditionnelle, la FIB est optimisée pour commuter les paquets en utilisant des étiquettes MPLS plutôt que des adresses IP. Elle associe les étiquettes MPLS à des interfaces de sortie ou à des chemins de commutation spécifiques, garantissant un acheminement efficace des paquets à travers le réseau MPLS.
5. **Label Forwarding Information Base (LFIB) :**
   Une table de routage spécifique aux routeurs MPLS qui stocke les correspondances entre les étiquettes MPLS entrantes et les interfaces de sortie.
6. **Label Distribution Protocol (LDP) :**
   Un protocole utilisé par les routeurs MPLS pour échanger des informations d'étiquetage et établir des chemins dans le réseau MPLS.
7. **Traffic Engineering :**
   MPLS permet une meilleure gestion du trafic en utilisant des étiquettes pour optimiser l'utilisation des ressources réseau.
   Des technologies telles que MPLS-TE (Traffic Engineering) sont utilisées pour équilibrer la charge et éviter les embouteillages.
8. **Quality of Service (QoS) :**
   MPLS prend en charge les mécanismes de QoS en permettant la classification et la gestion du trafic basées sur des étiquettes.
   Cela garantit que les paquets critiques sont transmis avec la priorité appropriée.
9. **Réseau privé virtuel (VPN) :**
   MPLS est souvent utilisé pour créer des VPN en utilisant des étiquettes pour segmenter le trafic de différents clients sur un réseau partagé.

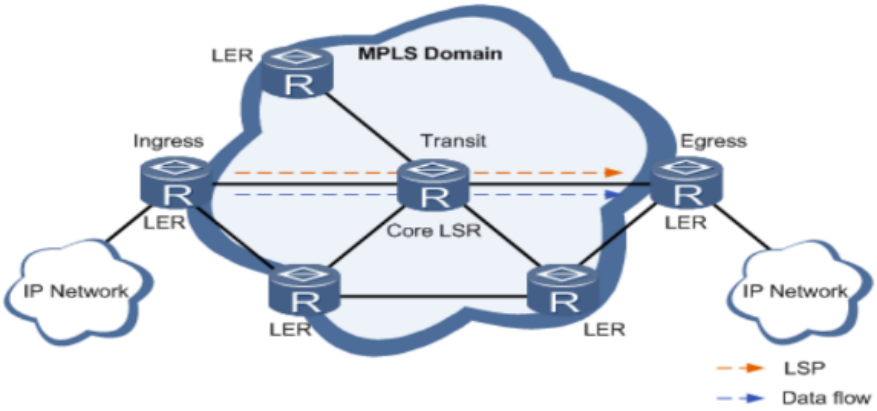

FIGURE 1.5 – Structure du réseau MPLS [11].

1.7.2 Structure de données des labels

Les routeurs du domaine MPLS construisent trois bases d'informations FIB, LFIB et LIB, ces bases d'informations sont construites selon plusieurs étapes : Les protocoles de routage (OSPF, IS-IS ou EIGRP) construisent les tables de routages.

• Chaque LSR alloue indépendamment un label à chaque destination dans sa table de routage.
• Les labels alloués sont enregistrés dans la LIB.
• Ces labels et leurs prochains sauts ont enregistrés dans la table LFIB avec l'action à effectuer.
• Le LSR envoie les informations sur sa LIB à ces voisins.
• Chaque LSR enregistre les informations reçues dans sa LIB.
• Les informations reçues des prochains sauts sont enregistrées dans la FIB.
• Chaque LSR construit ses propres structures FIB, LFIB et LIB.

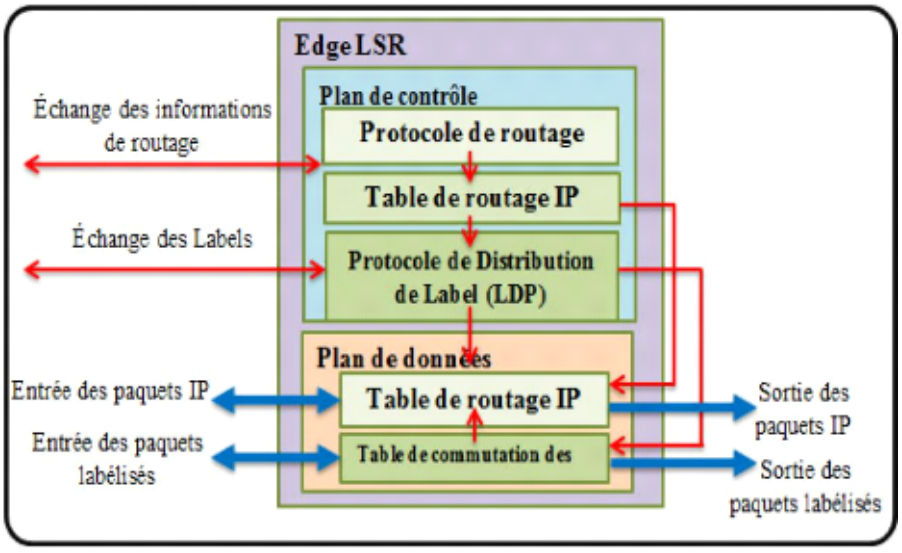

FIGURE 1.6 – Architecture simplifiée d'un réseau MPLS [12].

1.7.3 Fonctionnement de MPLS

Lorsqu'un paquet de données entre dans un réseau MPLS, un routeur spécifique appelé Label Edge Router (LER) lui assigne une étiquette MPLS. Cette étiquette est ensuite ajoutée à l'en-tête du paquet pour faciliter son identification et son traitement efficace au sein du réseau.

Une fois que le paquet est étiqueté, il est acheminé à travers le réseau en se basant sur cette étiquette plutôt que sur son adresse IP d'origine. Les routeurs MPLS le long du parcours, connus sous le nom de Label Switch Routers (LSR), utilisent ces étiquettes pour guider les paquets vers leur destination en suivant un chemin prédéterminé.

Pour établir ce chemin, un mécanisme appelé Label-Switched Path (LSP) est instauré entre les routeurs MPLS impliqués dans le parcours souhaité. Ce processus, déterminé par des protocoles de signalisation tels que LDP (Label Distribution Protocol) ou RSVP-TE (Resource Réservation Protocol - Traffic Engineering), assure une transmission efficace des paquets le long du réseau.

À chaque nœud MPLS traversé, les étiquettes MPLS sont utilisées pour commuter les paquets vers la prochaine étape du parcours. Lorsque le paquet atteint le dernier nœud MPLS du parcours, l'étiquette MPLS est retirée avant que le paquet ne soit transféré au réseau suivant.

Pour que les LSR puissent commuter correctement les paquets il doit procéder comme suit :

• Le Ingres LER (devise B) récupère le trafic des utilisateurs ayant la même adresse IP de destination (FEC) et leur attribue des labels avant de les envoyer vers l'interface de sortie (GE1/0/1) cette méthode appelé PUSH. Ensuite le paquet arrive au LSR, celui-ci consulte le label du paquet et le cherche dans sa LFIB pour déterminer vers quelle sortie commuter le paquet.

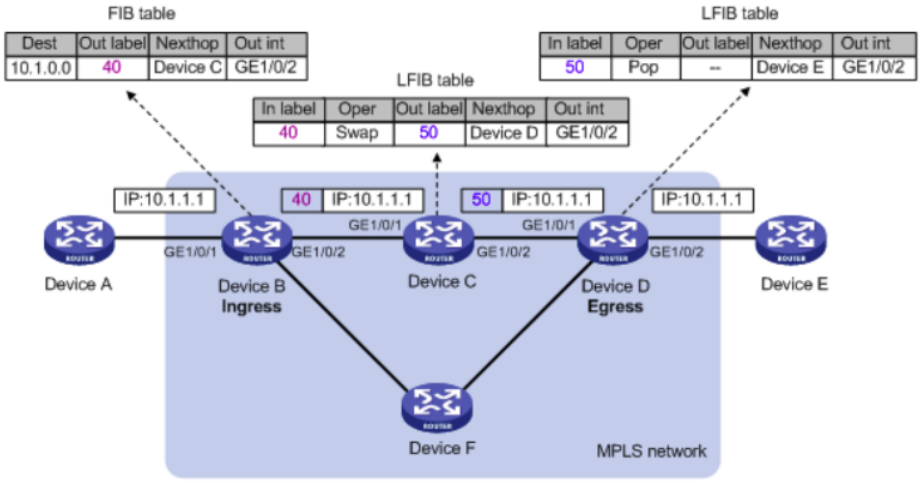

FIGURE 1.7 – Schéma de Routage et CommutationMPLS [13].

Les paquets arrivent au LSR (device C) ce dernier lui applique la méthode SWAP qui consiste à remplacer le label d'entrée (40) par le label de sortie (50) et consulte sa table LFIB pour déterminer vers quelle sortie les commuter, cette sortie n'est qu'autre que l'interface G1/0/2 qui relie le device C avec le device D.

• L'étape de commutation sera exécutée par tous les LSR du LSP jusqu'à atteindre le LER de sortie en l'occurrence le device D.

• A l'arrivée du trafic au device D, ce dernier consulte sa table LFIB et constate que l'opération appropriée est le POP qui consiste en la suppression du label est par conséquent le début d'un routage classique.

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

1.7.4 Architecture du MPLS

L'architecture logique du MPLS est conçue de telle manière à supporter plusieurs protocoles de niveau 2 (Ethernet ou ATM) ainsi que ceux de niveau 3 (OSPF, RIP et BGP...), cette architecture est constituée de deux plans séparés[14] :

•Le plan de contrôle :

1. Protocoles de Signalisation : Ces protocoles permettent aux routeurs MPLS de communiquer entre eux pour établir et maintenir les chemins Label-Switched Paths (LSP) et distribuer les étiquettes MPLS.
2. Routeurs de Contrôle : Ces routeurs sont responsables du calcul et de la distribution des chemins LSP dans le réseau. Ils utilisent les informations de routage pour prendre des décisions concernant la commutation des étiquettes.

3. Base de Données de Routage : Cette base de données contient des informations sur la topologie du réseau et les chemins LSP établis. Elle est utilisée par les routeurs de contrôle pour calculer les chemins optimaux et distribuer les étiquettes MPLS

•Le plan de données : Le plan de donnée connu également sous le nom de forwarding plane. Ce plan est indépendant des protocoles de routage et de distribution des labels. Il permet d'acheminer les paquets labélisés à travers le réseau MPLS en se basant sur la table LFIB et LIB.

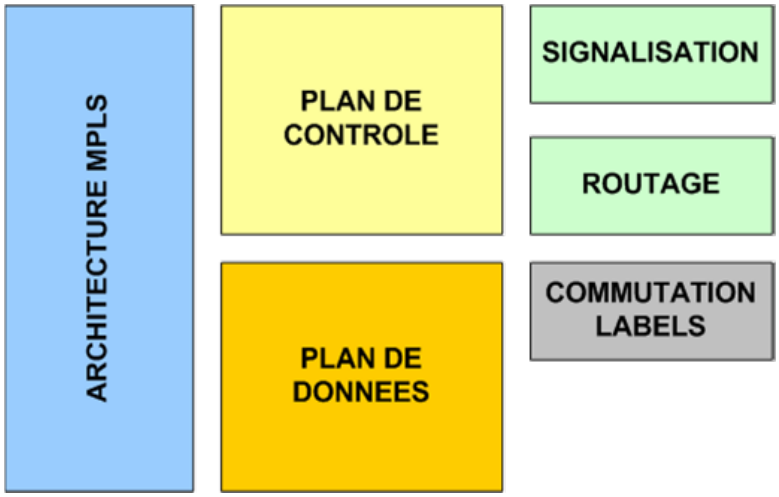

FIGURE 1.8 – Architecture de MPLS : Plans de Contrôle et de Données [15].

1.7.4.1 Format d'un label

Un label est un indice codé sur 32 bits inséré par le LER et identifie le chemin que le paquet doit suivre dès son entrée dans un nuage MPLS. Le label est directement encapsulé et transporté dans le paquet, pour être inséré entre l'entête de niveau 2 (adresses MAC) et celui de niveau 3 (adresses IP), chaque paquet devra suivre un voyage qui sera basé sur une commutation de labels dès qu'il reçoit son étiquette[16].

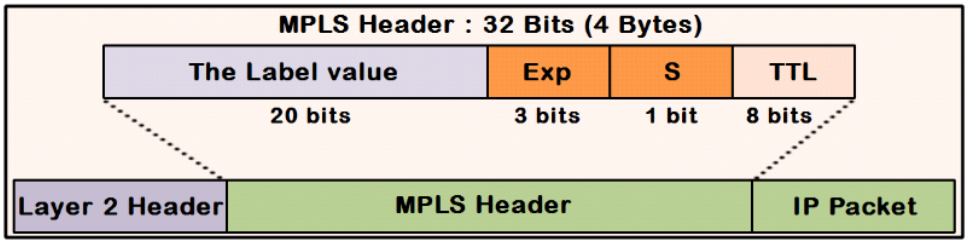

FIGURE 1.9 – Format générique d'une étiquette MPLS[17]

1. **Label Value (20 bits) :** Ce champ contient la valeur numérique du label MPLS, qui est utilisée pour identifier une entrée dans la table de commutation MPLS.

2. **Experimental (3 bits) :** Ces bits sont utilisés pour des fonctions expérimentales ou pour la qualité de service (QoS). Ils peuvent être utilisés pour définir différentes classes de traitement pour les paquets MPLS.
3. **Bottom of Stack (1 bit) :**Ce bit indique si le label actuel est le dernier dans la pile de labels. S'il est réglé à 1, cela signifie que c'est le dernier label dans la pile.
4. **Time to Live (TTL) (8 bits) :** Ce champ indique le nombre maximal de sauts (hops) que le paquet peut effectuer avant d'être rejeté. Il est utilisé pour éviter les boucles dans le réseau.

1.7.4.2 Pile de labels

Le concept d'empilement de labels dans MPLS permet à chaque paquet MPLS de transporter plusieurs étiquettes. Les LSR en périphérie du réseau ont la responsabilité de pousser ou de retirer les étiquettes pour indiquer le niveau d'utilisation actuel des étiquettes. Lorsqu'un LSR reçoit un paquet étiqueté, il examine uniquement la dernière étiquette de la pile pour déterminer comment commuter le paquet. L'empilement de labels permet notamment d'associer plusieurs contrats de services à un flux pendant son parcours dans le réseau MPLS. Les applications nécessitant l'empilement incluent les VPN, TE et LDP [18].

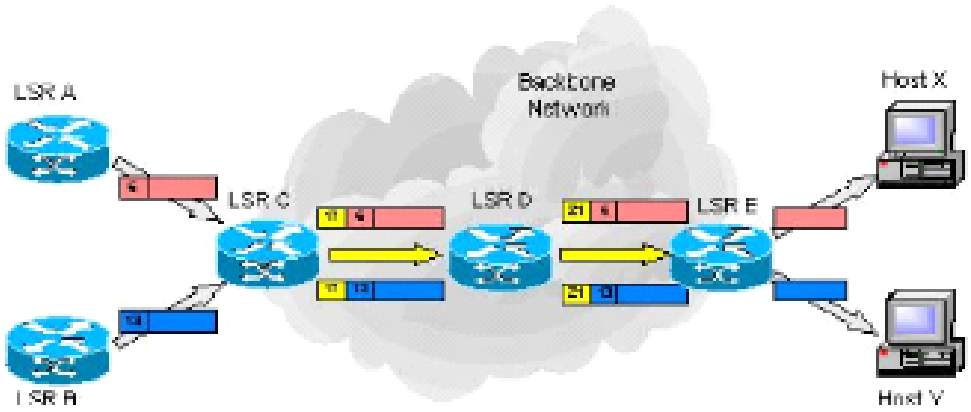

FIGURE 1.10 – Pile de labels[19].

1.7.4.3 Opérations sur les labels

Pour MPLS, les trois opérations de base sur les étiquettes (Empiler, Changer et Dépiler) constituent l'ensemble nécessaire des opérations[18].

•L'insertion/empilement (PUSH) : Est le processus d'ajout de labels aux paquets IP par les routeurs LER.

•Le processus d'échange (SWAP) : Consiste à échanger des étiquettes dans le réseau MPLS. Cette tâche est confiée aux routeurs situés au cœur du réseau du fournisseur de services. Les étiquettes sont échangées entre ces routeurs P à travers le LSP (Label Switch Path) qui est établi entre les routeurs PE frontières.

•La suppression ou dépilement (POP) : Est le processus par lequel le dernier label est retiré. Ce processus permet d'envoyer le trafic pur au client. Habituellement, la suppression est effectuée sur les routeurs PE, mais dans certains cas, elle peut être effectuée avant le routeur PE, sur le dernier routeur P. Ce processus spécifique est appelé Pénultième Hop Popping (PHP).

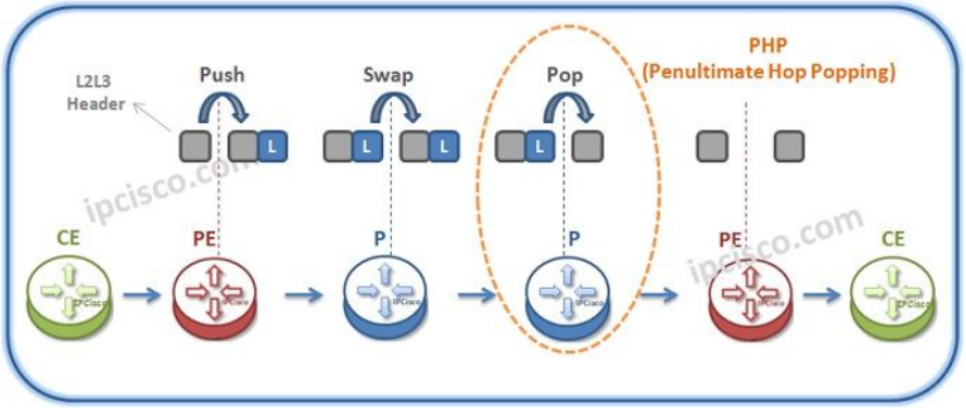

FIGURE 1.11 – Opérations sur les labels[20].

1.7.4.4 Principe de connexion du LDP

Le processus de connexion du LDP repose sur une séquence simple : tout d'abord, deux routeurs adjacents échangent des messages UDP de type "HELLO" pour signaler leur présence mutuelle. Ensuite, une connexion TCP est établie entre ces routeurs voisins en échangeant des messages "TCP Open". En réponse, un message "Initialisation" est renvoyé pour démarrer le transport des messages d'annonce des labels.

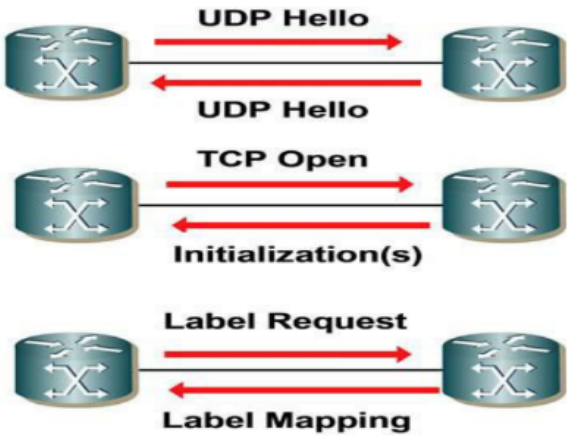

FIGURE 1.12 – Fonctionnement du protocole de signal LDP[21].

— Hello Messages : Utilisés pour établir des adjacences LDP et maintenir la connectivité.

— Initialization Messages : Négocient les paramètres initiaux de la session LDP.

— Advertisement Messages : Annoncent les informations de libellé aux routeurs voisins.

— Label Request Messages : Demandent un libellé spécifique pour une route donnée à un routeur voisin.

— Label Mapping Messages : Répondent aux demandes de libellés en envoyant le libellé demandé avec l'adresse IP associée.

— Withdrawal Messages : Retirent un libellé de la table de libellés du routeur voisin lorsqu'il n'est plus nécessaire ou valide.

— Notification Messages : Informent les routeurs voisins de tout événement important.

1.7.4.5 Distribution des labels

— **Distribution statique de labels :** Les libellés sont configurés manuellement sur chaque routeur MPLS. Cette approche est simple à mettre en œuvre mais manque de flexibilité pour s'adapter aux changements dynamiques du réseau[22].

— **Distribution dynamique de labels :** Les libellés sont attribués automatiquement aux FEC à mesure que les paquets traversent le réseau, généralement via des protocoles de signalisation comme LDP ou RSVP-TE. Cette approche offre une meilleure adaptation aux changements du réseau et des besoins en trafic, mais peut nécessiter plus de ressources de calcul et de gestion[22].

1. **LDP (Label Distribution Protocol) :** LDP est l'un des protocoles les plus couramment utilisés pour distribuer les labels dans un réseau MPLS. Il utilise un mécanisme de "push" pour distribuer les labels le long des chemins MPLS. Lorsqu'un routeur MPLS reçoit un paquet IP, il assigne un label au FEC (Forwarding Equivalence Class) correspondant, puis distribue ce label à ses routeurs voisins via le protocole LDP. Chaque routeur LDP maintient une table de libellé (Label Forwarding Information Base - LFIB) qui associe les FEC entrants avec les libellés sortants.
2. **RSVP-TE (Resource Reservation Protocol - Traffic Engineering) :** SVP-TE est utilisé pour fournir des fonctionnalités avancées de trafic engineering dans un réseau MPLS. Contrairement au LDP, qui distribue simplement des labels pour le commutateur de paquets, RSVP-TE permet aux routeurs MPLS de créer explicitement des chemins LSP (Label Switched Paths) à travers le réseau en réservant des ressources et en distribuant des libellés le long de ces chemins. Les libellés sont distribués en utilisant des messages RSVP-TE et sont utilisés pour étiqueter les paquets de données qui suivent ces chemins LSP.

1.7.5 Protocoles de signalisation

Dans un environnement IP/MPLS, la signalisation implique les échanges d'informations entre les Label Switching Routers (LSR), permettant ainsi de partager les informations de routage et les étiquettes associées aux paquets circulant dans le domaine MPLS. Les protocoles de signalisation

remplissent ce rôle crucial en informant les autres LSR sur les chemins à emprunter et les étiquettes à utiliser pour acheminer les paquets[23] :

- **CR-LDP, RSVP-TE (Resource Reservation Protocol - Traffic Engineering) :** Utilisés en trafic Engineering pour établir des LSP en fonction de critère de ressources.
- **BGP (Border Gateway Protocol) :** BGP est utilisé pour l'échange d'informations de routage entre les routeurs de bord MPLS, notamment pour la distribution de routes VPN (Virtual Privat Network) dans les réseaux MPLS VPN. Dans le contexte de MPLS, BGP est utilisé pour distribuer des routes IPv4 ou IPv6, ainsi que des labels MPLS associés.
- **OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System) :** Ces protocoles de routage interne sont souvent utilisés pour la distribution des informations de routage dans les réseaux MPLS. Ils peuvent être utilisés pour distribuer des préfixes IP ainsi que des informations de labels MPLS associés.
- **TDP/LDP (Tag/Label Description protocole) :**Pour le mapping des adresses unicast ,simple et largement utilisé pour les déploiements MPLS standard sans exigences strictes de QoS.

1.7.6 Applications du MPLS

L'un des principaux atouts de l'MPLS est sa capacité à intégrer de nouvelles fonctionnalités de gestion de qualité de services et d'ingénierie du trafic pour répondre aux exigences des clients

- **Ingénierie de trafic (MPLS-TE)**
  MPLS permet de définir des chemins de routage explicites pour le trafic, contournant ainsi les limitations du routage IP traditionnel basé sur le "meilleur chemin ».Cela offre plus de contrôle et de flexibilité pour optimiser l'acheminement des flux de données critiques, en tenant compte de paramètres comme la bande passante, la latence et la fiabilité[24].
- **VPN MPLS**
  MPLS est un outil précieux pour la création de réseaux privés virtuels (VPN) sécurisés. En utilisant des labels distincts pour chaque VPN, MPLS garantit la confidentialité et l'isolation du trafic sensible de chaque client.
- **Qualité de service (QoS)**
  MPLS facilite la mise en œuvre de la QoS en priorisant certains types de trafic sur le réseau.En fonction des labels attribués, MPLS peut réserver de la bande passante et minimiser la latence pour les applications critiques en temps réel, telles que la voix sur IP (VoIP) ou la vidéoconférence [25].
- **Migration vers IPv6**
  En s'appuyant sur l'infrastructure MPLS déjà en place pour les VPN, il permet de migrer progressivement les sites distants vers le nouveau protocole sans perturber le trafic global.

1.7.7 MLPS VPN

1.7.7.1 Définition MPLS/VPN

Un VPN (Virtual Private Network) est une liaison permanente, distante et sécurisée entre deux sites (ou plus) d'une organisation (entreprise). Les réseaux privés virtuels basés sur la technologie MPLS simplifient considérablement le déploiement des services VPN par rapport aux VPN traditionnels. La mise en place des VPN est garantie par les opérateurs avec deux technologies largement déployées : la technologie des VPN/IP et celle des VPN/MPLS.
IPSec est une autre approche permettant de mettre en œuvre des VPN sur le réseau IP.
L'IPSec privilégie la sécurisation des flux d'informations par encryptage des données alors que MPLS se concentre plutôt sur la gestion de la qualité de service et la priorité des flux. Le problème de sécurité dans MPLS/VPN est minimal dans le cas d'un réseau propriétaire (non Internet). Cependant, si cette garantie n'est pas suffisante, il existe des solutions qui permettent d'utiliser en même temps MPLS et IPSec et ainsi de construire des VPN disposant des avantages des deux approches en même temps : la souplesse de MPLS et la sécurisation d'IPSec[26].

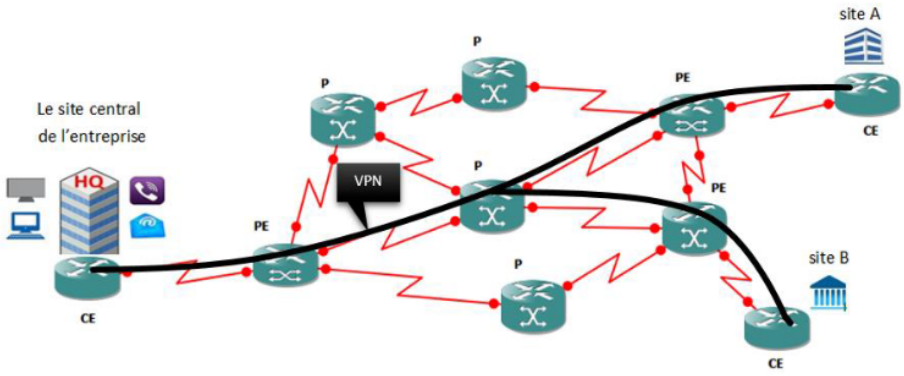

FIGURE 1.13 – Illustration d'un Réseau MPLS avec VPN[27].

1.7.7.2 Fonctionnement

Un VPN (Virtual Private Network) fonctionne en créant une connexion sécurisée entre votre appareil (comme un ordinateur ou un smartphone) et un serveur distant géré par un service VPN. Lorsque vous vous connectez à Internet via un VPN, vos données sont d'abord cryptées par votre appareil, puis envoyées via un « tunnel » sécurisé vers le serveur VPN. Ce serveur VPN est situé ailleurs et se charge de décrypter vos données et de les envoyer vers leur destination finale, comme un site Web. Par conséquent, sur les sites Web et autres services en ligne, il semble que vous accédez à Internet depuis l'emplacement du serveur VPN plutôt que depuis votre emplacement réel. Cette méthode masque votre véritable adresse IP, protégeant votre vie privée et rendant plus difficile la surveillance de vos activités en ligne par les pirates informatiques ou les FAI. Mieux encore, le cryptage des données empêche les intrus de lire les informations sensibles, ce qui est particulièrement utile lors de l'utilisation de réseaux Wi-Fi publics.

1.7.7.3 Avantages de VPN

- **Protection de la vie privée :** Il masque votre adresse IP, rendant votre activité en ligne plus difficile à suivre.
- **Sécurité des données :** Il chiffre vos données, les protégeant des pirates, surtout sur les réseaux Wi-Fi publics.
- **Accès aux contenus bloqués :** Il vous permet de contourner les restrictions géographiques pour accéder à des sites web et des services de streaming de n'importe où.
- **Navigation anonyme :** Il cache votre identité en ligne, utile pour protéger votre vie privée.

1.8 Conclusion

Les réseaux IP/MPLS jouissent d'un avenir prometteur, étant omniprésents dans les infrastructures des opérateurs. Leur valeur réside dans leur capacité à surmonter les limitations des protocoles de routage IP classiques en introduisant la commutation de labels. De plus, ces réseaux offrent une solution attrayante en intégrant aisément de nouvelles technologies axées sur la virtualisation des services réseau, comme le VPLS, pour fournir des offres virtuelles aux clients. La virtualisation devient ainsi un concept essentiel pour la transformation des réseaux d'opérateurs, ce qui constituera le thème central de notre prochain chapitre[28].

Chapitre 2

Protocoles de routage interne à état de lien

2.1 Introduction

Le protocole interne est responsable de la gestion des routeurs au sein du domaine. L'une de leurs principales fonctionnalités (au moins sur les réseaux de diffusion) est de rechercher automatiquement d'autres routeurs et de découvrir la topologie du réseau pour déterminer le chemin le plus approprié. Afin de créer des tables de routage, les routeurs doivent comprendre l'état du réseau. Chaque appareil doit diffuser des informations qui le concernent. Mais la diffusion ne doit pas provoquer de boucles ou de duplications de messages. Il existe deux grandes familles de protocoles : Algorithmes basés sur des vecteurs de distance où chaque routeur n'a qu'une vue partielle du réseau, ce qui est le cas du RIP. Les algorithmes basés sur l'état des liens, dans lesquels chaque routeur construit la vision globale du réseau, sont le cas d'OSPF et d'IS-IS dans le monde ISO.

2.1.1 Rôle crucial des IGP dans le routage des paquets au sein d'un réseau autonome

Les protocoles de routage interne (IGP), tels que RIP, OSPF et IS-IS, jouent un rôle essentiel dans le routage des paquets au sein des réseaux autonomes. Ils permettent aux routeurs de découvrir et d'échanger des informations sur les réseaux internes et de créer des tables de routage pour le routage intra-domaine.

1. Découverte de la topologie du réseau :

IGP permet à un routeur de découvrir automatiquement les réseaux connectés et les routeurs voisins. Cette découverte s'effectue en envoyant et en recevant des messages de routage spécifiques à chaque protocole. Le routeur construit ensuite une carte topologique du réseau sur la base des informations reçues.

2. Échange d'informations de routage :

IGP facilite l'échange d'informations de routage entre les routeurs, telles que les adresses IP du réseau, les mesures de routage (coût, nombre de sauts) et les informations sur les interfaces de connexion. Ces informations sont essentielles pour déterminer le meilleur chemin pour acheminer le paquet vers sa destination.

3. Création et maintenance des tables de routage :

Sur la base des informations de routage échangées, chaque routeur crée et gère sa propre table de routage. Une table de routage contient une entrée pour chaque destination possible, indiquant le meilleur chemin vers la destination. Les tables de routage sont mises à jour dynamiquement en fonction des changements de topologie ou des changements dans les informations de routage reçues.

4. Sélectionnez le meilleur chemin pour acheminer le paquet :

Lorsque les routeurs reçoivent un paquet, ils consultent les tables de routage pour déterminer le

meilleur chemin vers une destination donnée. La sélection du meilleur chemin se fait en fonction des métriques de routage associées à chaque chemin, en privilégiant le chemin le plus court ou le moins cher.

5. Convergence et stabilité du routage : IGP garantit une convergence rapide des tables de routage après des changements de topologie, tels que l'ajout ou la suppression de liens ou de routeurs. Cela permet au routeur de s'adapter rapidement aux changements du réseau et de maintenir un routage stable et efficace.

6. Optimisez le trafic et les performances du réseau : IGP aide à optimiser le trafic en choisissant le chemin le plus efficace pour acheminer les paquets, réduisant ainsi la latence et la congestion du réseau. Ils contribuent également à améliorer les performances globales du réseau en garantissant une utilisation optimale des ressources disponibles.

7. Facilitez la gestion du réseau : IGP simplifie la gestion du réseau en fournissant des informations précieuses sur la topologie du réseau, les routes disponibles et les mesures de routage. Ces informations permettent aux administrateurs réseau de mieux comprendre les opérations du réseau et d'identifier rapidement les problèmes de routage potentiels.

2.1.2 Comparaison détaillée entre les protocoles de routage interne (IGP) et les protocoles de routage externe (EGP)

TABLE 2.1 – Tableau comparatif : Fonctionnalités clés des protocoles IGP et EGP

Fonctionnalité	Protocoles de routage interne (IGP)	Protocoles de routage externe (EGP)
Portée	Utilisés au sein d'un réseau autonome ou d'une organisation	Employés pour le routage entre des réseaux autonomes ou des domaines de routage distincts.
Exemples	RIP, OSPF, IS-IS.	BGP (Border Gateway Protocol).
Fonctionnement et algorithmes de routage	Utilisent généralement des algorithmes de routage à vecteur de distance (par exemple, RIP) ou à état de liaison (par exemple, OSPF). Se basent sur des métriques de routage comme le nombre de sauts ou le coût pour déterminer le meilleur chemin.	Adoptent principalement l'algorithme de routage par vecteur de chemin (BGP). Échangent des informations sur les réseaux autonomes et leurs politiques de routage.
Échange d'informations de routage	Utilisent des messages de routage spécifiques à chaque protocole (par exemple, des paquets RIP, des paquets OSPF, des paquets IS-IS)Peuvent utiliser des techniques d'authentification et de filtrage pour limiter l'accès aux informations de routage..	Établissent des sessions BGP entre les routeurs frontaliers pour échanger des informations sur les réseaux autonomes. Utilisent des mécanismes de politique de routage pour contrôler le flux des informations de routage et la sélection du meilleur chemin.
Applications et considérations	Essentiels pour le routage intra-domaine, permettant une communication fluide entre les périphériques d'un même réseau.	Indispensables pour le routage inter-domaine, reliant les réseaux autonomes et permettant l'accès à Internet.

2.2 Fonctionnement détaillé des protocoles de routage interne

2.2.1 Protocole OSPF

2.2.1.1 Présentation du protocole OSPF

L'OSPF est un protocole de routage basé sur l'état des liens qui a été créé afin de substituer le protocole de routage basé sur le vecteur de distance RIP. Au début des réseaux et d'Internet, le protocole RIP était considéré comme un protocole de routage accepté. Toutefois, le protocole RIP était rapidement devenu problématique en se basant uniquement sur le nombre de sauts comme seule mesure pour déterminer la meilleure route. Les réseaux de grandes tailles avec plusieurs chemins de vitesses variables ne peuvent pas être utilisés avec le nombre de sauts. Les avantages du protocole OSPF par rapport au protocole RIP sont importants, car il permet une convergence plus rapide et s'adapte mieux aux réseaux de plus grande taille.

2.2.1.2 Fonctionnement du protocole OSPF

Afin de gérer efficacement un réseau OSPF, il est essentiel de saisir le fonctionnement interne du protocole. Lorsqu'ils sont utilisés dans une même zone, les routeurs qui utilisent OSPF doivent accomplir les tâches suivantes avant de pouvoir réaliser leur travail de routage[29] :

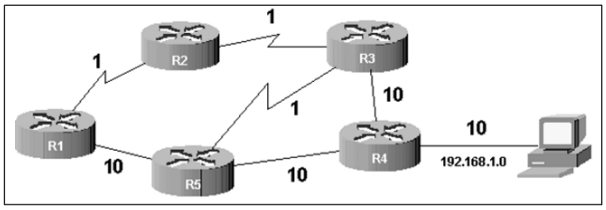

FIGURE 2.1 – Exemple d'une topologie utilisant OSPF comme protocole de routage[29].

État initial : Tous les routeurs de la figure sont inactifs dans le processus de routage OSPF.

Établir la liste des routeurs voisins : les routeurs OSPF sont très performants. Une fois qu'ils sont mis en marche, ils doivent se présenter et faire la connaissance de leurs voisins. Effectivement, une fois le processus de routage initié sur R1, des paquets de données (connus sous le nom de paquets HELLO) sont transmis à chaque interface où le routage dynamique a été activé. On utilise l'adresse multicast 224.0.0.5, tout routeur OSPF est considéré comme destinataire. L'objectif de ces paquets est de se faire connaître par ses voisins. On considère que deux routeurs sont voisins s'ils partagent au moins un lien commun. À titre d'illustration, dans la figure, R1 et R2 sont proches, mais pas R1 et R3. Les paquets HELLO émis par R1 sont récupérés par le processus de routage OSPF sur R2 toutes les 10 secondes. L'adresse IP de R1 est enregistrée dans une base de données appelée « base d'adjacences »

par R2. Les adresses des routeurs voisins sont contenues dans cette base. R2 répond à R1 en utilisant un seul paquet IP. L'adresse IP de R2 est ajoutée à la base d'adjacences de R1. Par la suite, appliquez ce processus à tous les routeurs de la zone. La découverte des voisins est une étape essentielle car OSPF est un protocole basé sur les liens. Il est nécessaire qu'il connaisse ses voisins afin de vérifier s'ils sont toujours accessibles et ainsi déterminer l'état du lien qui les relie.

Élire le routeur spécifié ainsi que le routeur spécifié pour les secours : À l'intérieur d'une zone OSPF qui comprend des réseaux de diffusion (broadcast networks) ou des réseaux à accès multiple sans diffusion (NBMA), il est nécessaire d'opter pour un routeur appelé "routeur désigné" (DR ou Designated Router) et un autre "routeur désigné de secours" (BDR ou Backup Designated Router). Le routeur DR est spécialement conçu pour atteindre trois objectifs :

- Minimiser le flux de données concernant l'état des liens ;
- Renforcer la fiabilité de la base de données topologique ;
- Accélérer le processus de convergence.

Le routeur choisi a la priorité la plus élevée (Router ID). Le nombre de priorité sur 8 bits est initialement fixé à 1 sur tous les routeurs. Afin de déterminer les routeurs ayant la même priorité, celui qui obtient la plus grande adresse IP sur une interface de boucle locale (Loopback Interface) ou sur un autre type d'interface active est élu. Le routeur avec la deuxième plus grande priorité sera le BDR.

Découvrir les routes : Les routeurs permettent automatiquement de transmettre les routes aux réseaux qui contribuent au routage dynamique. La relation entre chaque routeur (non DR ou BDR) et le DR est établie. Le DR démarre la communication en envoyant au routeur un résumé de sa base de données topologique à travers des paquets de données appelés LSA (Link State Advertisement). Il y a principalement l'adresse du routeur, le prix du lien et un numéro de séquence dans ces paquets. Ce numéro permet d'évaluer l'ancienneté des renseignements reçus.Ces paquets comprennent essentiellement l'adresse du routeur, le coût du lien et un numéro de séquence.Ce numéro permet d'évaluer l'ancienneté des renseignements reçus. Lorsque les LSA reçus diffèrent de ceux dans sa base topologique, le routeur sollicite une information plus exhaustive à travers un paquet LSR (Request Link State). Le DR répond en envoyant des paquets LSU (Link State Update) qui contiennent toutes les informations nécessaires. Par la suite, le routeur (non DR ou BDR) envoie les routes les plus avantageuses ou inconnues du DR.

Élire les routes à utiliser : Une fois que le routeur dispose de la base de données topologique, il peut générer la table de routage. L'application de l'algorithme du SPF repose sur la base topologique. Une table de routage est émise qui regroupe les routes les moins coûteuses.

Maintenir la base topologique : Quand un routeur remarque un changement de l'état d'un lien (détection par les paquets HELLO adressés périodiquement par le routeur à ses voisins), il émet un paquet LSU sur l'adresse multicast 224.0.0.6 : le DR et le BDR de la zone sont considérés comme destinataires, ils intègrent cette information à leur base topologique, le DR diffuse l'information sur l'adresse 224.0.0.5 (tous les routeurs OSPF sans distinction), tout changement de topologie déclenche une nouvelle exécution de l'algorithme du SPF et une nouvelle table de routage est crée.

2.2.1.3 Caractéristiques du protocole OSPF

Les caractéristiques du protocole OSPF sont :

- **Classless :** Par conception, il n'a pas de classe.Ainsi, il supporte les masques de sous-réseau de longueur variable (VLSM) et le routage inter-domaine sans classe (CIDR).
- **Efficace :** Les changements de routage déclenchent des mises à jour de routage. Il utilise l'algorithme Shortest Path First (SPF) pour déterminer le meilleur chemin.
- **La rapidité de convergence :** Il propage rapidement les modifications effectuées dans le réseau.
- **Évolutionaire :** Il s'adapte parfaitement aux petits et grands réseaux. Il est possible de grouper les routeurs en zones afin de gérer 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.

2.2.1.4 Algorithme Shortest Path First (SPF) :

L'algorithme SPF est utilisé par OSPF pour créer et calculer le chemin le plus court vers toutes les destinations connues. Le calcul du trajet le plus court est effectué en utilisant l'algorithme Dijkstra. L'algorithme lui-même est plutôt complexe. Une méthode simplifiée pour étudier les différentes étapes de l'algorithme est présentée[30] :

1. Pendant l'initialisation ou en cas de modification des informations de routage, un routeur génère une notification de l'état de la liaison pour la publication. La présente publication regroupe tous les états de liaison sur ce routeur.
2. Chaque routeur échange des informations de liaison en utilisant la propagation. Pour chaque routeur qui reçoit une mise à jour de l'état des liaisons, il est nécessaire de sauvegarder une copie dans sa base de données d'état de liaison, puis de la stocker.
3. Une fois que chaque routeur a rempli sa base de données, il calcule un arbre qui représente le chemin le plus court vers toutes les destinations.
4. Le routeur utilise l'algorithme Dijkstra pour déterminer l'arbre du chemin le plus court. La table de routage IP est composée des destinations, du coût associé et du prochain saut pour atteindre ces destinations.
5. Les paquets d'états de liaison transmettent toutes les modifications qui se produisent, ce qui permet de recalculer l'algorithme Dijkstra pour trouver le meilleur chemin. Chaque routeur est placé à la racine d'un arbre par l'algorithme, qui détermine le chemin le plus court vers chaque destination en se basant sur le coût total requis pour atteindre cette destination.
6. Si le réseau OSPF ne subit aucun changement, tel que le coût d'une liaison ou l'ajout ou la suppression d'un réseau, OSPF devrait être extrêmement silencieux.

Coût OSPF : Le coût d'OSPF est une mesure du coût d'une interface dans OSPF. Indicateur de la charge supplémentaire nécessaire pour envoyer des paquets à travers une interface spécifique. La bande passante d'une interface est inversement liée au coût d'une interface. Un coût plus bas est associé à une bande passante plus élevée.
Le calcul du coût OSPF se fait selon la formule suivante :

Le coût = Bande passante de référence / Bande passante de l'interface

Par défaut, la bande passante de référence est de 10^8 (100 000 000), ce qui signifie que la L'expression est la suivante :

Le coût = 100 000 000 (bits/s) /bande passante de l'interface en bits/s

2.2.1.5 Messages OSPF

Le RIP (ou IGRP) est un protocole à vecteur de distance qui utilise aveuglément le broadcast ou le Multicast en envoyant la table de routage complète à chaque interface toutes les 30 secondes par défaut. En revanche, les routeurs OSPF utilisent 5 types de paquets distincts afin de repérer leurs voisins et de mettre à jour les informations de routage en fonction de l'état de lien[31].
Il exicte 5 types de messages[32] :

1. **Hello :**
   Le routeur envoie des messages HELLO pour faire la connaissance des voisins et maintenir les relations de voisinage. Ils sont envoyés toutes les 10 secondes en unicast et toutes les 30 secondes en multicast. Si quatre HELLO successifs ne sont pas répondus, le voisin est considéré comme DOWN.
2. **Database Description Packet (DBD) :**
   Résumé de l'ensemble des liens que le routeur possède. Lorsqu'un voisin remarque une connexion inconnue dans la DBD, il la demande en utilisant un LSR.
3. **Link-State Request (LSR) :**
   Demande des informations précises concernant les bases de données d'état de liens des routeurs OSPF.
4. **Link-State Update (LSU) :**
   Différents LSA (Link-State Advertisment) sont inclus, c'est une mise à jour qui fournit des informations sur un lien. Il y a différents types :
   - **Type 1 :** Décrit les interfaces d'un routeur.
   - **Type 2 :**Fait référence aux routeurs reliés au segment. Le DR l'a envoyé sur les liens Broadcast.
   - **Type 3 :** Résumé de route envoyée dans une autre Area par l'ABR – Area Border Router.

— **Type 4 :**Présentation de l'ASBR - Autonomous System Border Router. Produit par l'ASBR et distribué dans les autres régions. Facilite la diffusion du routeur ID dans d'autres régions.

— **Type 5 :** Routes redistribuées par l'ASBR (routes externes, RIP, EIGRP, etc...).

5. **Link-State Acknowledgment (LSAck) :** Demandes de réception des DBD, LSR, LSA, LSU provenant des voisins.

2.2.1.6 Zones OSPF :

L'une des principales caractéristiques d'OSPF est sa capacité à supporter des réseaux interconnectés très vastes en regroupant les routeurs dans des entités logiques appelées areas ou zones.
La communication entre zones ne permet que des échanges d'informations minimales de routage dans le but de connecter les zones entre elles. Cela peut être réalisé de deux manières différentes :

— **OSPF à zone unique :** Chaque routeur se trouve dans une seule zone appelée zone fédératrice (zone 0). .

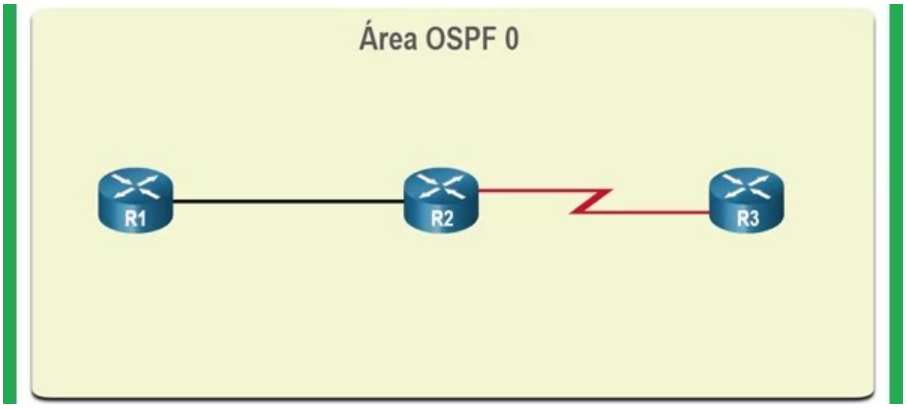

FIGURE 2.2 – Topologie OSPF à zone unique[33].

— **OSPF multizone :**Le protocole OSPF est appliqué en utilisant différentes zones et hiérarchiques. La connexion de toutes les zones de la Figure 1.3 : Topologie OSPF multizones à la zone de réseau fédérateur (zone 0) est nécessaire. Les routeurs qui relient les zones sont désignés sous le nom de routeurs ABR (Router Area Border).

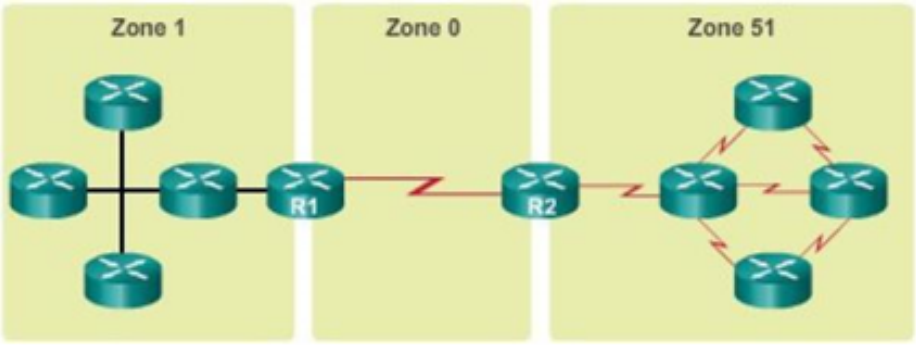

FIGURE 2.3 – Topologie OSPF multizones[33].

Voici une comparaison entre le protocole OSPF à zone unique et OSPF multizones :

TABLE 2.2 – Comparaison entre OSPF à zone unique et à multizones

OSPF à zone unique	OSPF multizones
Taille excessive de la table de routage de grande taille	Réduction de la taille de table de routage
Taille excessive de la base de données d'états de liens	Réduction de la surcharge liée aux mises à d'états de liens
Fréquence élevée des calculs de l'algorithme SPF	Réduction de la fréquence des calculs SPF

2.2.1.7 Avantages et les inconvénients du protocole OSPF

Avantages du protocole OSPF[32] :

1. OSPF a été élaboré dans le but de gérer de vastes réseaux : Il n'y a pas de limite de taille du réseau et il est possible de diviser le domaine de routage afin de faciliter sa gestion.
2. OSPF utilise peu de trafic : Quand la topologie reste inchangée, les petits messages "hello" sont utilisés pour vérifier la connectivité.
3. OSPF gère l'équilibrage du trafic entre les routes de même coût.
4. OSPF offre différents critères : À titre d'exemple, la gestion de la qualité de service (QoS) englobe le délai.
5. OSPF peut collaborer avec les EGP : On peut "étiqueter" les routes OSPF, par exemple en utilisant le numéro de l'AS de destination de la route.

Inconvénients du protocole OSPF :[32]

1. OSPF peut être complexe :Il offre de multiples possibilités, améliorations qui complètent le processus de type "link state".

2. OSPF peut nécessiter beaucoup de calcul et de mémoire.
3. Il n'est pas toujours optimal de faire le routage entre deux aires de routage au sein d'un domaine de routage.

2.2.2 Protocole IS-IS

2.2.2.1 Présentation du protocole IS-IS

Leprotocole IS-IS fait l'objet d'une spécification détaillée dans la norme ISO/IEC 10589 [16]. Il définit un protocole de routage de type intra-domaine pour les réseaux de type CLNP dont les principes sont décrits dans les normes ISO/IEC 8473[34].En adaptant son fonctionnement au protocole IP, il devient un IGP de type Link State similaire au protocole OSPF.

- **Modèle CLNS**
  Selon le modèle CLNS ISO/ IEC 8473, il existe deux catégories d'éléments de réseau :
  les End Systems (ES), qui peuvent émettre ou recevoir des données. Cependant, ils ne peuvent pas les gérer. On les désigne sous le nom de **systèmes terminaux ;**
  les Intermediate Systems (IS), qui ont la capacité d'émettre, recevoir et gérer des données. On les nomme **routeurs.**
  La transmission de datagrammes CLNP à l'intérieur d'un domaine CLNS s'appuie finalement sur la combinaison des deux protocoles suivants :
  — Le protocole ES-IS, défini dans ISO 9542[35][36], offre la possibilité aux éléments ES et IS proches de se rencontrer ;
  — Le protocole IS-IS, défini dans ISO 10589 [37], permet d'échanger des informations de routage entre les IS. La structure à deux niveaux de son modèle permet de diviser un domaine de routage en plusieurs zones afin de diminuer la taille du graphe stocké dans chaque système d'information.

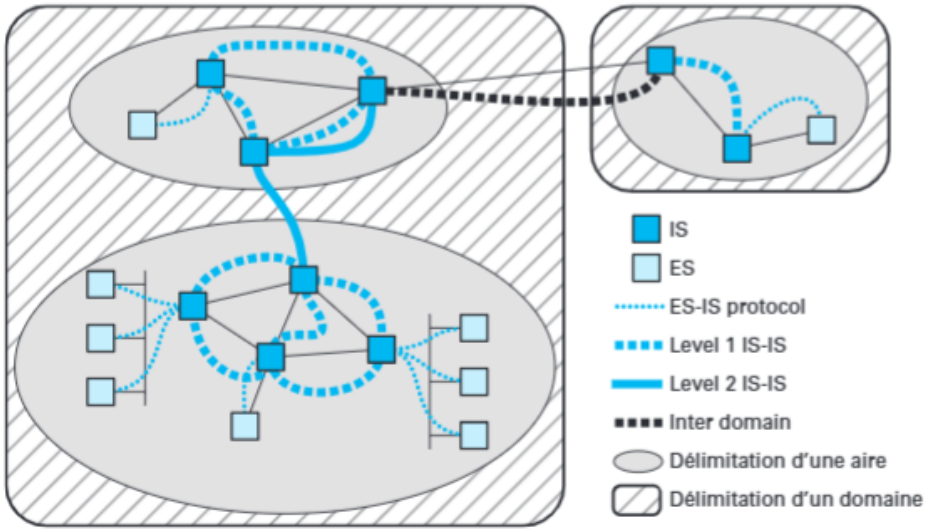

FIGURE 2.4 – Modèle de routage CLNS[38].

2.2.2.2 Identification des nœuds

La NSAP (Network Service Access Point) constitue l'adresse réseau du protocole CLNP. Dans ISO/IEC 10589 [37], cette adresse, dont la longueur totale varie de 8 à 20 octets, est constituée de trois champs :

—l'Area, de taille variable, qui définit l'aire dans laquelle se situe le nœud ;

—le System ID, codé sur 6 octets, qui identifie le nœud physique de manière globale (et non pas par interface) ;

—le Selector Byte, codé sur 1 octet, qui est uniquement utilisé pour indexer les éventuels pseudoNodes. Le sélecteur est toujours positionné à 0.

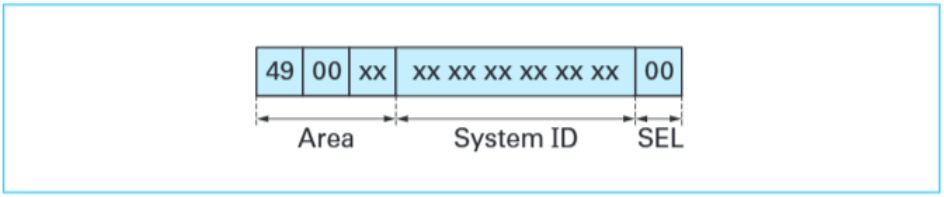

FIGURE 2.5 – Format courant d'adressage[38].

2.2.2.3 Fonctionnement du protocole IS-IS

L'apprentissage de la topologie du réseau et la mise à jour des bases de données se réalisent en plusieurs phases grâce à l'échange de différents types de messages. Ces messages sont composés d'une succession d'éléments TLV (Type, Longueur, Valeur), une structure d'encodage couramment utilisée en télécommunications[37].

a.Reconnaissance des interfaces La configuration du routeur fournit diverses informations sur les

interfaces :
Si le protocole IS-IS est activé sur une interface. Les niveaux autorisés sur cette interface (L1, L2 ou L1L2). Les métriques associées à cette interface. Le mot de passe à utiliser sur cette interface. Toutes ces informations sont stockées par interface dans la CDB, avec des informations complémentaires comme les caractéristiques de l'interface (point à point ou broadcast), son état, et les messages Hello émis. La mise à jour de cette base de données permet de mettre à jour d'autres bases de données.
b.Découverte des voisins Pour chaque interface, le routeur envoie des messages Hello pour découvrir les voisins en fonction du type d'interface (point à point ou broadcast).
c.Génération et propagation des LSP : inondationLes messages Link State PDU(LSP) décrivent les liens et lesfeuilles présents sur un nœud du réseau. Chaque nœud est res-ponsable de la génération de son propre LSP vers chacun de sesvoisins directs, mais également de la propagation des LSP qu'ilreçoit de ces mêmes voisins. La propagation des LSP de proche enproche assure la diffusion de la base à l'ensemble d'une « zone »au sens large (c'est-à-dire d'une aire L1 ou du backboneL2).

2.2.2.4 Messages IS-IS

a.Identifiant d'un LSP L'identifiant d'un LSP est une concaténation du System ID du nœud à l'origine du LSP, d'un numéro de séquence incrémenté et du numéro de fragment (si le LSP est fragmenté).
b.Synchronisation des LSDB La correspondance univoque entre l'identifiant et le contenu du LSP permet de synchroniser le contenu des LSDB à partir des messages suivants :
*Le Complete Sequence Number Paquet (CSNP) message, qui contient la liste des identifiants des LSP présents dans la LSDB du nœud à l'origine du message.
* Le Partial Sequence Number Paquet (PSNP) message, qui contient soit la liste des identifiants des LSP qui viennent d'être reçus, soit une liste de LSP dont le nœud origine ne dispose pas.
c.Portée des messages CSNP et PSNP Les messages CSNP et PSNP n'ont qu'une portée locale et ne peuvent s'adresser qu'aux voisins directs.
d.Flags pour la propagation des LSP Deux flags sont définis pour faciliter la propagation des LSP et la génération des messages SNP :
* Le flag SRM (Send Routing Message), qui indique que le LSP doit être envoyé.
* Le flag SSN (Send Sequence Number), qui indique qu'un message PSNP devra être envoyé.
e.Valorisation des flags Les flags SRM et SSN peuvent être valorisés dans différents cas, tels que :-
* Réception d'un nouveau LSP.
* Réception d'un CSNP affichant des lacunes.
* Réception d'un PSNP affichant des informations périmées.
* Réception sur une interface point à point d'un LSP nouveau.
* Réception sur une interface broadcast d'un CSNP listant des LSP nouveaux.

2.2.2.5 Quelques spécificités d'IS-IS

1. **Indication de surcharge** : L'indication de surcharge permet d'insérer un routeur dans une topologie IS-IS sans affecter le trafic de transit. Cette fonctionnalité était initialement conçue pour gérer les problèmes de saturation mémoire, mais elle est maintenant utilisée pour synchroniser IS-IS et éviter les erreurs de routage lors d'un redémarrage de routeur.
2. **Mode d'encapsulation** : Les messages IS-IS sont directement positionnés au-dessus d'une couche de niveau 2, contrairement aux protocoles de routage IP qui se situent au-dessus de la couche IP.
3. **Taille des messages Hello** : Un bourrage (padding) est systématiquement appliqué aux messages IIH pour vérifier que la MTU configurée sur le routeur est effectivement utilisable sur un lien. Si un IIH est reçu avec une taille inférieure à la MTU, le routeur ajustera sa MTU et transmettra les prochains messages IIH avec la nouvelle valeur.

2.2.2.6 Zone IS-IS

1. **Une seule aire, un seul niveau**
   Lorsque le réseau n'est pas de trop grande taille, les routeurs supportent la configuration du réseau en une seule aire. Dans cette situation, il n'y a qu'un seul niveau de routage (le niveau L2) et une seule base topologique est partagée par tous les routeurs du domaine. On peut décrire cette base de la manière suivante :
   — Chaque nœud IS est un point culminant du graphe ;
   — Chaque lien physique point à point reliant une paire de ces nœuds IS et sur lequel IS-IS est activé à chaque extrémité correspond à une arête du graphe ;
   — Les réseaux de type broadcast (on parle de pseudo-nœud) remplacent le média partagé par un nœud virtuel. Les nœuds réels connectés à cemédium sont alors reliés en étoile par ce nœud virtuel.
2. **Plusieurs aires, deux niveaux**
   Quand le réseau est de grande taille, il est fortement conseillé de le diviser en plusieurs aires, ce qui nécessite un routage à deux niveaux hiérarchiques :
   — le niveau L1, qui fournit uniquement des informations sur la topologie de l'aire locale. Il est impossible d'établir une adjacence L1 entre deux routeurs d'une même aire ;
   — le niveau L2, qui représente une topologie généralement partielle du domaine, mais qui n'est pas liée à l'aire d'appartenance de chaque routeur respectivement. Le niveau L2 garantit la continuité du routage entre les différentes aires. Une adjacence L2 se crée indépendamment entre deux routeurs d'une même zone ou d'autres zones.

2.2.2.7 Caractéristiques du protocole IS-IS

Le protocole IS-IS (Intermediate System to Intermediate Systems) est un protocole de liaison-état standardisé qui a été créé dans le but de servir de protocole de routage définitif pour le modèle OSI (Open Systems Interconnect) développé par l'ISO. IS-IS présente de nombreux points communs avec OSPF. Malgré sa conception en tant que protocole de passerelle intérieure (IGP), IS-IS est principalement employé par les fournisseurs d'accès Internet, en raison de sa capacité à évoluer. IS-IS est conforme aux éléments suivants de l'État de liaison :

— IS-IS permet une conception hiérarchique du réseau en utilisant les zones.

— IS-IS formera des relations de voisinage avec des routeurs adjacents du même type IS-IS.

— Au lieu de faire de la publicité sur la distance des réseaux connectés,l'IS-IS annonce l'état des "liens" directement connectés sous la forme de paquets Link-State. (LSPs).

— IS-IS n'enverra des mises à jour que lorsqu'il y a un changement à l'un de ses liens, et ne enverra la modification que dans la mise à jour.

— IS-IS utilise l'algorithme Dijkstra Shortest Path First pour déterminer le chemin le plus court.

— IS-IS est un protocole sans classe, et supporte donc les VLSM.

2.3 Conclusion

Ce chapitre a exploré en détail les protocoles de routage interne IS-IS et OSPF, en analysant leurs caractéristiques, leurs avantages, et leurs inconvénients. Les deux protocoles sont largement utilisés pour gérer le routage au sein des réseaux de grande taille et présentent des différences significatives en termes de conception, de performance, et de scalabilité.
Le protocole IS-IS a démontré une robustesse et une scalabilité supérieures, particulièrement adaptées aux réseaux très larges et complexes.En revanche, le protocole OSPF se distingue par sa rapidité de convergence et sa simplicité de configuration, idéal pour les réseaux de taille moyenne à grande avec des hiérarchies de routage bien définies. OSPF offre également une bonne performance en gestion des ressources et en adaptabilité aux changements de topologie.

Chapitre 3

Simulation et résultats

3.1 Introduction

L'objet de ce chapitre est de presenter et d'analyser les resultats de simulation de diverses protocoles de routage, obtenus via l'outil de simulation ensp huawei .

Le processus de préparation de l'environnement de simulation réseau implique plusieurs étapes clés pour configurer et simuler efficacement les communications réseau. Tout d'abord, il est essentiel de configurer minutieusement les routeurs en suivant des paramètres spécifiques, tout en structurant une topologie de réseau qui reflète l'environnement réel à émuler. Ensuite, l'intégration du protocole OSPF est cruciale pour établir une connectivité robuste entre les routeurs, assurant ainsi une distribution efficace des informations de routage au sein du réseau simulé.

Par la suite, la configuration du protocole MPLS joue un rôle central en optimisant la gestion du trafic réseau. En assignant des labels aux paquets de données, MPLS permet de définir des chemins prédéfinis, améliorant ainsi la qualité de service et l'efficacité du routage. De plus, la mise en place de VPN est essentielle pour garantir la confidentialité et la sécurité des communications réseau, assurant que les données transitant entre les routeurs sont protégées contre toute interception non autorisée.

Enfin, la configuration du protocole BGP complète le processus en facilitant l'échange d'informations de routage entre les différents routeurs de manière dynamique. Cela permet d'optimiser la performance du réseau en ajustant les chemins de routage en fonction des conditions du réseau et des politiques spécifiques établies. Ensemble, ces étapes assurent une émulation réseau précise et efficace, offrant ainsi une plateforme robuste pour le développement, le test et l'optimisation des infrastructures réseau complexes.

3.2 Description de la solution

Notre solution consiste à établir deux topologies identiques, nous configurons : dans la première le protocole OSPF et dans l'autre le protocole IS-IS.

Afin de choisir le meilleur protocole IGP pour les réseaux IP/MPLS, nous comparons les deux topologie par l'analyse de la latence.
La figure 3.1 illustre l'organigramme des différentes étapes à suivre pour implémenter notre solution.

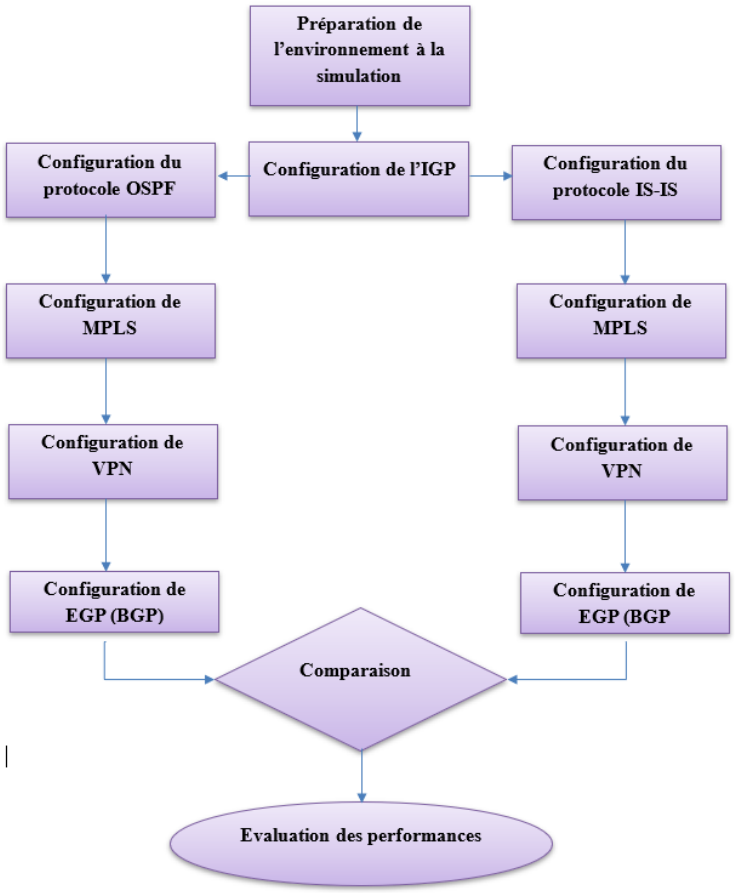

FIGURE 3.1 – Les différentes étapes de notre solution.

3.3 Outils déployés

3.3.1 Simulateur eNSP

eNSP Simulateur est un outil puissant et gratuit pour la simulation de réseaux. Il permet aux utilisateurs de :

- Concevoir et implémenter des réseaux virtuels.
- Configurer des périphériques réseau.
- Tester des scénarios réseau.

Avantages d'eNSP Simulator :

- Gratuit.
- Facile à utiliser.
- Puissant.

Utilisations d'eNSP Simulator :

- Apprendre les concepts de réseau.
- Tester de nouvelles configurations de réseau.
- Dépanner des problèmes de réseau.

3.3.2 Wireshark

Wireshark est un logiciel libre et open source d'analyse de protocoles réseau. Il permet de capturer,inspecter et analyser en temps réel les paquets de données circulant sur un réseau. Utilisé par les administrateurs réseau, les ingénieurs en sécurité et les développeurs, Wireshark aide à diagnostiquer des problèmes réseau, analyser la performance et vérifier la sécurité des communications en décomposant les paquets de données jusqu'au niveau des bits et des octets.

3.3.3 Critère d'évaluation

La latence : C'est le délai de propagation des données d'un point à un autre sur un réseau, mesuré en millisecondes. Elle comprend le temps de transmission, de traitement et de propagation. Essentielle pour la performance réseau, une faible latence est cruciale pour les applications sensibles au temps,comme la VoIP, les jeux en ligne et les transactions financières, afin d'assurer une réactivité optimale et une expérience utilisateur fluide.

$$\text{Latence} = \text{packet } (n+1) - \text{packet}(n)$$

3.4 Préparation de l'environnement de simulation

Cette section décrit la préparation de l'environnement pour simulation et les configurations initiales à effectuer sur les routeurs, en se concentrant sur les étapes suivantes :

1. Établissement de la topologie à simuler (couche physique)
2. Configuration de protocole PPP (Couche liaison de données)
3. Configuration de la couche réseau, comprenant :
   - Établissement du plan d'adressage.
   - Nomination des routeurs.
   - Attribution des adresses IP aux interfaces physiques et logiques (Loop back) des routeurs.

3.4.1 Couche physique

La topologie du réseau que nous étudions est présentée dans la figure 1. Elle est composée de dix routeurs constituant une même zone de routage.

•Les routeurs centraux : P ,P1, P3 et P4 forment le cœur de ce réseau.
•Les routeurs Edge : PE1 et PE2, représentent la périphérie de ce réseau.
•Les routeurs Customer Edge : CE1, CE2 CE3, CE4, connecte le réseau interne d'un client au réseau d'un fournisseur de services. Les interfaces utilisées sont de types Gigabit Ethernet.

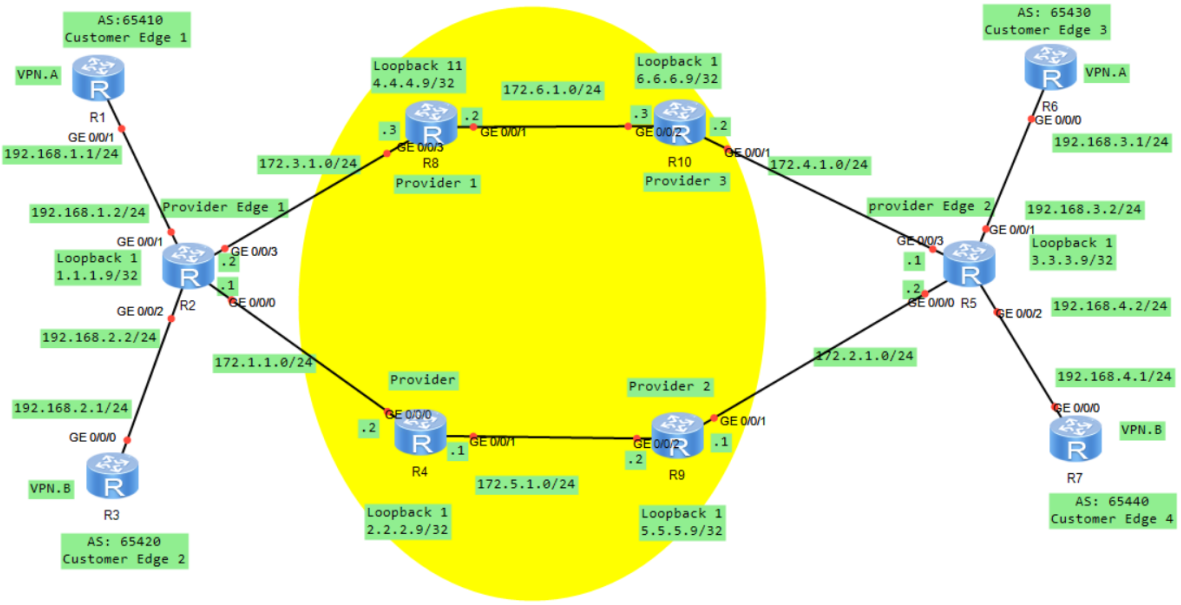

FIGURE 3.2 – Topologie pour la simulation du réseau.

3.4.2 Couche liaison de données

Le protocole exécuté au niveau de la couche liaison de données est le protocole Point-to-Point Protocol (PPP).
Le PPP est un protocole de liaison de données qui assure l'échange fiable de données sur une liaison point à point. Sa principale caractéristique est de permettre à plusieurs protocoles de transférer des données simultanément une fois que la liaison est établie et configurée. Ce protocole est largement utilisé dans l'environnement Internet.

3.4.3 Couche réseau

Plan d'adressage

La distribution des adresses IP assignées aux interfaces de chaque routeur est illustrée dans le tableau.

PE2	GE0/0/0	172.2.1.2	/24
	GE0/0/1	192.168.3.2	/24
	GE0/0/3	172.4.1.1	/24
	GE0/0/2	192.168.4.2	/24
	LO1	3.3.3.9	/32
P	GE0/0/0	172.1.1.2	/24
	GE0/0/1	172.5.1.1	/24
	LO1	2.2.2.9	/32
P1	GE0/0/3	172.3.1.3	/24
	GE0/0/1	172.6.1.2	/24
	LO1	4.4.4.9	/32
P2	GE0/0/2	172.5.1.2	/24
	GE0/0/1	172.2.1.1	/24
	LO1	5.5.5.9	/32
P3	GE0/0/2	172.6.1.3	/24
	GE0/0/1	172.4.1.2	/24
	LO1	6.6.6.9	/32
CE1	GE0/0/1	192.168.1.1	/24
CE2	GE0/0/0	192.168.2.1	/24
CE3	GE0/0/0	192.168.3.1	/24
CE4	GE0/0/0	192.168.4.1	/24

FIGURE 3.3 – La table d'adressage.

3.5 Configuration d'un routeur Provider Edge :

a. Appellation des routeurs

Les routeurs doivent être nommés afin d'organiser et de simplifier notre environnement d'émulation.La commande qui utiliser nommer un routeur est " sysname".

b. Attribution des adresses IP

Les commandes présentées dans la figure 2 sont celles exécutées sur le routeur PE2.

Il convient de noter que les mêmes configurations sont appliquées sur les autres routeurs, seules les adresses des interfaces physiques et logiques diffèrent.

Les paragraphes suivants détaillent la fonctionnalité de chaque commande.

•**"sys-view" :** est utilisée pour accéder au mode de configuration système.

•**"sysname" :** est utilisée dans ENSP pour définir le nom d'hôte du périphérique réseau.

•**"interface Gigabit Ethernet x/y " :** est utilisé pour accéder à l'interface physique.

•**"ip address " :** est utilisée pour configurer les adresses IP en spécifiant une adresse ainsi qu'un masque de sous-réseau.

•**"undo shutdown " :** permet de réactiver une interface réseau précédemment désactivée.

•**"interface Loop back 1" :** Utilisée pour activer une interface Loop back virtuelle numérotée 1 utilisée pour la gestion et diagnostic des périphériques et lui attribuer ensuite une adresse IP et masque.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sys
[Huawei]sysname PE2
[PE2]interface LoopBack 1
[PE2-LoopBack1]ip add
May 29 2024 19:43:45-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 2, the c
hange loop count is 0, and the maximum number of records is 4095.
[PE2-LoopBack1]ip address 3.3.3.9 32
[PE2-LoopBack1]q
[PE21
[PE2]interface GigabitEthernet 0/0/0
[PE2-GigabitEthernet0/0/0]ip add 172.2.1.2 24
[PE2-GigabitEthernet0/0/0]
May 29 2024 19:48:32-08:00 PE2 %%01IFNET/4/LINK_STATE(l)[0]:The line protocol IP
 on the interface GigabitEthernet0/0/0 has entered the UP state.und
May 29 2024 19:48:35-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 4, the c
hange loop count is 0, and the maximum number of records is 40
[PE2-GigabitEthernet0/0/0]undo shu
[PE2-GigabitEthernet0/0/0]undo shutdown
Info: Interface GigabitEthernet0/0/0 is not shutdown.
[PE2-GigabitEthernet0/0/0]q
[PE2]inter
[PE2]interface gi
[PE2]interface GigabitEthernet 0/0/3
[PE2-GigabitEthernet0/0/3]ip add 172.4.1.1 24
[PE2-GigabitEthernet0/0/3]
May 29 2024 19:49:27-08:00 PE2 %%01IFNET/4/LINK_STATE(l)[1]:The line protocol IP
 on the interface GigabitEthernet0/0/3 has entered the UP state.
[PE2-GigabitEthernet0/0/3]undo shu
[PE2-GigabitEthernet0/0/3]undo shutdown
May 29 2024 19:49:35-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 5, the c
hange loop count is 0, and the maximum number of records is 4095.
Info: Interface GigabitEthernet0/0/3 is not shutdown.
[PE2-GigabitEthernet0/0/3]q
[PE2]
```

FIGURE 3.4 – Attribution d'adresse IP a une interface.

3.5.1 Configuration de L'IGP

1. **Configuration de protocole OSPF**

   Cette section traite de la configuration du protocole OSPF sur les Six routeurs pour assurer leur connectivité. Tous les routeurs appartiennent à la même zone, l'area 0, car nous simulons uniquement le réseau de transport " backbone ".

   L'activation de ce protocole est effectuée à l'aide des commandes suivantes :

   •**" ospf " :** activer le protocole OSPF sur le routeur.

   •**" area 0 " :** Tous les routeurs sont configurés dans la même zone, appelée zone 0.

   •**" network " :** Cette commande permet de spécifier le réseau sur lequel OSPF est activé.

   •**"quit" :** Utilisée pour quitter le mode configuration.

```
[PE2]ospf
[PE2-ospf-1]are
May 29 2024 19:51:36-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 6, the c
hange loop count is 0, and the maximum number of records is 4095.
[PE2-ospf-1]area 0
[PE2-ospf-1-area-0.0.0.0]net
[PE2-ospf-1-area-0.0.0.0]network
May 29 2024 19:54:16-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 7, the c
hange loop count is 0, and the maximum number of records is 4095.172
[PE2-ospf-1-area-0.0.0.0]network 172.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0]net
[PE2-ospf-1-area-0.0.0.0]network 3.3.3
May 29 2024 19:55:16-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 8, the c
hange loop count is 0, and the maximum number of records is 4095..9
[PE2-ospf-1-area-0.0.0.0]network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0]
May 29 2024 19:55:26-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 9, the c
hange loop count is 0, and the maximum number of records is 4095.
[PE2-ospf-1-area-0.0.0.0]q
[PE2-ospf-1]q
[PE2]ospf
[PE2-ospf-1]area 0
[PE2-ospf-1-area-0.0.0.0]net
[PE2-ospf-1-area-0.0.0.0]network 172
May 29 2024 19:55:56-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 10, the
change loop count is 0, and the maximum number of records is 4095..4
[PE2-ospf-1-area-0.0.0.0]network 172.4.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0]
May 29 2024 19:56:16-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 11, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-ospf-1-area-0.0.0.0]net
[PE2-ospf-1-area-0.0.0.0]network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0]q
[PE2-ospf-1]q
[PE2]
```

FIGURE 3.5 – Activation du protocole OSPF.

•**"display ospf peer" :** est une commande utile pour le débogage, la vérification et la surveillance des connexions OSPF. Elle fournit des informations détaillées sur l'état des pairs OSPF, ce qui peut aider à identifier et à résoudre les problèmes de connectivité OSPF.

```
[PE2-ospf-1]display ospf peer

       OSPF Process 1 with Router ID 3.3.3.9
            Neighbors

 Area 0.0.0.0 interface 172.2.1.2(GigabitEthernet0/0/0)'s neighbors
 Router ID: 2.2.2.9          Address: 172.2.1.1
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 172.2.1.1  BDR: 172.2.1.2  MTU: 0
   Dead timer due in 33  sec
   Retrans timer interval: 5
   Neighbor is up for 00:02:25
   Authentication Sequence: [ 0 ]

            Neighbors

 Area 0.0.0.0 interface 172.4.1.1(GigabitEthernet0/0/3)'s neighbors
 Router ID: 4.4.4.9          Address: 172.4.1.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 172.4.1.2  BDR: 172.4.1.1  MTU: 0
   Dead timer due in 40  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:51
   Authentication Sequence: [ 0 ]
```

FIGURE 3.6 – Affichage les détails des relations de voisinage sur différentes interfaces.

•**"display ip routing-table" :** est utilisée pour afficher la table de routage du routeur pour

comprendre comment le trafic est acheminé sur le réseau et dépanner les problèmes de connectivité. Les résultats de cette commande montrent la table de routage du routeur, qui contient les informations suivantes :

a) **Destination/Mask :**l'adresse IP de destination et le masque de sous-réseau associé.

b) **Proto :** le protocole utilisé pour apprendre la route (ospf).

c) **Pre (pereferance) :** La préférence est une valeur numérique qui indique la préférence du routeur pour un itinéraire particulier. Plus la valeur de préférence est élevée signifie que la route est préférée.

d) **Cost (cout) :** Le coût est une mesure de la distance entre le routeur et la destination. Le coût est généralement calculé en fonction du nombre de sauts entre le routeur et la destination, un coût plus faible signifie que la route est préférée.

e) **Flags :** Les drapeaux de la route. Les drapeaux suivants sont utilisés dans cette table de routage : (D) la route est téléchargée dans la table de transfert (FIB).

f) **Nexthop :** indique l'adresse IP du prochain saut pour la route. C'est l'adresse IP du périphérique qui est utilisé pour acheminer le trafic vers la destination.

g) **Interfaces :** L'interface sur laquelle la route est reçue.

```
<PE2>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.9/32  OSPF    10   2           D   172.2.1.1       GigabitEthernet
0/0/0
                    OSPF    10   2           D   172.4.1.2       GigabitEthernet
0/0/3
        2.2.2.9/32  OSPF    10   1           D   172.2.1.1       GigabitEthernet
0/0/0
        3.3.3.9/32  Direct  0    0           D   127.0.0.1       LoopBack1
        4.4.4.9/32  OSPF    10   1           D   172.4.1.2       GigabitEthernet
0/0/3
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      172.1.1.0/24  OSPF    10   2           D   172.2.1.1       GigabitEthernet
0/0/0
      172.2.1.0/24  Direct  0    0           D   172.2.1.2       GigabitEthernet
0/0/0
      172.2.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
      172.3.1.0/24  OSPF    10   2           D   172.4.1.2       GigabitEthernet
0/0/3
      172.4.1.0/24  Direct  0    0           D   172.4.1.1       GigabitEthernet
0/0/3
      172.4.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/3

<PE2>
```

FIGURE 3.7 – Affichage de la Table de Routage IP.

2. **Configuration de l'IS-IS**

•" isis" : Cette commande permet d'accéder au mode de configuration ISIS (Intermediate System to Intermediate System) sur le routeur PE1.

•"network-entity 49.0001.0000.0000.0001.00 " : Cette commande configure l'entité de réseau ISIS sur l'interface PE1-isis-1. L'entité de réseau est un identifiant unique qui permet d'identifier le réseau ISIS.

— 49 : Indique un domaine de routage privé.

— 0001.0000.0000.0001 : Indique l'identifiant de système unique.

— 00 : Sélecteur NSEL, généralement mis à zéro.

•"is-level level-2" : Cette commande configure un routeur pour fonctionner en tant que routeur de niveau 2 dans le protocole IS-IS. Cela permet au routeur de participer au routage inter-domaine, essentiel pour une structure de réseau hiérarchique et pour assurer une connectivité et une résilience optimales dans un environnement IS-IS.

•"q" : Pour quitte le mode de configuration ISIS sur l'interface PE1-isis-1.

```
[PE1]isis
[PE1-isis-1]net
[PE1-isis-1]network-entity 49.0001.0000.0000.0001.00
[PE1-isis-1]
Jun 15 2024 17:11:47-08:00 PE1 %%01ISIS/4/START_ENABLE_ISIS(l)[6]:ISIS 1 enabled
 all ISIS modules.is
Jun 15 2024 17:11:55-08:00 PE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 7, the c
hange loop count is 0, and the maximum number of records is 4095.-level level-
[PE1-isis-1]is-level level-2
Info: IS Level Changed, Resetting ISIS...
[PE1-isis-1]
Jun 15 2024 17:12:06-08:00 PE1 %%01ISIS/4/START_DISABLE_ISIS(l)[7]:ISIS 1 disabl
ed all ISIS modules.
Jun 15 2024 17:12:06-08:00 PE1 %%01ISIS/4/START_ENABLE_ISIS(l)[8]:ISIS 1 enabled
 all ISIS modules.
[PE1-isis-1]q
```

FIGURE 3.8 – Implementation du protocole IS-IS.

•" int LoopBack 1 " : Crée une interface de bouclage virtuelle sur le routeur. Les interfaces de bouclage sont utilisées pour tester la connectivité, héberger des services ou comme adresse IP principale pour un routeur.

•" isis enable " : Active les fonctionnalités IS-IS sur l'interface de bouclage. Cela permet au routeur de participer au processus de routage IS-IS.

•"q " : Termine la configuration de l'interface de bouclage.

•"int g0/0/0" : Configure l'interface physique g0/0/0 du routeur

•"isis enable " : Active le protocole IS-IS sur l'interface physique g0/0/0.

```
[PE1]int LoopBack 1
[PE1-LoopBack1]isis en
[PE1-LoopBack1]isis enable
[PE1-LoopBack1]
Jun 15 2024 17:12:45-08:00 PE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 12, the
change loop count is 0, and the maximum number of records is 4095.
[PE1-LoopBack1]q
[PE1]int g0/0/0
[PE1-GigabitEthernet0/0/0]isis en
[PE1-GigabitEthernet0/0/0]int g0/0/3
[PE1-GigabitEthernet0/0/3]isis
Jun 15 2024 17:15:35-08:00 PE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 13, the
change loop count is 0, and the maximum number of records is 4095. em
                                    ^
Error: Unrecognized command found at '^' position.
[PE1-GigabitEthernet0/0/3]isis en
[PE1-GigabitEthernet0/0/3]
```

FIGURE 3.9 – Implementation du protocole IS-IS (2).

3.5.2 Configuration de MPLS

Cette partie concerne la configuration du MPLS sur les Six routeurs pour optimise la gestion du trafic réseau en utilisant des labels pour acheminer les données via des chemins prédéfinis, ce qui améliore la performance et l'efficacité par rapport aux adresses IP classiques.

•**"mpls lsr-id 3.3.3.9" :** On utilise pour attribuer l'identifiant unique 3.3.3.9 au routeur MPLS, ce qui est crucial pour l'identification et la gestion des échanges de labels dans le réseau MPLS.

•**"lsp-trigger all" :** On utilise pour déclencher la création de tous les chemins de commutation de labels (Label Switched Paths), garantissant ainsi que le routage MPLS est configuré pour tous les chemins possibles dans le réseau.

•**"mpls ldp" :** pour active le protocole de distribution des labels MPLS, permettant une gestion efficace des paquets réseau.

•**"interface GX/Y " :** Accédez à l'interface physique pour configurer le protocole MPLS.

•**"mpls" :** permet d'activer le MPLS.

•**"q" :** Utilisée pour quitter le mode de configuration.

```
<PE2>system-view
Enter system view, return user view with Ctrl+Z.
[PE2]mpls
[PE2]mpls lsr
[PE2]mpls lsr-id 3.3.3.9
[PE2]mpls
May 29 2024 20:12:47-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 12, the
change loop count is 0, and the maximum number of records is 4095.
Info: Mpls starting, please wait... OK!
[PE2-mpls]lsp
[PE2-mpls]lsp-trigger
May 29 2024 20:12:57-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 13, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-mpls]lsp-trigger all
[PE2-mpls]
May 29 2024 20:13:07-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 14, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-mpls]q
[PE2]mpls
[PE2-mpls]lsp
[PE2-mpls]lsp-trigger all
[PE2-mpls]q
[PE2]
[PE2]mpls ldp
[PE2-mpls-ldp]q
[PE2]
```

FIGURE 3.10 – Configuration de protocole MPLS.

```
[PE2]interface GigabitEthernet 0/0/0
[PE2-GigabitEthernet0/0/0]mpls
[PE2-GigabitEthernet0/0/0]mpls l
May 29 2024 20:16:17-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 16, the
change loop count is 0, and the maximum number of records is 4095.dp
[PE2-GigabitEthernet0/0/0]mpls ldp
[PE2-GigabitEthernet0/0/0]q
[PE2]
May 29 2024 20:16:27-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 17, the
change loop count is 0, and the maximum number of records is 4095.
[PE2]inte
[PE2]interface gi
[PE2]interface GigabitEthernet 0/0/3
[PE2-GigabitEthernet0/0/3]mpls
[PE2-GigabitEthernet0/0/3]
May 29 2024 20:16:47-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 18, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-GigabitEthernet0/0/3]mpls ldp
[PE2-GigabitEthernet0/0/3]q
[PE2]
May 29 2024 20:16:57-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 19, the
change loop count is 0, and the maximum number of records is 4095.
[PE2]q
<PE2>
```

FIGURE 3.11 – Configuration de protocole MPLS (2).

•**"display mpls ldp session " :** affiche les sessions LDP (Label Distribution Protocol) qui sont actives sur le périphérique.

a) **Ldp session (s) in public network :** Cette ligne indique que les sessions LDP sont dans le réseau public.

b) **LAM (Lable Advertisement Mode) :** indique le mode d'annonce des étiquettes LDP, "DU" signifie "Downstream Unsolicited" (Annonce non sollicitée en aval).

c) **SsnAge Unit (DDDD : HH : MM) :** indique l'âge de la session, exprimé en jours, heures et minutes.

d) **PeerID :** Identifie l'identifiant du pair (le routeur voisin) avec lequel la session est établie

e) **Status :** État de la session LDP. Ici, toutes les sessions sont "Operational", indiquant qu'elles fonctionnent correctement.

f) **KASsent/Rcv :** Nombre d'annonces de label envoyées/reçues par le routeur local.

g) **SsnRole :** la session LDP. "Active" signifie que la session est initiée par le routeur local, tandis que "Passive" signifie que la session est initiée par un routeur voisin.

```
<PE2>display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.9:0         Operational DU   Active   0000:00:02   11/11
 4.4.4.9:0         Operational DU   Passive  0000:00:00   3/3
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.

<PE2>
```

FIGURE 3.12 – Affichage des Sessions LDP MPLS.

3.5.3 Configuration de VPN

La configuration d'un VPN (Virtual private network) est essentielle pour assurer la confidentialité, la sécurité et la connectivité dans les communications réseau, que ce soit pour les entreprises ou les utilisateurs individuels.

•**"ip vpn-instance vpna " :** On utilise pour créer et configurer une instance VPN nommée "vpna", ce qui permet d'isoler et de gérer de manière spécifique le trafic VPN associé à cette instance dans un réseau MPLS.

•**"route-distinguisher 200 :1" :** Cette commande configure le routeur PE2 pour utiliser le routeur 200 :1 comme un routeur de distinction.

•**"vpn-target 111 :1 both " :** Cette commande configure le routeur PE2 pour utiliser le routeur 111 :1 comme un routeur de cible pour l'instance VPN.

•**"ip vpn-instance vpnb" :** On utilise pour créer et configurer une instance VPN nommée "vpnb", ce qui permet d'isoler et de gérer de manière spécifique le trafic VPN associé à cette instance dans un réseau MPLS.

```
[PE2]ip vpn-instance vpna
[PE2-vpn-instance-vpna]
May 29 2024 20:49:48-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 20, the
change loop count is 0, and the maximum number of records is 4095.rout
[PE2-vpn-instance-vpna]route-distinguisher 200:1
[PE2-vpn-instance-vpna-af-ipv4]
May 29 2024 20:50:18-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 21, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-vpn-instance-vpna-af-ipv4]vpn
[PE2-vpn-instance-vpna-af-ipv4]vpn-target 111:1 both
 IVT Assignment result:
Info: VPN-Target assignment is successful.
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-vpna-af-ipv4]
May 29 2024 20:50:58-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 22, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-vpn-instance-vpna-af-ipv4]q
[PE2-vpn-instance-vpna]q
[PE2]ip vpn
[PE2]ip vpn-instance vpnb
[PE2-vpn-instance-vpnb]
May 29 2024 20:51:28-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 23, the
change loop count is 0, and the maximum number of records is 4095.rout
[PE2-vpn-instance-vpnb]route-distinguisher 200;2
                                           ^
Error: Wrong parameter found at '^' position.
[PE2-vpn-instance-vpnb]route-distinguisher 200:2
[PE2-vpn-instance-vpnb-af-ipv4]
May 29 2024 20:51:58-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 24, the
change loop count is 0, and the maximum number of records is 4095.vpn
[PE2-vpn-instance-vpnb-af-ipv4]vpn-target 222:2 both
 IVT Assignment result:
Info: VPN-Target assignment is successful.
 EVT Assignment result:
Info: VPN-Target assignment is successful.
[PE2-vpn-instance-vpnb-af-ipv4]q
May 29 2024 20:52:18-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 25, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-vpn-instance-vpnb]q
[PE2]
```

FIGURE 3.13 – Configuration d'un VPN.

•**"ip binding vpn-instance vpnb" :**est utilisée pour lier une interface physique à une instance VPN spécifique, ce qui permet de diriger le trafic de cette interface à travers cette instance VPN.

```
[PE2]interface GigabitEthernet 0/0/2
[PE2-GigabitEthernet0/0/2]ip add 192.168.4.2 24
[PE2-GigabitEthernet0/0/2]
May 29 2024 20:57:47-08:00 PE2 %%01IFNET/4/LINK_STATE(l)[1]:The line protocol IP
 on the interface GigabitEthernet0/0/2 has entered the UP state.
[PE2-GigabitEthernet0/0/2]
May 29 2024 20:57:49-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 28, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-GigabitEthernet0/0/2]undo shu
[PE2-GigabitEthernet0/0/2]undo shutdown
Info: Interface GigabitEthernet0/0/2 is not shutdown.
[PE2-GigabitEthernet0/0/2]ip bin
[PE2-GigabitEthernet0/0/2]ip binding vpn
[PE2-GigabitEthernet0/0/2]ip binding vpn-instance vpnb
Info: All IPv4 related configurations on this interface are removed!
Info: All IPv6 related configurations on this interface are removed!
[PE2-GigabitEthernet0/0/2]
May 29 2024 20:58:27-08:00 PE2 %%01IFNET/4/LINK_STATE(l)[2]:The line protocol IP
 on the interface GigabitEthernet0/0/2 has entered the DOWN state.
May 29 2024 20:58:29-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 29, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-GigabitEthernet0/0/2]
[PE2-GigabitEthernet0/0/2]ip add 192.168.4.2 24
[PE2-GigabitEthernet0/0/2]
May 29 2024 20:59:24-08:00 PE2 %%01IFNET/4/LINK_STATE(l)[3]:The line protocol IP
 on the interface GigabitEthernet0/0/2 has entered the UP state.
[PE2-GigabitEthernet0/0/2]undo
May 29 2024 20:59:29-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 30, the
change loop count is 0, and the maximum number of records is 4095.shu
[PE2-GigabitEthernet0/0/2]undo shutdown
Info: Interface GigabitEthernet0/0/2 is not shutdown.
[PE2-GigabitEthernet0/0/2]q
[PE2]
```

FIGURE 3.14 – Configuration d'un VPN (2).

•**"display ip vpn-instance verbose" :** est utilisée pour afficher de manière détaillée des informations sur les instances VPN configurées sur un périphérique réseau, telles que les adresses IP, les interfaces associées, les routes VPN, les VPN cibles, etc.

```
<PE2>display ip vpn-instance ver
 Total VPN-Instances configured : 2

 VPN-Instance Name and ID : vpna, 1
  Interfaces : GigabitEthernet0/0/1
 Address family ipv4
  Create date : 2024-05-29 20:50:18-08:00
  Up time : 0 days, 00 hours, 15 minutes and 11 seconds
  Route Distinguisher : 200:1
  Export VPN Targets :  111:1
  Import VPN Targets :  111:1
  Label Policy : label per route
  The diffserv-mode Information is : uniform
  The ttl-mode Information is : pipe
  Log Interval : 5

 VPN-Instance Name and ID : vpnb, 2
  Interfaces : GigabitEthernet0/0/2
 Address family ipv4
  Create date : 2024-05-29 20:51:57-08:00
  Up time : 0 days, 00 hours, 13 minutes and 32 seconds
  Route Distinguisher : 200:2
  Export VPN Targets :  222:2
  Import VPN Targets :  222:2
  Label Policy : label per route
  The diffserv-mode Information is : uniform
  The ttl-mode Information is : pipe
  Log Interval : 5
```

FIGURE 3.15 – Affichage des Instances VPN IP.

3.5.4 Configuration de BGP (Border Gateway Protocol)

•**"bgp 100" :** permet d'activer le protocole BGP sur l'interface. Le nombre 100 correspond au numéro AS (Autonomous System) du routeur.
•**"ipv4-family vpn-instance vpna" :** crée une instance de VPN nommée "vpna" pour le protocole BGP.
•**"peer 192.168.3.1 as-number 65430" :** Cette commande ajoute un pair BGP (un autre routeur BGP) avec l'adresse IP 192.168.3.1 et le numéro AS 65430.
•**"import-route direct" :** indique que les routes apprises par BGP doivent être ajoutées directement au tableau de routage du routeur.
•**"quit" :** quitte le mode de configuration du VPN BGP.

```
<PE2>system-view
Enter system view, return user view with Ctrl+Z.
[PE2]bgp 100
[PE2-bgp]
May 29 2024 21:09:39-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 31, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp]ipv4
[PE2-bgp]ipv4-family vpn
[PE2-bgp]ipv4-family vpn-instance vpna
[PE2-bgp-vpna]
May 29 2024 21:13:19-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 32, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp-vpna]peer 192.168.3.1 as-
[PE2-bgp-vpna]peer 192.168.3.1 as-nu
[PE2-bgp-vpna]peer 192.168.3.1 as-number 65430
[PE2-bgp-vpna]impo
[PE2-bgp-vpna]import-route dire
[PE2-bgp-vpna]import-route direct
[PE2-bgp-vpna]
May 29 2024 21:14:09-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 34, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp-vpna]q
[PE2-bgp]
```

FIGURE 3.16 – Configuration de protocole BGP.

-La même configuration pour instance VPN nommée vpnb

```
[PE2-bgp]ipv4-family vpn-instance vpnb
[PE2-bgp-vpnb]peer 192
May 29 2024 13:44:02-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 35, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp-vpnb]peer 192.168.4.1 as-nu
[PE2-bgp-vpnb]peer 192.168.4.1 as-number 65440
[PE2-bgp-vpnb]impo
[PE2-bgp-vpnb]import-route dire
[PE2-bgp-vpnb]import-route direct
[PE2-bgp-vpnb]
May 29 2024 13:44:42-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 37, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp-vpnb]q
[PE2-bgp]q
[PE2]
[PE2]q
<PE2>
```

FIGURE 3.17 – Configuration de protocole BGP (2).

"display bgp vpnv4 vpn-instance peer" : utilisée pour afficher des informations détaillées sur une session BGP VPN établie entre deux routeurs virtuels. Elle permet aux administrateurs réseau de déboguer et de surveiller les sessions BGP VPN et de s'assurer qu'elles fonctionnent correctement.

```
<PE2>display bgp vpnv4 vpn-instance vpna peer

 BGP local router ID : 3.3.3.9
 Local AS number : 100

 VPN-Instance vpna, Router ID 3.3.3.9:
 Total number of peers : 1            Peers in established state : 1

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv

  192.168.3.1     4       65430        4        4     0 00:01:47 Established
   1
<PE2>
```

FIGURE 3.18 – Affichage des Pairs BGP VPNv4 pour l'Instance VPN 'VPNA'.

•**"System-view" :** pour acceder au mode de configuration globale.
•**"bgp 100" :** Cette commande configure le protocole BGP (Border Gateway Protocol) sur le routeur. Le nombre 100 représente le AS (Autonomes System) du routeur.
•**"peer 1.1.1.9 as-number 100" :** Cette commande configure un voisin BGP avec l'adresse IP 1.1.1.9. La commande as-number est utilisée pour définir le numéro AS du voisin.
•**"peer 1.1.1.9 connect–interface loopback 1 " :** Cette commande configure l'interface de connexion pour le voisin BGP 1.1.1.9 à l'interface de bouclage LoopBack 1 du routeur.
•**"ipv4-family vpn " :** Cette commande configure les routes IPv4 pour les VPN (Virtual Private Networks).
•**"peer 1.1.1.9 enable " :** Cette commande active la connexion BGP vers le voisin avec l'adresse IP 1.1.1.9, permettant ainsi l'échange de routes BGP avec ce voisin.

```
<PE2>system-view
Enter system view, return user view with Ctrl+Z.
[PE2]bgp 100
[PE2-bgp]peer 1.1.1.9 as-num
[PE2-bgp]peer 1.1.1.9 as-number 100
[PE2-bgp]
May 29 2024 13:49:32-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 38, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp]peer 1.1.1.9 conn
[PE2-bgp]peer 1.1.1.9 connect-interface lo
[PE2-bgp]peer 1.1.1.9 connect-interface LoopBack 1
[PE2-bgp]
May 29 2024 13:50:02-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 39, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp]ipv4
[PE2-bgp]ipv4-family vpn
[PE2-bgp]ipv4-family vpn
May 29 2024 13:50:32-08:00 PE2 %%01BGP/3/STATE_CHG_UPDOWN(l)[5]:The status of th
e peer 1.1.1.9 changed from OPENCONFIRM to ESTABLISHED. (InstanceName=Public, St
ateChangeReason=Up) v4
[PE2-bgp]ipv4-family vpnv4
[PE2-bgp-af-vpnv4]
May 29 2024 13:50:52-08:00 PE2 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 40, the
change loop count is 0, and the maximum number of records is 4095.
[PE2-bgp-af-vpnv4]peer 1.1.1.9 ena
[PE2-bgp-af-vpnv4]peer 1.1.1.9 enable
```

FIGURE 3.19 – Configuration BGP sur un routeur avec un voisin IPv4 et activation d'une connexion VPN.

•**"display bgp vpnv4 all peer " :** est utilisée dans eNSP pour afficher l'état de tous les pairs BGP configurés pour le VPNv4.

a) **BGP local router ID :** L'identifiant du routeur local BGP.

b) **Local AS number :** Le numéro AS du routeur local BGP.

c) **Total number of peers :** Le nombre total de pairs BGP configurés.

d) **Peers in established state :** Le nombre de pairs BGP dans l'état établi.

e) **Peer fRcv :** L'adresse IP du pair BGP distant.

f) **V :** Le nombre de messages reçus du pair distant.

g) **AS :** Le numéro AS du pair distant.

h) **MsgRcvd :** Le nombre de messages reçus du pair distant.

i) **MsgSent :** Le nombre de messages envoyés au pair distant.

j) **OutQ :** Le nombre de messages en file d'attente pour être envoyés au pair distant.

k) **Up/Down :** Le temps écoulé depuis que le pair BGP est établi.

l) **State :** L'état du pair BGP.

```
<PE2>display bgp vpnv4 all peer

 BGP local router ID : 3.3.3.9
 Local AS number : 100
 Total number of peers : 3            Peers in established state : 2

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv

  1.1.1.9         4         100        4        4     0 00:00:28 Established
   2

  Peer of IPv4-family for vpn instance :

 VPN-Instance vpna, Router ID 3.3.3.9:
  192.168.3.1     4       65430       11       12     0 00:08:31 Established
   1

 VPN-Instance vpnb, Router ID 3.3.3.9:
  192.168.4.1     4       65440        0        0     0 00:07:37     Connect
   0
<PE2>
```

FIGURE 3.20 – Affichage de Tous les Pairs BGP VPNv4.

3.6 Configuration d'un routeur Provider

La figure ci-dessous représente la même configuration pour P2,P3 et P4.
On en mode de vue système et nous avons configuré le nom d'hôte de l'appareil comme "P1", on a également configuré l'adresse IP de l'appareil à 4.4.4.9.

```
[Huawei]sys
[Huawei]sysname
[Huawei]sysname P1
[P1]
May 29 2024 12:44:14-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 1, the ch
ange loop count is 0, and the maximum number of records is 4095.
[P1]INter
[P1]interface lo
[P1]interface Logic-Channel
[P1]interface LoopBack 1
[P1-LoopBack1]ip
May 29 2024 12:44:34-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 2, the ch
ange loop count is 0, and the maximum number of records is 4095.a
[P1-LoopBack1]ip address 4.4.4.9 32
[P1-LoopBack1]q
```

FIGURE 3.21 – Configuration des interfaces d'un Provider.

La capture ci-dessous montre les commandes configurent les interfaces Gigabit Ethernet 0/0/3 et 0/0/1. Les commandes incluent l'ajout d'une adresse IP, la vérification de l'état du lien et la mise en place ou la désactivation de l'arrêt.

```
[P1]interface GigabitEthernet 0/0/3
[P1-GigabitEthernet0/0/3]ip add 172.3.1.3 24
[P1-GigabitEthernet0/0/3]
Jun 12 2024 13:53:43-08:00 P1 %%01IFNET/4/LINK_STATE(l)[2]:The line protocol IP
on the interface GigabitEthernet0/0/3 has entered the UP state.undo
[P1-GigabitEthernet0/0/3]undo shu
[P1-GigabitEthernet0/0/3]undo shutdown
Info: Interface GigabitEthernet0/0/3 is not shutdown.
[P1-GigabitEthernet0/0/3]
Jun 12 2024 13:53:50-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 4, the ch
ange loop count is 0, and the maximum number of records is 4095.
[P1-GigabitEthernet0/0/3]q
[P1]inter
[P1]interface gi
[P1]interface GigabitEthernet 0/0/1
[P1-GigabitEthernet0/0/1]ip add 172.6.1.2 24
[P1-GigabitEthernet0/0/1]
Jun 12 2024 13:54:14-08:00 P1 %%01IFNET/4/LINK_STATE(l)[3]:The line protocol IP
on the interface GigabitEthernet0/0/1 has entered the UP state.
[P1-GigabitEthernet0/0/1]undo shu
Jun 12 2024 13:54:20-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 5, the ch
ange loop count is 0, and the maximum number of records is 4095.
[P1-GigabitEthernet0/0/1]undo shutdown
Info: Interface GigabitEthernet0/0/1 is not shutdown.
[P1-GigabitEthernet0/0/1]q
```

FIGURE 3.22 – Configuration des interfaces d'un provider(2).

Cette capture affiche les informations de configuration OSPF d'un routeur, incluant les modifications récentes de configuration et les détails sur la base de données OSPF.

```
[P1]ospf
[P1-ospf-1]area 0
[P1-ospf-1-area-0.0.0.0]net
[P1-ospf-1-area-0.0.0.0]network 172.6.1
Jun 12 2024 13:54:50-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 7, the ch
ange loop count is 0, and the maximum number of records is 4095..0
[P1-ospf-1-area-0.0.0.0]network 172.6.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0]net
[P1-ospf-1-area-0.0.0.0]network
Jun 12 2024 13:55:00-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 8, the ch
ange loop count is 0, and the maximum number of records is 4095.172
[P1-ospf-1-area-0.0.0.0]network 172.3.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0]net
[P1-ospf-1-area-0.0.0.0]network 4.4.4.9 0.0.0.0
Jun 12 2024 13:55:20-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 9, the ch
ange loop count is 0, and the maximum number of records is 4095.
[P1-ospf-1-area-0.0.0.0]qq
                        ^
Error: Unrecognized command found at '^' position.
[P1-ospf-1-area-0.0.0.0]q
[P1-ospf-1]q
```

FIGURE 3.23 – Configuration du protocole OSPF d'un provider.

Cette capture montre la configuration de protocole MPLS, avec des changements de configuration enregistrés et des commandes standard pour la mise en place d'un réseau MPLS avec des LSR et des LDP.

```
[P1]mpls lsr-id 4.4.4.9
[P1]mpls
Jun 12 2024 13:55:50-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 11, the c
hange loop count is 0, and the maximum number of records is 4095.
Info: Mpls starting, please wait... OK!
[P1-mpls]lsr
[P1-mpls]l
Jun 12 2024 13:56:00-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 12, the c
hange loop count is 0, and the maximum number of records is 4095.
[P1-mpls]lsp-trigger all
[P1-mpls]
Jun 12 2024 13:56:10-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 13, the c
hange loop count is 0, and the maximum number of records is 4095.q
[P1]mpls ldp
[P1-mpls-ldp]q
[P1]
Jun 12 2024 13:56:30-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 14, the c
hange loop count is 0, and the maximum number of records is 4095.
[P1]inter
[P1]interface gi
[P1]interface GigabitEthernet 0/0/3
[P1-GigabitEthernet0/0/3]mpls
[P1-GigabitEthernet0/0/3]mpls ldp
[P1-GigabitEthernet0/0/3]q
[P1]inte
Jun 12 2024 13:57:00-08:00 P1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 16, the c
hange loop count is 0, and the maximum number of records is 4095.r
[P1]interface gi
[P1]interface GigabitEthernet 0/0/1
[P1-GigabitEthernet0/0/1]mpls
[P1-GigabitEthernet0/0/1]mpls ldp
[P1-GigabitEthernet0/0/1]q
```

FIGURE 3.24 – Configuration de protocole MPLS dans un provider.

3.7 Configuration d'un Routeur customer edge

La même configuration pour les autres routeurs R3, R6, R7.
La capture ci-doussous montre la configuration de l'interface Gigabit Ethernet 0/0/1 d'un routeur Huwei pour une adresse IP statique de 192.168.1.1 avec un masque de sous-réseau de 24, en utilisant les commandes de configuration système pour définir le nom de système (sysname CE1), configurer l'interface Gigabit Ethernet 0/0/1 avec l'adresse IP et le masque de sous-réseau, puis annuler le shutdown de l'interface pour la rendre opérationnelle. La capture d'écran montre des configurations BGP classiques utilisées pour établir des connexions BGP avec des voisins et échanger des informations de routage.
•**"bgp 65410 " :** cette commande configure le protocole BGP sur le routeur avec l'AS number 65410.

```
<Huawei>sys
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sys
[Huawei]sysname CE1
[CE1]
May 29 2024 13:28:42-08:00 CE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 1, the c
hange loop count is 0, and the maximum number of records is 4095.
[CE1]inter
[CE1]interface gig
[CE1]interface GigabitEthernet 0/0/1
[CE1-GigabitEthernet0/0/1]ip add 192.168.1.1 24
[CE1-GigabitEthernet0/0/1]
May 29 2024 13:29:51-08:00 CE1 %%01IFNET/4/LINK_STATE(l)[0]:The line protocol IP
 on the interface GigabitEthernet0/0/1 has entered the UP state.
May 29 2024 13:29:53-08:00 CE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 2, the c
hange loop count is 0, and the maximum number of records is 4095.
[CE1-GigabitEthernet0/0/1]undo shu
[CE1-GigabitEthernet0/0/1]undo shutdown
Info: Interface GigabitEthernet0/0/1 is not shutdown.
[CE1-GigabitEthernet0/0/1]q
```

FIGURE 3.25 – Configuration des interfaces d'un customer edge.

•**" peer 192.168.1.2 as-number 100" :** cette commande configure un voisin BGP avec l'adresse IP 192.168.1.2. Le paramètre "as-number" permet de spécifier l'AS number du voisin.
•**"import-route direct" :** commande configurent la façon dont le routeur doit importer les routes des voisins BGP.

```
[CE1]bgp 65410
[CE1-bgp]
May 29 2024 13:35:13-08:00 CE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 3, the c
hange loop count is 0, and the maximum number of records is 4095.
[CE1-bgp]peer 192.168.1.2 as
[CE1-bgp]peer 192.168.1.2 as-nu
[CE1-bgp]peer 192.168.1.2 as-number 100
[CE1-bgp]
May 29 2024 13:36:23-08:00 CE1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25
.191.3.1 configurations have been changed. The current change number is 4, the c
hange loop count is 0, and the maximum number of records is 4095.
[CE1-bgp]impo
[CE1-bgp]import-route dire
[CE1-bgp]import-route direct
[CE1-bgp]
```

FIGURE 3.26 – Configuration du BGP d'un customer edge.

3.8 Evaluation des performances

Dans cette partie, nous testons et comparons les performances des deux réseaux implémentant OSPF et ISIS. Les performances sont évaluées par l'analyse de la latence et le temps moyen du RTT (Round Trip Time) en fonction des itérations de ping.

3.8.1 Analyse de la latence

La latence est calculée à partir des temps de transmission des paquets du protocole ICMP, prélevés grâce à Wireshark. La figure 3.27 présente la latence en fonction du temps

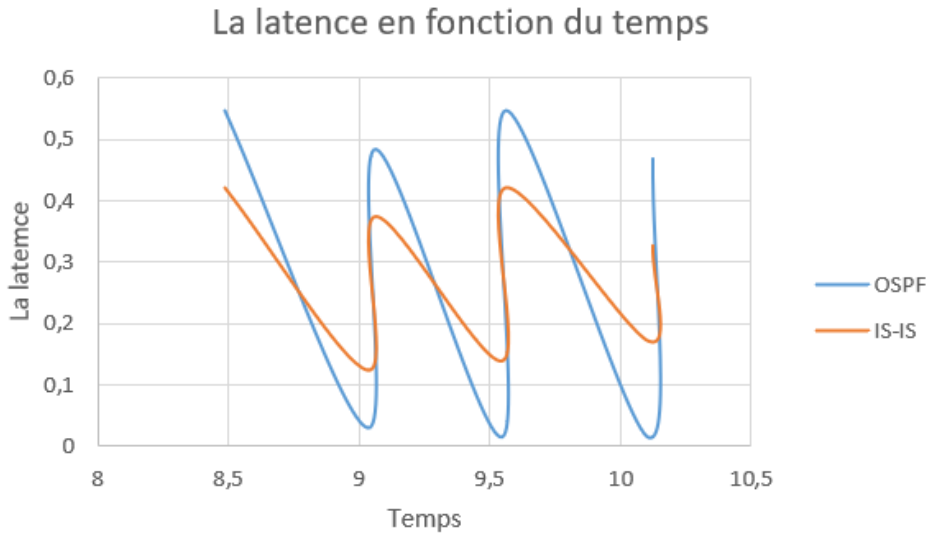

FIGURE 3.27 – Analyse de la latence en fonction du temps des deux réseaux OSPF et IS-IS.

Nous remarquons que la latence du réseau utilisant l'IS-IS comme IGP est nettement inférieur à celle d'un réseau implémentant l'OSPF.

3.8.2 Analyse de RTT moyenne

Le RTT (Round Trip Time) moyenne est prélevés pour les deux réseaux OSPF et IS-IS, en effectuant dix itérations de ping. Le RTT est une durée en millisecondes (ms) du voyage (aller-retour) d'un paquet, et est considéré comme un paramètre important permettant d'évaluer la rapidité du réseau. Cette étude est vérifiée pour deux cas : réseau sans panne et avec panne.
Les figures 3.28 et 3.29 illustrent respectivement le RTT moyen dans le cas d'un fonctionnement normal (cas sans panne) et le RTT moyen dans le cas d'une panne.

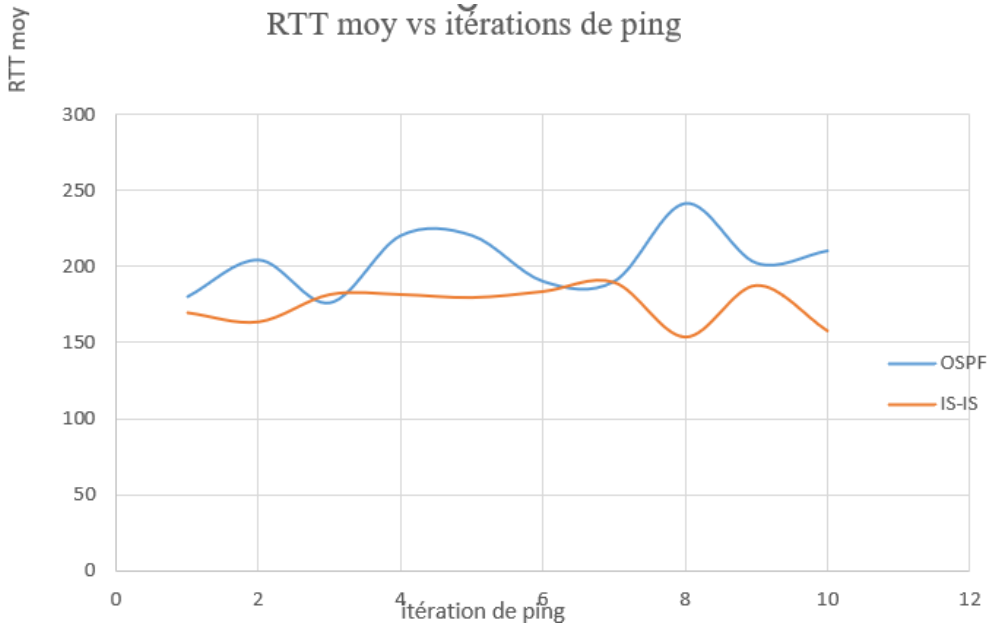

FIGURE 3.28 – RTT moy en fonction des itérations de ping des deux réseaux OSPF et IS-IS (cas sans panne).

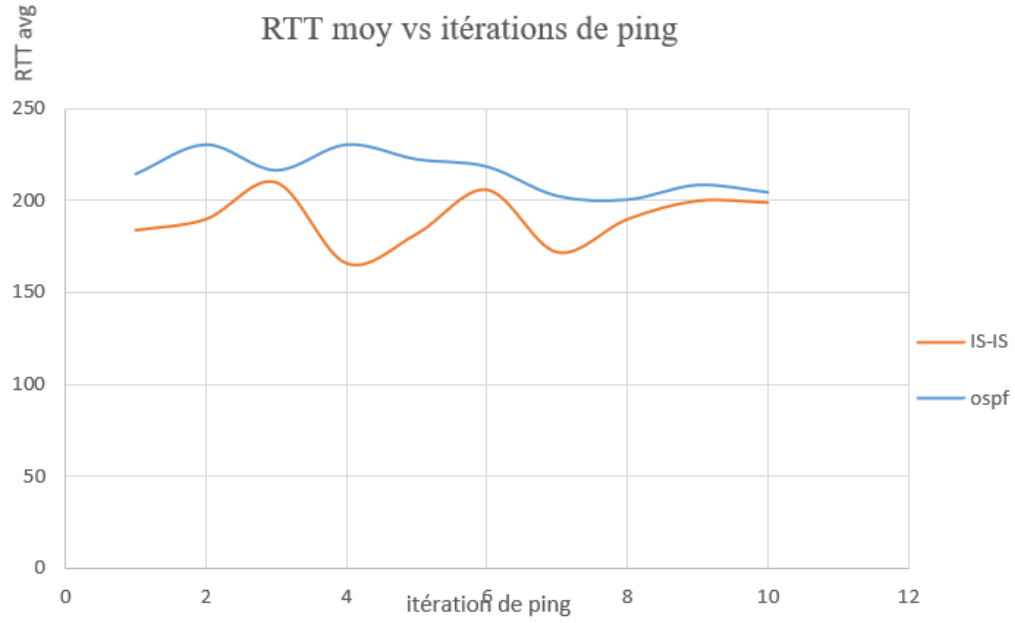

FIGURE 3.29 – RTT moy en fonction des itérations de ping des deux réseaux OSPF et IS-IS cas de panne).

En analysant les deux figures, nous remarquons, que réseau avec ISIS présente également des résultats plus intéressants que ceux d'un réseau avec OSPF.

3.9 Conclusion

Ce chapitre a présenté les simulations et les résultats obtenus pour évaluer les performances des protocoles de routage OSPF et IS-IS dans des environnements de réseaux NGN utilisant les technologies IP/MPLS. Les simulations ont été réalisées dans des scénarios variés, en tenant compte de plusieurs métriques de performance clés telles que la convergence, la latence, la gestion des ressources et la scalabilité.

Les résultats de nos simulations montrent clairement que le protocole IS-IS surpasse le protocole OSPF dans plusieurs aspects critiques. IS-IS a démontré une meilleure scalabilité, gérant plus efficacement les grands réseaux avec des topologies complexes. En termes de convergence, IS-IS a également montré une performance supérieure, s'adaptant plus rapidement aux changements de topologie et minimisant les interruptions de service.

Conclusion et perspectives

Ce mémoire a exploré en profondeur la configuration et l'optimisation des réseaux de nouvelle génération (NGN), en se concentrant sur les technologies de protocole IP/MPLS, l'intégration des VPN et la comparaison des protocoles de routage OSPF et IS-IS.

L'objectif principal était de démontrer comment ces technologies peuvent être utilisées pour créer des réseaux modernes, sécurisés, et efficaces, répondant aux exigences croissantes de la communication numérique. La première partie de notre étude a porté sur la configuration des réseaux NGN en utilisant le protocole IP/MPLS. Nous avons démontré que l'IP/MPLS permet une gestion efficace du trafic et une qualité de service (QoS) supérieure, en offrant une solution flexible et évolutive adaptée aux besoins des réseaux modernes. La mise en œuvre pratique a montré comment MPLS peut être utilisé pour optimiser la performance et la résilience du réseau.

L'intégration des réseaux privés virtuels (VPN) a été une étape cruciale pour garantir la sécurité et la segmentation du trafic dans les réseaux NGN. Les résultats de notre étude ont montré que les VPN peuvent offrir des niveaux élevés de sécurité sans compromettre les performances du réseau. L'intégration des VPN dans une architecture IP/MPLS a permis de protéger les données sensibles et d'assurer une gestion efficace des différentes unités d'organisation au sein du réseau.

La comparaison des protocoles de routage interne, OSPF et IS-IS, a révélé des différences significatives en termes de performance, de complexité de configuration, et de gestion des ressources. OSPF a montré une convergence rapide et une grande adaptabilité aux changements de topologie, ce qui le rend particulièrement efficace dans les réseaux où la hiérarchie de routage est importante.

En revanche, IS-IS a démontré une meilleure scalabilité et une performance robuste dans les environnements de routage plat, grâce à sa flexibilité dans la gestion des adresses IPv6 et des larges topologies. Sur la base des résultats obtenus, nous recommandons OSPF pour les réseaux de taille moyenne à grande avec des hiérarchies de routage claires, en raison de sa simplicité de configuration et de sa rapidité de convergence, et IS-IS pour les très grands réseaux ou ceux nécessitant une gestion avancée des adresses IPv6, en raison de sa scalabilité et de sa robustesse.

Cette thèse apporte des contributions significatives au domaine des réseaux de nouvelle génération en fournissant des recommandations pratiques pour la configuration et l'optimisation des infrastructures réseau modernes.

Les ingénieurs réseaux et les décideurs peuvent s'appuyer sur ces résultats pour choisir et configurer les technologies adaptées à leurs besoins spécifiques, assurant ainsi des réseaux plus robustes, sécurisés et performants.

• **Perspectives Futures**

Pour les travaux futurs, il serait pertinent d'explorer l'intégration de technologies émergentes telles que le SDN (Software-Defined Networking) et le NFV (Network Functions Virtualization) dans les réseaux NGN. De plus, une analyse approfondie des impacts de la sécurité et de la gestion des menaces dans ces environnements avancés offrirait des insights supplémentaires précieux pour l'optimisation et la protection des infrastructures réseau. En conclusion, cette thèse a permis de mieux comprendre les dynamiques complexes des réseaux NGN et de fournir des directives pratiques pour leur configuration et optimisation, contribuant ainsi de manière significative au domaine des technologies de l'information et des communications.

Bibliographie

[1] J. F. KUROSE, K. W. ROSS, *Computer Networking : A Top-Down Approach*, 6th, Pearson Education, **2013**.

[2] ITU-T, Recommendation Y.2001 : General Overview of NGN, ITU-T Recommendation Y.2001, International Telecommunication Union, **2006**.

[3] 3GPP, TS 23.002 : Network Architecture, Technical Specification 23.002, 3rd Generation Partnership Project, **2004**.

[4] M. Z. ELQASMI, mém. de mast., École Nationale Supérieure des Mines de Rabat, **2012**.

[5] ETSI, *TS 123 002 : Network Architecture*, European Telecommunications Standards Institute, **2005**.

[6] A. VAUCAMPS, protocole et concept de routage, `https://www.cisco.com/c/fr_fr/training-events/training-events-calendar/2010/france/paris/10-13-october-cisco-networking-academy-instructor-training-paris.html`, Conférence CISCO, **2010**.

[7] F. NOLOT, mém. de mast., Académie Cisco, Reims, **2009**.

[8] S. BELLALI, thèse de doct., Université USTHB, **2016**.

[9] GIANTSNET, Comment foctionner le Switch ?, Consulté le 1 mai 2024, **2014**.

[10] CISCO NETWORKING ACADEMY in *CCNA 2 Version 6*, Cisco Systems, **2016**, chap. 1.

[11] QKZK, Cours de Routage, Consulté le 16 Avril 2024, **2024**.

[12] F. R. TANGUEP, Conception et déploiement de la technologie MPLS dans un réseau métropolitain, Consulté le 4 mai 2024, **2013**.

[13] H. P. E. D. LP, MPLS Forwarding, Consulté le 26 avril 2024, **2017**.

[14] MAROT, Architecture du MPLS.

[15] M. MAROT, Architecture MPLS, Consulté le 28 mai 2024, **2006**.

[16] E. ROSEN, G. FEDORKOW, Y. REKHTER, D. TAPPAN, D. FARINACCI, T. LI, A. CONTA, *Request for Comments* **2001**, *3032*.

[17] J. N. MAYELE, mém. de mast., Université de Kinshasa, **2016**.

[18] C. SYSTEMS in *MPLS and Next-Generation Networks*, Cisco Press, **2005**.

[19] A. AMINE, mém. de mast., Université Paris-Est Marne-la-Vallée, **2011**.

[20] IPCISCO, MPLS Label Switching, **2024**.

[21] S. IBRAHIM, M. ELQUZWINI, *ResearchGate* **2024**.

[22] L. ANDERSSON, I. MINEI, B. THOMAS, LDP Specification, Request for Comments 5036, Internet Engineering Task Force (IETF), **2007**.

[23] In Dunod, **2004**, chap. 4.

[24] Y. KARKAB in *Les réseaux IP/MPLS*, Dunod, **2004**, chap. 4.

[25] G. PUJOLLE, *Contrôle dans les réseaux IP*, Lavoisier, Paris, **2005**.

[26] G. PUJOLLE, Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2, **2014**.

[27] Z. ZHANG, Y.-Q. ZHANG, X. CHU, B. LI, *Photonic network communications* **2004**, 213-225.

[28] ANONYMOUS, *Réseaux IP/MPLS - Principes et applications*, Introduction aux réseaux IP/MPLS, Éditions Eyrolles, **2003**, chap. 1.

[29] P. MASSOL, *Linux Magazine* **2003**.

[30] CISCO SYSTEMS, Guide de conception OSPF, **2024**.

[31] E. H. E. AMRI, OSPF IPv4 & IPv6, **2014**.

[32] CISCO NETWORKING ACADEMY, Routing and Switching Essentials, **2024**.

[33] F.-E. GOFFINET, Introduction OSPF, **2012**.

[34] ISO/IEC, Technologies de l'information – Protocole du service réseau en mode sans connexion : Fourniture du service sous-jacent sur des canaux B à commutation de circuits du RNIS, ISO/IEC 8473-5 :1997, **1997**.

[35] ISO, Systèmes de traitement de l'information – Téléinformatique – Protocole de routage d'un système d'extrémité à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion, ISO 9542 :1988, **1988**.

[36] ISO, Amendement 1 à la norme ISO 9542 d'août 1988, ISO 9542/A1 :1999, **1999**.

[37] ISO/IEC, Technologies de l'information – Communication de données et échange d'informations entre systèmes – Protocole intra-domaine de routage d'un système intermédiaire à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 8473), ISO/IEC 10589 :2002, **2002**.

[38] B. FONDEVIOLE, Protocole de routage IS-IS, **2008**.