République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie M'HAMED BOUGARA

Faculté de Génie Electrique
Domaine Sciences et Technologie
Filière : TÉLÉCOMMUNICATION
Mémoire de Master

Spécialité : RÉSEAUX

Thème

Optimisation d'un réseau cœur IP/MPLS par les techniques de TE "Trafic Engineering"

Encadré et dirigé par :

M^me^ HEDIR

M^r^ SKOUDARLI A.

Présenté par :

ADDOU Billel

SELOUANI Rostom

Promotion : Juin 2024

ملخص

تحسين شبكة القلب IP/MPLS باستخدام تقنيات الهندسة المرورية (TE) يعزز كفاءة وأداء وموثوقية الشبكة من خلال إدارة حركة المرور لتحسين استخدام الموارد، وتقليل الازدحام، وضمان جودة الخدمة (QoS). التقنيات مثل مسارات التحويل بالملصقات (LSP) وبروتوكول RSVP-TE تتيح حجز الموارد وتوزيع الحمل بشكل متوازن. تشمل الفوائد تحسين استخدام عرض النطاق الترددي، وتقليل زمن الانتقال، وزيادة الموثوقية بفضل مسارات النسخ الاحتياطي، ومرونة كبيرة للتكيف مع التغيرات في الشبكة.

Résumé

L'optimisation d'un réseau cœur IP/MPLS avec les techniques de Trafic Engineering (TE) améliore l'efficacité, la performance et la fiabilité du réseau en gérant le trafic pour optimiser l'utilisation des ressources, réduire la congestion et garantir la qualité de service (QoS). Les techniques comme les Label Switched Paths (LSP) et le protocole RSVP-TE permettent de réserver des ressources et de répartir la charge de manière équilibrée. Les avantages incluent une meilleure utilisation de la bande passante, des temps de latence réduits, une fiabilité accrue grâce aux chemins de sauvegarde et une grande flexibilité pour s'adapter aux changements du réseau.

Abstract

Optimizing an IP/MPLS core network using Traffic Engineering (TE) techniques enhances the efficiency, performance, and reliability of the network by managing traffic to optimize resource utilization, reduce congestion, and ensure Quality of Service (QoS). Techniques like Label Switched Paths (LSP) and the RSVP-TE protocol allow for resource reservation and balanced load distribution. The benefits include improved bandwidth utilization, reduced latency, increased reliability through backup paths, and significant flexibility to adapt to network changes.

Table des matières

Chapitre 3 : Implémentation d'un réseau MPLS

Liste des figures

Liste des tableaux

Liste des abréviations

AS	Autonomous System
ATM	Automated Teller Machine
BGP	Border Gateway Protocol
BGPv1	Border Gateway Protocol version 1
BGPv2	Border Gateway Protocol version 2
BGP	Border Gateway Protocol.
CE	Customer Edge
CoS	Class of Service
DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	External BGP
ER	Edge Router
FEC	Forwarding Equivalency Class
FW	Firewall
GNS3	Graphical Network Simulator
GRE	Generic Routing Encapsulation
EGP	Exterior Gateway Protocol
EVPN	Ethernet VPN
iBGP	Internal BGP
IGP	Interior Gateway Protocol
ILM	Ingress Label Manage
IP	Internet Protocol
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
IS-IS	Intermediate System to Intermediate System
LDP	Label Distribution Protocol
LER	Label Edge Router

LL	Label Link
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NE	Network Element
NGN	Next Generation Network
OSPF	Open Shortest Path First
PE	Provider Edge
PG	Policer
QOS	Quality of Service
RIP	Routing Information Protocol
RSVP	Resource Reservation Protocol
RT	Route Target
RD	Route Distinguisher
SDN	Software-Defined Networking
SG	Service Gateway
SIP	Session Initiation Protocol
SR	Segment Routing
TCP	Transmission Control Protocol
VoIP	Voice over IP

Introduction générale

Avec l'évolution de la taille des entreprises, les systèmes d'information ont connu une transformation spectaculaire, accompagnée d'une diversification des besoins en applications de transmission de données et d'une gestion devenue primordiale pour les différents services. En conséquence, on observe une convergence des réseaux de la téléphonie fixe, et mobile, des réseaux broadcastent réseaux informatique IP.

La plupart des entreprises disposent aujourd'hui de réseaux basés sur des protocoles de routage pour améliorer leur efficacité. Le protocole IP, presque universel, a été conçu pour interconnecter des réseaux hétérogènes et permettre le transport de données de bout en bout. Cependant, son caractère non connecté pose des difficultés pour l'intégration de services en temps réel, nécessitant l'introduction de nouvelles technologies réseau visant à améliorer l'acheminement des données.

Le succès d'Internet s'est traduit par une forte augmentation du trafic de données, dépassant celui de la voix. Cette augmentation du trafic et du débit des circuits physiques a mis à rude épreuve l'architecture classique des réseaux IP. L'extension des tables de routage et le traitement des segments IP limitent la capacité des routeurs traditionnels. Pour résoudre ces problèmes liés à l'accroissement de la taille des réseaux (nombre d'utilisateurs, largeur de bande passante, gestion de multiples protocoles), le MPLS (Multi-Protocol Label Switching) a été mis en place.

Le MPLS, conçu pour intégrer les avantages de l'IP et d'une technologie en mode circuit répond aux besoins de fiabilité et de disponibilité. Il permet de transporter des paquets IP en leur attribuant des étiquettes (labels) courtes et faciles à traiter. Ce protocole a connu un succès important grâce à des temps de commutation plus rapides que ceux du routage IP. Dans ce travail ou s’est intéressé à l’optimisation d’un réseau cœur IP/MPLS pour améliorer ces performées. Le MPLS-TE (MPLS Traffic Engineering) est aujourd'hui déployé par plusieurs opérateurs de réseau IP pour optimiser l'utilisation des ressources en bande passante et éliminer le problème de perte de paquets.

Le présent mémoire est structuré de la manière suivante : dans le premier chapitre, nous introduirons des généralités sur les cœurs de réseaux, en nous concentrant essentiellement sur les réseaux de nouvelle génération (NGN). Nous présenterons également le routage classique et les différents protocoles de routage utilisés. Le deuxième chapitre sera consacré au Protocol IP/MPLS, son fonctionnement, ses avantages et ses applications. Enfin, le troisième chapitre

constituera la partie pratique, décrivant les différentes étapes de l'implémentation et l’optimisation d'un réseau IP/MPLS. Le mémoire se conclura par une conclusion générale.

Chapitre 1
Généralités sur les réseaux
Cœurs

I.1 Introduction

Ce chapitre vise à présenter de manière générale les réseaux NGN (Next Generation Network), qui sont reconnus et mis en œuvre comme le cœur d'un réseau de fournisseur, en mettant l'accent sur le routage et les divers protocoles de routage utilisés dans le cœur de réseau. Nous concluons en examinant l'évolution vers le réseau MPLS (Multiprotocol label switching), considéré comme un exemple de réseau NGN.

I.2 Les réseaux NGN

Le projet NGN a démarré à la fin de la décennie 90. Les réseaux téléphoniques étaient bien établis et le matériel était récent. Les industriels devaient donc trouver de nouveaux débouchés. Pour cela, ils devaient proposer des solutions qui permettaient d'élargir l'offre au-delà des services téléphoniques, notamment des services multimédias. Les opérateurs de leur côté, enregistraient une croissance exponentielle du trafic des données. Pour répondre à ces besoins, ils ont donc établi des réseaux de transport en mode paquet, en utilisant les technologies ATM (Automated Teller Machine) ou IP (Internet protocol) [1].

I.2.1 Définition des Réseaux NGN

Le terme NGN (Next Generation Network) traduit littéralement par "Réseau de Nouvelle Génération", représente l'évolution centrale des architectures de réseaux pour la téléphonie sur IP et les services multimédia. Ces réseaux, basés sur des transmissions par paquets, permettent la convergence des services de télécommunications (voix, vidéo et données) en utilisant diverses technologies de transport à large bande avec une qualité de service déterminée. Dans ces systèmes, les fonctions de service sont dissociées des technologies de transport. Plus précisément, le NGN désigne le réseau principal d'une entreprise de télécommunications, conçu sur une infrastructure de transfert par paquets, visant à remplacer les réseaux téléphoniques commutés et autres infrastructures traditionnelles. Cette architecture centralisée permet à l'opérateur de fournir une gamme étendue de services (voix, données, contenus audiovisuels, etc.) à ses abonnés, via diverses technologies d'accès fixes et mobiles.

I.2.2 les caractéristiques des réseaux NGN

D'après l'ITU-T, un réseau NGN se caractérise par les éléments suivants [2] :

- Capacité à fournir des services de télécommunication via une infrastructure de transmission basée sur le mode paquet, permettant ainsi une gestion plus efficace des données et des ressources du réseau.
- Utilisation de différentes technologies de transport à large bande, offrant ainsi une flexibilité et une adaptabilité aux besoins évolutifs de la connectivité.
- Garantie d'un accès ouvert et non discriminatoire aux opérateurs choisis par les utilisateurs, favorisant ainsi la concurrence et l'innovation sur le marché des télécommunications.
- Support de multiples technologies d'accès, ce qui permet aux utilisateurs d'accéder au réseau via une variété de dispositifs et de méthodes de connexion.
- Intégration de la notion de mobilité généralisée, permettant aux utilisateurs de bénéficier de services de communication sans interruption lors de leurs déplacements entre différents réseaux ou zones de couverture.
- Assurant l'interopérabilité avec les réseaux basés sur des technologies plus anciennes, facilitant ainsi la transition et la coexistence harmonieuse entre les infrastructures existantes et les nouveaux environnements de réseau.
- Permettant à l'opérateur de satisfaire à ses obligations réglementaires en matière de qualité de service, de sécurité des données et de respect des normes de confidentialité et de protection des utilisateurs.

I.2.3 L'architecture des NGN

Les réseaux NGN reposent sur une architecture en couches (Fig. I.1) qui favorise l'interopérabilité et l'efficacité des communications. Les différentes couches sont citées comme suit [1,3] :

- **Couche "Accès"** : Cette couche constitue le point d'entrée des utilisateurs dans le réseau. Elle comprend une diversité de technologies et de supports de transmission, tels que les réseaux DSL, câblés, sans fil (Wi-Fi, 4G, 5G), et autres. L'objectif principal de cette couche est de fournir une connectivité fiable et haut débit aux abonnés, tout en prenant en charge divers types d'appareils et de terminaux.
- **Couche "Transport" :** Au sein de cette couche, le trafic est acheminé de manière efficace et sécurisée à travers le réseau. Elle utilise des protocoles de routage avancés pour garantir une distribution optimale des données vers leur

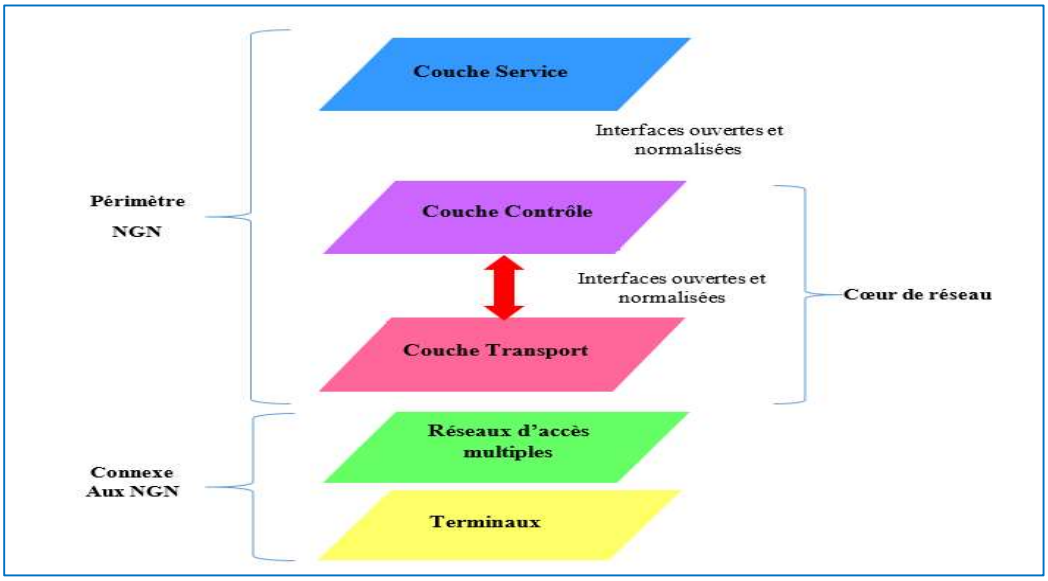

Fig. I.1 : Architecture des réseaux NGN

Destination finale. Cette couche est également responsable de la gestion des ressources de réseau et de la QoS (Qualité de Service) pour assurer une expérience utilisateur optimale.

- **Couche "Contrôle" :** Cette couche est composée de serveurs Soft-switch qui jouent un rôle central dans la gestion des appels et des sessions de communication. Les Soft-switches contrôlent les flux de trafic, établissent et terminent les connexions, et fournissent des fonctionnalités avancées telles que la signalisation SIP (Session Initiation Protocol) pour la gestion des appels VoIP (Voix sur IP) et d'autres services.
- **Couche "Services"** : Cette couche héberge les plates-formes logicielles et les applications qui fournissent une variété de services aux utilisateurs finaux. Elle comprend des éléments tels que les serveurs d'applications, les passerelles multimédias, les serveurs de messagerie, les services de voix, de données et de multimédia, ainsi que les services à valeur ajoutée tels que la messagerie unifiée, la vidéoconférence, et les services de divertissement. Cette couche est essentielle pour offrir une gamme diversifiée de services personnalisés et évolutifs aux abonnés.

Pour résumer, les réseaux NGN se caractérisent par une architecture en couches qui permet une distribution efficace des services de télécommunication, une gestion optimale du trafic et une flexibilité pour répondre aux besoins évolutifs des utilisateurs et des applications.

Chaque couche joue un rôle crucial dans la fourniture de services de haute qualité et dans l'optimisation des performances du réseau dans son ensemble.

I.3 Routage et Protocoles de Routage

I.3.1 Routage

Le routage dans le cœur de réseau est crucial pour garantir une connectivité fluide et efficace entre les différents points d'un réseau de communication. Il implique la gestion du trafic de données à travers les routeurs situés au cœur du réseau, où le trafic est dense et les débits élevés. Les protocoles de routage tels qu'OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System) et BGP (Border Gateway Protocol) sont utilisés pour échanger des informations sur les chemins disponibles et calculer les routes les plus efficaces. L'optimisation du routage dans le cœur de réseau est essentielle pour maintenir des performances élevées, assurer la fiabilité et la sécurité du réseau, et maximiser l'utilisation des ressources disponibles. Il existe deux méthodes de routage distinctes lors de la mise en place d'un protocole de routage : le routage statique et le routage dynamique.

I.3.1.1 Routage statique

Dans le cas du routage statique, les administrateurs réseau configurent manuellement les chemins de routage sur chaque routeur du réseau. Cela consiste à entrer manuellement les routes spécifiques dans la table de routage de chaque routeur, en précisant les interfaces de sortie ou les adresses IP de destination pour atteindre divers réseaux. Cette configuration est fixe et ne s'ajuste pas automatiquement en cas de modifications de la topologie du réseau. Le tableau I.1 présente les avantages et les inconvénients du routage statique [4].

I.3.1.2 Routage dynamique

Dans le cas du routage dynamique, les administrateurs réseaux mettent en place des protocoles de routage qui permettent aux routeurs de découvrir automatiquement les meilleurs chemins vers les autres réseaux. Les protocoles de routage dynamique échangent des informations sur la topologie du réseau entre les routeurs, leur permettant de s'adapter aux changements de manière automatique et réactive. Le tableau I.2 présente avantages et inconvénients du routage dynamique [5].

Table I.1 : Avantages et inconvénient du routage statique

Avantages	**Simplicité :** Le routage statique est facile à configurer et à gérer.
	Contrôle : Les administrateurs réseau ont un contrôle total sur les chemins de routage.
	Prévisibilité : Le comportement du routage est prévisible et ne dépend pas des changements de la topologie du réseau.
	Stabilité : Le routage statique est stable et ne subit pas de fluctuations de performances.
Inconvénients	**Manque de scalabilité :** Le routage statique peut devenir difficile à gérer dans les grands réseaux complexes.
	Manque d'adaptabilité : Le routage statique ne s'adapte pas automatiquement aux changements de la topologie du réseau.
	Charge administrative : La configuration et la maintenance manuelles des routes peuvent être fastidieuses et sujettes à des erreurs.
	Risque d'erreurs : Des erreurs de configuration peuvent entraîner des problèmes de connectivité et des pannes de réseau.

Table I.2 : Avantages et inconvénient du routage dynamique

Avantages	**Évolutivité :** Le routage dynamique s'adapte automatiquement aux changements de la topologie du réseau, ce qui le rend idéal pour les grands réseaux complexes.
	Adaptabilité : Le routage dynamique optimise automatiquement les chemins de routage en fonction des conditions du réseau, ce qui améliore les performances et la fiabilité.
	Automatisation : Le routage dynamique élimine la nécessité d'une configuration manuelle des routes, ce qui réduit la charge administrative et le risque d'erreurs.
	Efficacité : Le routage dynamique utilise des algorithmes intelligents pour trouver les chemins de routage les plus efficaces, ce qui optimise l'utilisation des ressources réseau.
Inconvénients	**Complexité :** Le routage dynamique peut être plus complexe à configurer et à gérer que le routage statique.
	Overhead : Les protocoles de routage dynamique peuvent générer du trafic supplémentaire sur le réseau, ce qui peut avoir un impact sur les performances.
	Convergence : Le routage dynamique peut prendre un certain temps pour converger après des changements de topologie du réseau, ce qui peut entraîner des interruptions de service temporaires.
	Sécurité : Les protocoles de routage dynamique peuvent être vulnérables aux attaques, il est donc important de mettre en place des mesures de sécurité appropriées.

Le routage dynamique est généralement utilisé dans les grands réseaux ou les environnements dynamiques où la flexibilité, l'adaptabilité et l'automatisation sont primordiales. Dans les petits réseaux ou les environnements statiques, le routage statique peut être suffisant. Dans le contexte des réseaux NGN, le routage dynamique est couramment utilisé pour :

- Découvrir et maintenir des tables de routage précises et à jour.
- Optimiser les chemins de routage pour le trafic voix, données et multimédia.
- Équilibrer la charge du trafic sur plusieurs liaisons.
- Implémenter des politiques de routage basées sur des règles.
- S'interconnecter avec d'autres réseaux et fournisseurs de services.

Le choix entre le routage statique et le routage dynamique dépend de plusieurs facteurs, tels que la taille du réseau, la complexité de la topologie, les exigences de performance et les contraintes de sécurité. En général, le routage dynamique est l'option préférable pour les réseaux NGN en raison de ses avantages en matière d'évolutivité, d'adaptabilité, d'automatisation et d'efficacité.

I.3.2 Les Protocoles de Routage

Les protocoles de routage dynamique sont classifiés selon la figure I.2. On distingue [6] :

- Classification par type de fonctionnement :
  - **Routage statique** : Les chemins de routage sont configurés manuellement par les administrateurs réseau.
  - **Routage dynamique** : Les protocoles de routage permettent aux routeurs de découvrir et de maintenir automatiquement les chemins de routage optimaux.
- Classification par niveau d'opérateur :
  - **Routage Intérieur (IGP)** : Utilisé au sein d'un même domaine d'administration autonome (AS).
  - **Routage Extérieur (EGP)** : Utilisé entre différents domaines d'administration autonomes (AS).
- Classification par algorithme de routage :
  - **Protocoles de vecteur distance** : Échangent des informations sur la distance (nombre de sauts) entre les réseaux. (ex: RIP).
  - **Protocoles d'état de liaison** : Échangent des informations détaillées sur l'état des liens adjacents. (ex: OSPF, IS-IS).

I.3.2.1 Le protocole RIP (Routing Information Protocol)

Le protocole RIP (Routing Information Protocol) est l'un des premiers protocoles de routage utilisés dans les réseaux informatiques [7].

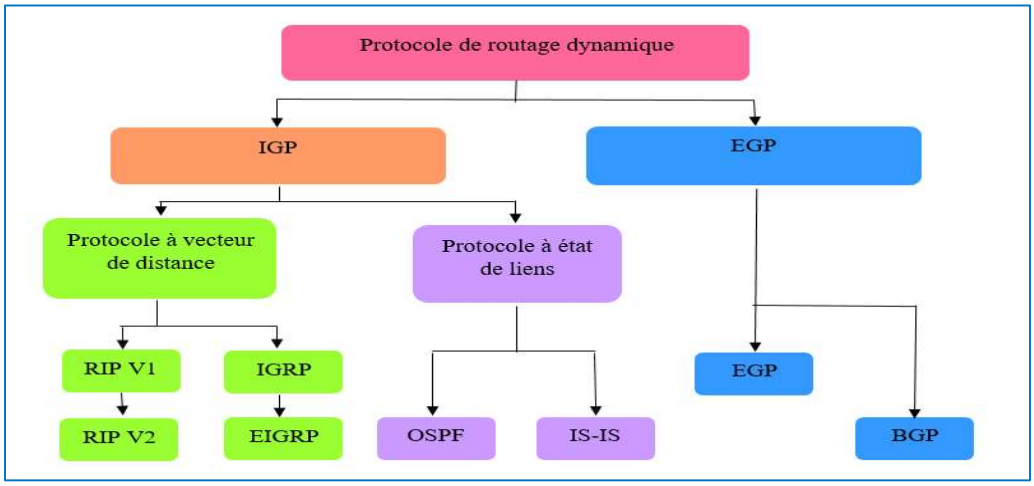

Fig. I.2 : Les protocoles de routage dynamique

Algorithme de routage à vecteur de distance : RIP utilise un algorithme de routage à vecteur de distance pour déterminer les meilleures routes vers les réseaux de destination. Chaque routeur maintient une table de routage contenant des informations sur les réseaux accessibles et le coût pour y accéder. Le coût est généralement mesuré en nombre de sauts (ou de routes traversées).

Échange périodique de mises à jour : Les routeurs RIP échangent périodiquement des mises à jour de routage pour informer les autres routeurs des réseaux auxquels ils peuvent accéder. Ces mises à jour sont diffusées sous forme de messages RIP.

Comptage des sauts : RIP utilise le nombre de sauts comme métrique pour déterminer le meilleur chemin vers une destination. Par défaut, le nombre maximal de sauts est limité à 15. Si un réseau est à plus de 15 sauts [7]. RIP considérera cette route comme inaccessible.

Limitations de RIP : Bien que RIP soit simple à configurer et à utiliser, il présente certaines limitations. Notamment, sa lenteur de convergence et son manque de scalabilité le rendent moins adapté aux réseaux de grande taille ou complexes. De plus, sa métrique basée sur le nombre de sauts peut ne pas toujours refléter le chemin optimal vers une destination.

Versions de RIP : RIP existe en plusieurs versions, notamment RIP version 1 (RIPv1) et RIP version 2 (RIPv2). RIPv2 offre des fonctionnalités supplémentaires par rapport à RIPv1, telles que la prise en charge de la transmission des masques de sous-réseau et l'authentification des mises à jour de routage.

En résumé, bien que le protocole RIP ait été largement utilisé dans le passé, il est progressivement remplacé par des protocoles de routage plus avancés et adaptés aux besoins des réseaux modernes, tels que OSPF et BGP.

I.3.2.2 Le protocole OSPF (Open Shortest Path First Protocol)

Dans le paysage complexe des réseaux informatiques, la connectivité efficace est essentielle pour garantir le bon fonctionnement des applications et des services. Le protocole OSPF joue un rôle vital en assurant une connectivité fiable, flexible et dynamique au sein des réseaux IP.

OSPF, est un protocole de routage à état de lien utilisé pour déterminer les meilleures routes vers les destinations dans un réseau IP. Contrairement aux protocoles de routage à vecteur de distance comme RIP, OSPF se base sur la topologie du réseau, en échangeant des informations sur les liens et les routes disponibles entre les routeurs.

OSPF fonctionne en échangeant des messages de routage entre les routeurs, connus sous le nom de "routeurs OSPF". Ces messages contiennent des informations sur les réseaux locaux, les coûts de liaison et les routes vers d'autres réseaux. À partir de ces informations, chaque routeur OSPF construit une base de données de topologie du réseau, appelée "base de données de liens".

En utilisant l'algorithme Dijkstra, chaque routeur utilise le protocole OSPF calcule ensuite le chemin le plus court vers toutes les destinations à partir de sa propre perspective. Cette information est utilisée pour construire la table de routage de chaque routeur, qui répertorie les meilleures routes vers toutes les destinations dans le réseau.

Caractéristiques principales :

- **Convergence rapide :** OSPF offre une convergence rapide en détectant rapidement les changements dans la topologie du réseau et en recalculant les routes en conséquence.
- **Évolutivité :** OSPF est conçu pour les réseaux de taille variable, des petites entreprises aux grands fournisseurs de services Internet, offrant une évolutivité efficace grâce à la segmentation en zones et à la hiérarchisation.
- **Flexibilité :** OSPF est hautement configurable, permettant aux administrateurs réseau de définir des politiques de routage personnalisées, de contrôler la propagation des informations de routage et de définir des priorités pour le trafic.

En conclusion, OSPF est un protocole de routage robuste et largement utilisé dans les réseaux IP, offrant une connectivité efficace et une gestion flexible de la topologie du réseau. Son architecture à état de lien, sa convergence rapide et sa capacité à s'adapter à des environnements réseau variés en font un choix certain pour les entreprises et les fournisseurs de services Internet à travers le monde [8,9].

I.3.2.3 Le Protocole BGP (Border Gateway Protocol)

Le Border Gateway Protocol (BGP) est un protocole de routage utilisé sur Internet pour échanger des informations de routage entre les systèmes autonomes (AS). C'est le protocole de routage externe principal d'Internet, responsable de la détermination des chemins de routage optimaux pour atteindre des destinations spécifiques à travers le réseau internet.

Au cœur de l'infrastructure d'Internet se trouve le protocole BGP, jouant un rôle critique dans l'acheminement du trafic entre les réseaux autonomes. Contrairement aux protocoles de routage internes qui gèrent les réseaux locaux, BGP est un protocole de routage de la couche 4

Principes de fonctionnement :

- **Échange de messages :** BGP utilise des messages pour échanger des informations de routage entre les routeurs de bordure. Ces messages incluent des mises à jour de routage, des notifications d'événements de routage et des messages de maintenance.
- **Attributs de route :** BGP utilise des attributs de route pour déterminer le chemin le plus approprié vers une destination. Ces attributs comprennent des informations telles que la longueur du préfixe, la préférence de chemin, le type de service, etc.
- **Politiques de routage :** Les opérateurs réseau utilisent les politiques de routage BGP pour contrôler le trafic entrant et sortant de leur réseau. Cela inclut la manipulation des annonces de routage, la sélection des chemins préférés et la gestion du trafic de transit.
- **Mise en œuvre de la politique :** BGP offre une grande flexibilité pour implémenter des politiques de routage personnalisées, permettant aux opérateurs de réseau de contrôler efficacement le flux de trafic à travers leur infrastructure.

Caractéristiques principales :

- **Évolutivité :** BGP est conçu pour gérer l'échelle d'Internet, avec la capacité de gérer des milliers de routes et des centaines de milliers de préfixes.

- **Stabilité :** BGP est conçu pour être stable et résilient, avec des mécanismes intégrés pour éviter les boucles de routage et minimiser les perturbations dans le réseau.
- **Sécurité :** BGP prend en charge des mécanismes de sécurité tels que l'authentification des annonces de routage pour prévenir les attaques telles que le détournement de trafic.

En résumé, le protocole BGP est un pilier fondamental d'Internet, permettant aux systèmes autonomes de coopérer pour acheminer efficacement le trafic à travers le réseau internet. Sa conception robuste, sa flexibilité et sa capacité à gérer la scalabilite d'Internet en font un élément essentiel de l'infrastructure de communication moderne. (Fig. I.3) [10].

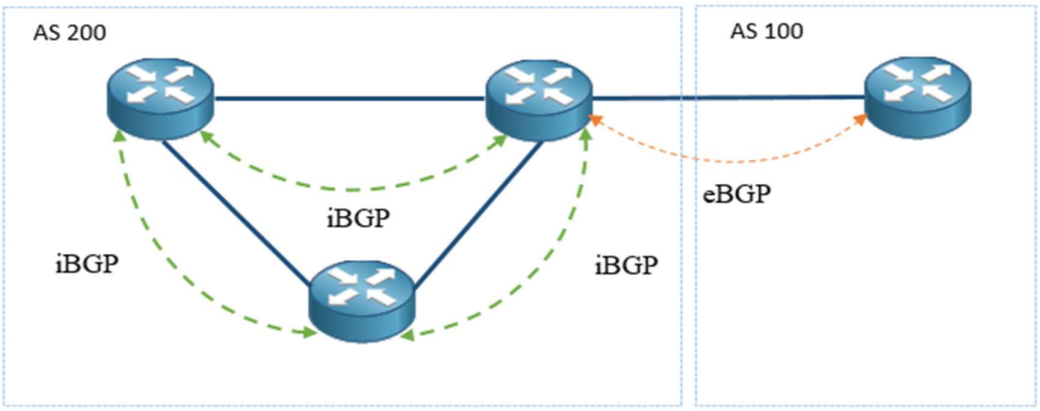

Fig. I.3 : La différence entre eBGP et IBGP

Les types de configuration BGP :

Les types de configuration BGP se réfèrent aux différentes manières dont le protocole BGP peut être configuré pour échanger des informations de routage entre les systèmes autonomes.

a) **eBGP (External BGP) :** Permet l'échange d'informations de routage entre des AS distincts.

- **Rôle :** Connecter des routeurs situés dans des AS distincts.
- **Configuration :** Généralement mis en place entre les bords de différents réseaux, comme la connexion entre le réseau client et celui de votre fournisseur d'accès Internet (FAI).
- **Exigence de connectivité :** Les routeurs eBGP doivent être directement connectés ou avoir une connectivité IP complète entre eux.

- **Configuration du numéro AS :** Lors de la configuration d'une session eBGP, vous devez spécifier le numéro AS du voisin distant avec lequel vous établissez la connexion.

b) **iBGP (Internal BGP) :** Facilite l'échange d'informations de routage au sein d'un même AS.

- **Rôle :** Échanger des informations de routage BGP à l'intérieur d'un même AS.
- **Configuration :** Généralement mis en place entre les routeurs internes d'un même réseau.
- **Exigence de connectivité :** Contrairement à eBGP, iBGP ne requiert pas une connexion directe entre les routeurs. Ils peuvent être séparés par plusieurs sauts.
- **Configuration du numéro AS :** Lors de la configuration d'une session iBGP, vous devez également spécifier le numéro AS du voisin, mais il s'agit du numéro AS local, car tous les routeurs iBGP appartiennent au même AS.

iBGP exige une connectivité IP complète entre tous les routeurs iBGP. Pour y parvenir, des configurations de routeurs supplémentaires ou des routeurs réflecteurs sont souvent utilisés pour simplifier la topologie et éviter les boucles de routage. La communication entre les routeurs BGP se fait via le protocole TCP (Transmission Control Protocol), assurant ainsi une communication fiable et ordonnée entre les pairs BGP [10].

I.4 IP/MPLS (Internet Protocol /Multiprotocol Label Switching)

IP MPLS est une technique de commutation de paquets qui combine les avantages de deux protocoles principaux : l'IP et le MPLS. Il permet de diriger le trafic de manière efficace et fiable à travers un réseau en attribuant des étiquettes (labels) à chaque paquet de données. Ces étiquettes sont utilisées pour déterminer le chemin optimal que doivent emprunter les paquets à travers le réseau, offrant ainsi des performances et une qualité de service améliorées pour les applications réseau. En résumé, IP MPLS est une technologie de commutation de paquets qui améliore l'efficacité, la fiabilité et la qualité de service des réseaux IP [12].

I.5 Conclusion

Dans ce chapitre, nous avons examiné les NGN et mis en lumière leur importance croissante, ainsi que leurs caractéristiques distinctives et leur architecture hiérarchique. Nous avons souligné que ces réseaux se distinguent les uns des autres par l'introduction de nouveaux

services innovants, une amélioration de la continuité des communications et une qualité de service améliorée. En outre, nous avons abordé le changement progressif des réseaux IP vers les réseaux IP/MPLS, où les meilleures pratiques de routage et de commutation sont intégrées pour offrir des performances optimales. Cette évolution vers les réseaux IP/MPLS permet de fusionner les fonctionnalités avancées de la commutation et du routage, ouvrant ainsi la voie à des réseaux plus flexibles, efficaces et évolutifs.

Dans le prochain chapitre, nous explorerons en profondeur la technologie MPLS, en détaillant son fonctionnement, ses avantages et ses applications spécifiques. Nous examinerons comment MPLS améliore la gestion du trafic, garantit une meilleure qualité de service et permet une plus grande souplesse dans la conception des réseaux. Enfin, nous envisagerons la façon dont nous pouvons intégrer la technologie MPLS dans la mise en œuvre de notre projet pour répondre aux besoins spécifiques de notre environnement réseau.

Chapitre 2

Protocole IP /MPLS et ses Applications

II.1 Introduction

Le Multi Protocol Label Switching (MPLS) est une technologie de réseau qui améliore l'efficacité et la rapidité de la transmission des données en utilisant des étiquettes courtes pour le routage, au lieu des longues adresses réseau traditionnelles. Ce système fonctionne en ajoutant une étiquette aux paquets de données, ce qui permet aux routeurs de diriger rapidement les paquets à travers le réseau sans consulter les informations de destination complètes à chaque étape. Les avantages du MPLS incluent une performance accrue, une grande flexibilité, une meilleure qualité de service (QoS), et une excellente scalabilité, ce qui en fait une solution idéale pour des applications variées comme les VPN (Virtual Privat Networks), la voix sur IP (VoIP), la vidéo, et l'interconnexion des centres de données. Grâce à sa capacité à gérer efficacement différents types de trafic et à garantir des niveaux de service élevés, MPLS est devenu une technologie essentielle pour les infrastructures de réseau cœur modernes.

Ce chapitre exploré en profondeur le principe et les caractéristiques de la technologie MPLS, mettant en lumière son rôle essentiel dans l'optimisation des réseaux de communication.

II.2 Caractéristiques des réseaux MPLS

Le protocole MPLS est un mécanisme de transmission dans lequel les paquets sont transmis selon leurs étiquettes (Label), il s'appuie à la fois sur le routage IP de niveau 3 (couche réseau) et les mécanismes de la commutation de niveau 2 (couche liaison) (Fig. II.1), il est d'ailleurs souvent fait référence comme appartenant à la couche 2.5 du modèle OSI [12]. Donc il fusionne l'intelligence du routage avec les performances de la commutation et procure des avantages de transport pratiquement pour tous types de trafic. Les principales caractéristiques du MPLS sont :

- **Multi Protocoles** : MPLS prend en charge différents protocoles de la couche inférieure de l'OSI, tels que Frame Relay, IPv4, IPv6, Ethernet et ATM.
- **Label Switching (Commutation par Étiquette)** : MPLS utilise une étiquette (label) pour la commutation des paquets. Cette étiquette est attribuée au paquet à son entrée dans l'infrastructure MPLS et retirée à sa sortie.
- **Position dans l'en-tête** : L'en-tête MPLS se situe entre les couches 2 (liaison) et 3 (réseau), comprenant quatre champs :
    - **Label** : Chaque label a une signification spécifique entre deux routeurs adjacents (Label Switching Routers, LSR), facilitant le flux du trafic le long

du chemin d'étiquetage (Label Switching Path, LSP). À chaque saut, le label est utilisé pour obtenir des informations de routage et déterminer les actions à effectuer sur le label (insertion, modification ou suppression).

- **Exp (Experimental Use)** : Trois bits utilisés comme champ de classe de service (CoS), permettant de traiter différemment les paquets en fonction de leur nature, même avec le même numéro de label.
- **S (bottom of stack)** : Indique le bas de la pile de labels (1 bit). Le bit "S" est à 1 lorsque le dernier label de la pile est atteint.
- **TTL (Time to Live)** : Temps pendant lequel le paquet peut exister (8 bits).

II.3 Composants de l'Architecture MPLS

Pour décrire les dispositifs constituant l'architecture MPLS, plusieurs composants spécifiques ont été définis (Fig. II.2) :

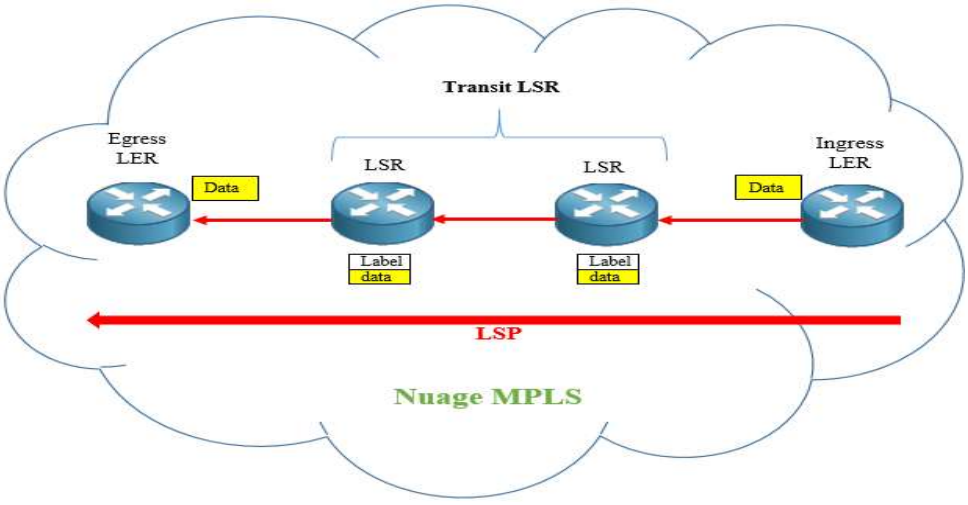

Fig. II.2 : Exemple d'un Nuage MPLS

- **Label Switching Router (LSR)** : Le routeur à commutation de label, également appelé P (Provider router), est un routeur situé au cœur du réseau MPLS. Il participe à la mise en place des chemins par lesquels les paquets sont acheminés et gère les paquets marqués dans le domaine MPLS.
- **Label Edge Router (LER) ou ELSR** : Le routeur de bordure à label, également appelé PE (Provider Edge router), sert d'interface entre un domaine MPLS et le monde extérieur. Il gère les paquets marqués à l'intérieur d'un domaine MPLS ainsi que les paquets IP à l'intérieur et à l'extérieur du domaine.

  INGRESS LER : Routeur qui gère le trafic entrant dans un réseau MPLS.

EGRESS LER : Routeur qui gère le trafic sortant d'un réseau MPLS.

II.4 Fonctionnement de base du MPLS

Le fonctionnement du MPLS repose sur trois étapes principales :

- **Étiquetage des Paquets** : Lorsqu'un paquet entre dans le réseau MPLS, le routeur spécifique LER lui attribue une étiquette (label). Cette étiquette contient des informations sur la destination du paquet et les instructions de traitement pour les routeurs suivants.
- **Commutation par Étiquette** : Les routeurs MPLS, connus sous le nom de Label LSR, utilisent les étiquettes pour acheminer les paquets à travers le réseau. Ils consultent l'étiquette du paquet pour déterminer le prochain saut et le transfèrent au routeur approprié.
- **Retrait de l'Étiquette** : Une fois le paquet arrivé à sa destination finale, un autre LER retire l'étiquette MPLS et transmet le paquet à son destinataire en utilisant le protocole de couche 3 approprié (IP, Ethernet, etc.).

II.4.1 Le fonctionnement traditionnel du routage IP

Routage classique

Dans le routage classique, le protocole IP fonctionne de manière non connectée, ce qui signifie que chaque paquet est traité individuellement et peut suivre des chemins différents. Les routeurs maintiennent des tables de routage contenant des informations sur les destinations, les ports de sortie et les prochains routeurs vers ces destinations (Fig. 2.3).

Lorsqu'un paquet est reçu, les routeurs intermédiaires déterminent le prochain relais optimal pour acheminer le paquet vers sa destination.

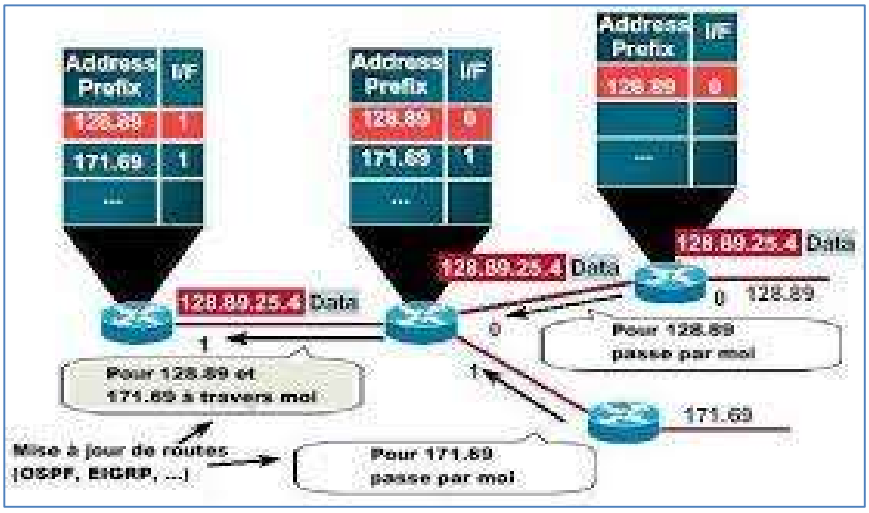

Fig. II.3 : Le Routage classique [13]

II.4.2 Mécanisme fondamental du MPLS

La permutation d'étiquettes, fondement du mécanisme de transfert du MPLS, ouvre la voie à de nouveaux paradigmes de contrôle et à de nouvelles applications. À chaque LSR (Label Switch Router) dans le réseau MPLS, cette permutation est réalisée en analysant une étiquette entrante, puis en le remplaçant par une étiquette de sortie avant de l'envoyer au prochain saut. En utilisant des étiquettes pour acheminer le trafic, le MPLS permet de réduire les délais de traitement et d'acheminement des paquets, améliorant ainsi les performances globales du réseau.

II.5 La gestion du label dans un réseau MPLS

Lorsqu'un paquet traverse un réseau MPLS, il est muni d'une étiquette (label) qui guide son chemin vers sa destination. La gestion de ces étiquettes est un processus crucial pour le bon fonctionnement du réseau MPLS. Voici les étapes clés de la gestion des labels [13] :

1) **Allocation de labels :** Pour chaque classe d'équivalence de transfert (FEC), un label unique est attribué. La FEC représente un groupe de paquets partageant la même destination et les mêmes exigences de traitement.
2) **Distribution des labels :** Les labels attribués sont ensuite distribués aux routeurs du réseau MPLS via un protocole de distribution de labels, comme LDP (Label Distribution Protocol) ou RSVP (Resource Reservation Protocol).

3) **Association des labels :** Sur chaque lien MPLS, les labels d'entrée et de sortie sont associés. Cela implique la coordination entre les routeurs adjacents pour s'assurer qu'ils utilisent les mêmes labels pour le même trafic.
4) **Propagation des informations sur les labels :** Les informations sur les labels, telles que les associations et les FEC, se propagent à travers le réseau MPLS. Cela permet à chaque routeur de connaître le chemin à suivre pour chaque paquet en fonction de son label.

En effet, la gestion des labels dans un réseau MPLS implique la création, la distribution, l'association et la propagation d'informations sur les labels. Ce processus garantit que chaque paquet est correctement acheminé vers sa destination de manière efficace et flexible (**Fig. II.4)**. On notera, aussi :

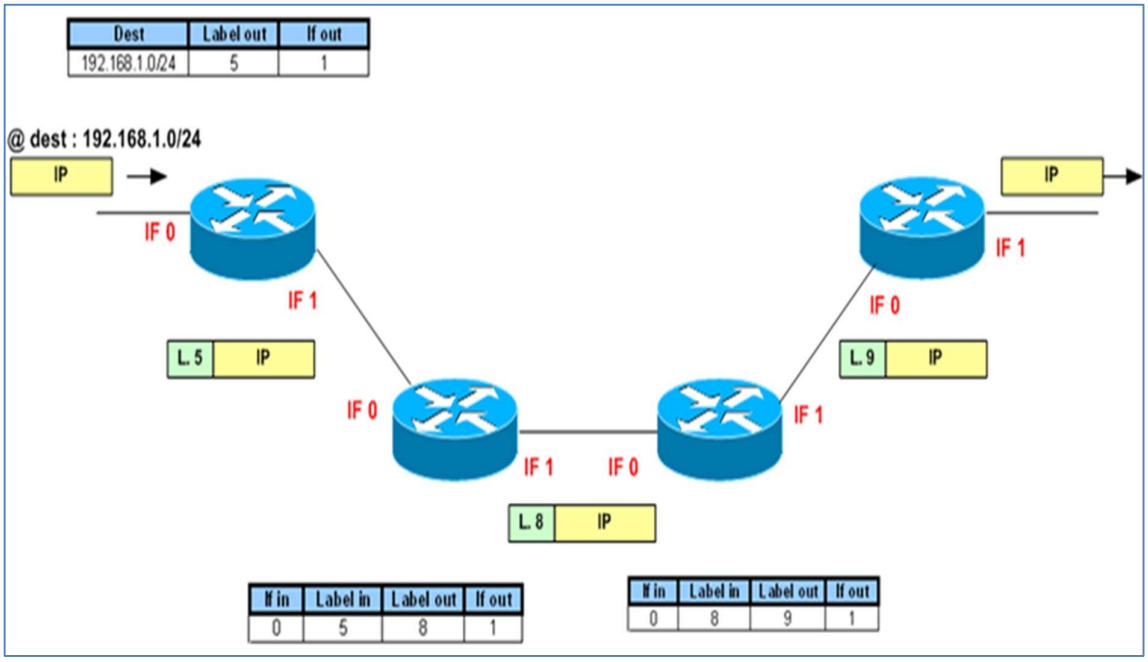

Fig. II.4 : Commutation du Label dans un nuage MPLS [14]

- Les labels MPLS ne remplacent pas les adresses IP. Ils sont utilisés comme une couche supplémentaire d'information pour optimiser le routage des paquets.
- Le protocole de routage de la couche réseau n'est pas utilisé à l'intérieur du réseau MPLS. Les décisions de commutation sont basées uniquement sur les labels.
- La gestion des labels est un processus complexe qui nécessite une coordination étroite entre les routeurs du réseau MPLS.

Le MPLS offre un large éventail d'applications qui améliorent la connectivité, la sécurité et les performances des réseaux. Dans cette section, on citera quelques-unes des applications les plus importantes du MPLS :

II.6 Protocoles implémentés dans un réseau

II.6.1 LDP (Label Distribution Protocol) : Ce protocole est essentiel pour la gestion des labels dans un réseau MPLS. Il permet aux routeurs d'échanger des informations sur les labels et d'établir des chemins de commutation d'étiquettes (LSP) qui guident le trafic à travers le réseau (Fig. II.5).

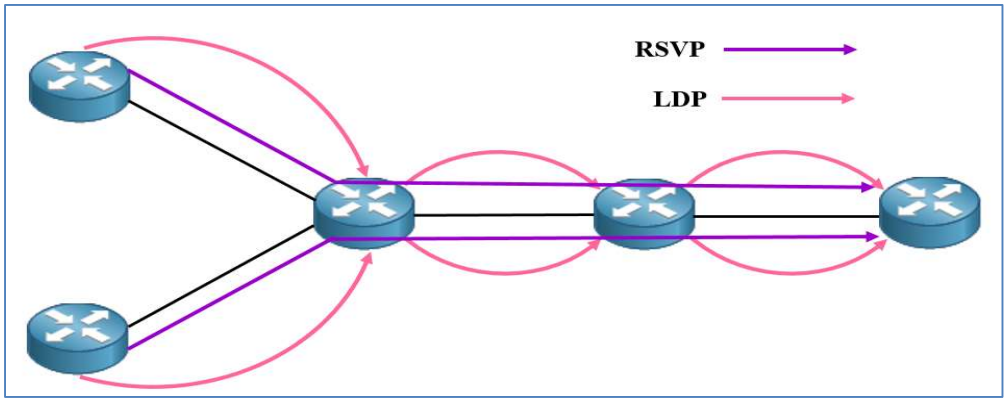

Fig. II.5 : LDP vs RSVP

II.6.2 RSVP (Resource Reservation Protocol) : Ce protocole permet de réserver des ressources réseau, telles que la bande passante, pour des applications critiques en temps réel. Il garantit que ces applications disposent de la bande passante nécessaire pour fonctionner de manière fluide et fiable (Fig. II.5).

En effet, ces protocoles garantissent une gestion efficace du trafic dans un réseau MPLS, permettant ainsi de répondre aux exigences de qualité de service et de fournir une connectivité fiable pour les applications.

II.7 Application MPLS

L'ingénierie du trafic et la qualité de service (QoS) sont deux domaines essentiels de la gestion de réseau qui visent à optimiser les performances et la fiabilité des réseaux. Et pour garantir une expérience utilisateur optimale et la performance globale du réseau. L'ingénierie du trafic fournit une structure pour la répartition efficace des ressources réseau, tandis que la

QoS assure que ces ressources sont allouées en fonction des besoins spécifiques des applications et des utilisateurs. Ensemble, ils permettent de répondre aux exigences variées des applications modernes, en assurant que les flux de données critiques bénéficient de la priorité nécessaire, tout en optimisant l'utilisation du réseau pour prévenir la congestion et maximiser les performances. La synergie entre ces deux domaines permet aux opérateurs de réseau de fournir des services fiables et performants, même dans des environnements de réseau complexes et fortement sollicités.

II.7.1 VPN MPLS : Création de réseaux privés virtuels sécurisés

Le MPLS est une technologie de choix pour la création de VPN (Virtual Private Networks). Il permet aux entreprises de connecter leurs sites distants de manière sécurisée sur une infrastructure réseau partagée, en isolant le trafic de chaque client et en garantissant la confidentialité des données (Fig. II.6).

VRF (Virtual Routing and Forwarding) : Cette technologie permet de créer plusieurs instances de tables de routage sur un même routeur, isolant ainsi le trafic entre différents clients ou services au sein du VPN MPLS (Fig. II.6).

Route Distinguisher (RD) : Le RD est un identifiant unique qui différencie les routes au sein d'une même instance de VRF, garantissant que les routes ne sont pas en conflit.

Route Target (RT) : Le RT est utilisé pour contrôler la distribution des routes entre différentes instances de VRF, permettant de cibler le trafic vers les destinations appropriées et de maintenir l'isolation du VPN.

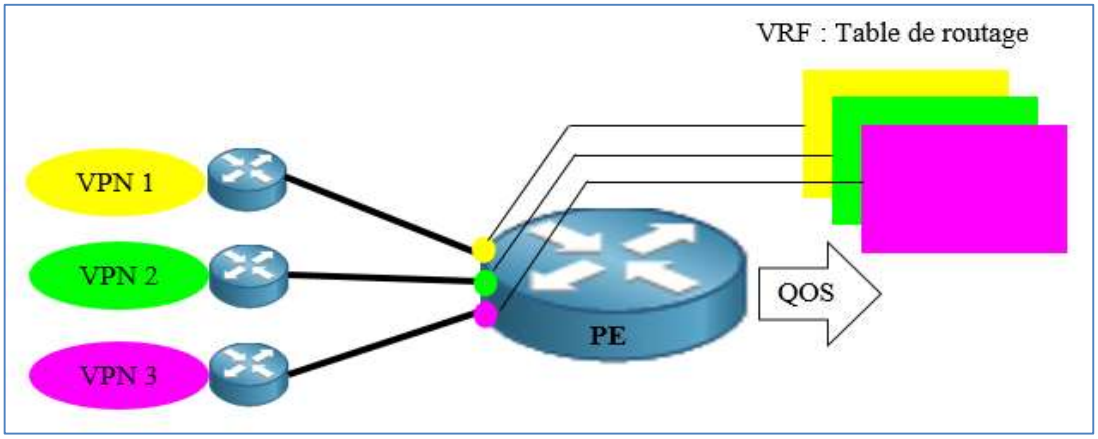

Fig. II.6 : la relation entre VPN et VRF

En effet, le MPLS offre une solution flexible et puissante pour la gestion du trafic réseau, la création de VPN sécurisés et la prise en charge d'applications critiques en temps réel. Sa capacité à combiner les avantages du routage IP et de la commutation de liaison de données le rend idéal pour les entreprises qui ont besoin d'un réseau performant, évolutif et sécurisé.

II.7.1 Ingénierie du trafic (Traffic Engineering)

L'ingénierie du trafic consiste à contrôler le flux de données à travers un réseau afin d'en optimiser les performances [15,17]. Son objectif principal est d'utiliser les ressources réseau de manière efficace pour améliorer les performances globales et éviter la congestion. Cela inclut diverses techniques telles que l'acheminement basé sur les contraintes, où les chemins des paquets sont déterminés en fonction de la capacité et de la charge des liens, et l'équilibrage de charge, qui répartit le trafic de manière uniforme sur plusieurs chemins pour éviter la surcharge de certains liens. En plus, l'ingénierie du trafic implique souvent l'utilisation de protocoles comme le MPLS pour diriger les flux de données de manière plus flexible et efficace. L'analyse continue du trafic et la capacité à ajuster dynamiquement les routes permettent de répondre rapidement aux variations de la demande et aux pannes, assurant ainsi une utilisation optimale des ressources réseau. Elle permet de :

- Réduire la congestion et les goulots d'étranglement
- Équilibrer la charge sur les différents liens et équipements du réseau
- Améliorer l'efficacité de l'utilisation de la bande passante
- Garantir des performances prévisibles pour les applications critiques

Méthodes d'ingénierie du trafic :

- **Routage basé sur les contraintes :** Choisir les chemins de routage en fonction de critères tels que la bande passante disponible, la latence et la perte de paquets.
- **Réservation de bande passante :** Allouer des ressources réseau dédiées à des flux de trafic spécifiques, comme la voix sur IP (VoIP) ou la vidéoconférence.
- **Optimisation des chemins :** Identifier les itinéraires les plus efficaces pour le trafic en fonction de divers critères.

Objectifs de l'ingénierie du trafic :

- Minimiser la latence (délai entre l'envoi et la réception d'un paquet)
- Réduire la perte de paquets (paquets perdus pendant la transmission)

- Optimiser l'utilisation de la bande passante
- Améliorer la disponibilité du réseau
- Garantir une expérience utilisateur fluide et fiable

Techniques et Protocoles Utilisés :

- **OSPF-TE (Open Shortest Path First - Traffic Engineering)** : Une extension du protocole OSPF standard, OSPF-TE incorpore des informations sur les liens tels que la bande passante et la latence dans son algorithme de routage, permettant une sélection de chemin basée sur des contraintes spécifiques.
- **RSVP-TE (Resource Reservation Protocol - Traffic Engineering)** : RSVP-TE est utilisé pour réserver explicitement des ressources réseau le long d'un chemin de routage, garantissant que les besoins en bande passante et autres critères de QoS sont satisfaits avant l'établissement de la connexion.

Applications de l'ingénierie du trafic :

- Réseaux des fournisseurs de services Internet (ISP)
- Réseaux d'entreprise
- Réseaux de centres de données
- Réseaux WAN (Wide Area Network)

II.7.2 Qualité de service (QoS)

La QoS vise à garantir un niveau de performance spécifique pour certains types de trafic, tels que la voix, la vidéo ou les applications critiques pour l'entreprise [16]. Et reçoivent le traitement nécessaire pour fonctionner correctement sans interruption. Les techniques de QoS incluent la classification et le marquage des paquets, où les paquets de données sont identifiés et étiquetés selon leur importance, ainsi que la mise en file d'attente et la planification, qui déterminent l'ordre de traitement des paquets en fonction de leurs priorités. La QoS utilise également des mécanismes de gestion de la bande passante pour allouer des parts spécifiques de la capacité du réseau aux différentes classes de service, garantissant ainsi que les applications prioritaires disposent toujours des ressources nécessaires. La gestion de la gigue, de la latence et de la perte de paquets est cruciale pour maintenir la qualité des services sensibles au délai, comme la VoIP et la vidéo en temps réel.

Elle permet de :

- Prioriser le trafic en fonction de son importance
- Limiter la bande passante consommée par certains types de trafic
- Gérer les files d'attente de paquets pour éviter la congestion
- Assurer la fiabilité et la disponibilité des services

Mécanismes de QoS :

- **Priorisation du trafic :** Attribuer des priorités aux différents types de trafic pour garantir un traitement préférentiel aux applications critiques.
- **Limitation du débit :** Contrôler la quantité de bande passante qu'un flux de trafic peut utiliser pour éviter de surcharger le réseau.
- **Gestion de la file d'attente :** Utiliser des files d'attente et des algorithmes de gestion pour garantir un traitement équitable du trafic et éviter la saturation des ressources.

Objectifs de la QoS :

- Garantir des niveaux de performance prévisibles pour les applications critiques
- Minimiser la latence et la gigue (variation de la latence)
- Assurer la fiabilité et la disponibilité des services
- Améliorer l'expérience utilisateur pour les applications sensibles à la performance

Applications de la QoS :

- Voix sur IP (VoIP)
- Vidéoconférence
- Streaming vidéo
- Jeux en ligne
- Applications critiques pour l'entreprise

En combinant l'ingénierie du trafic et la QoS, les opérateurs réseau peuvent concevoir et gérer des réseaux qui répondent efficacement aux exigences de performance et de qualité de service de leurs utilisateurs, tout en optimisant l'utilisation des ressources disponibles.

II.8 Conclusion

Le protocole MPLS suscite un intérêt croissant en tant que solution unificatrice pour l'avenir, et de nombreux efforts de recherche sont déployés pour faciliter les décisions à prendre à son sujet. En raison de ses mécanismes de commutation de labels avancés et de sa facilité de déploiement sur les infrastructures réseau existantes, le MPLS se positionne comme une technologie incontournable pour demain, offrant à la fois souplesse, évolutivité et performances accrues à un coût réduit. L'avènement de cette technologie ouvre de nouvelles perspectives pour les entreprises, éliminant la nécessité de limiter les temps de communication et simplifiant la gestion des factures réseaux cœurs.

Chapitre 3
Implémentation et Optimisation d'un réseau cœur IP/MPLS

III.1 Introduction

Dans le précédent chapitre, nous avons exploré en profondeur le principe et les caractéristiques de la technologie MPLS, mettant en lumière son rôle essentiel dans l'optimisation des réseaux de communication. Dans ce chapitre, nous franchissons le pas vers la mise en œuvre pratique de cette technologie. Nous commençons par la description des outils de travail. Par la suite, nous décrivons la topologie du réseau et la démarche suivie pour sa réalisation. À la fin de ce chapitre, les objectifs doivent être atteints et le réseau doit fonctionner.

III.2 Outils de simulation :

III.2.1 Logiciel de simulation : GNS3 :

GNS3 (Graphical Network Simulator) ou simulateur graphique de réseau est un logiciel open source qui permet d'établir avec précision la topologie d'un système d'exploitation réseau pour des fonctions avancées de routage, de pare-feu ou d'hôte sans malmener vos équipements.

Afin de répondre au mieux ces besoins, **GNS3** supporte un grand nombre de types de routeurs et commutateurs, ce qui permet aux professionnels de simuler à base des équipements des de réviser efficacement leurs examens de certification Cisco et Juniper, tout en se révélant parfaitement utile aux ingénieurs et administrateurs réseau.

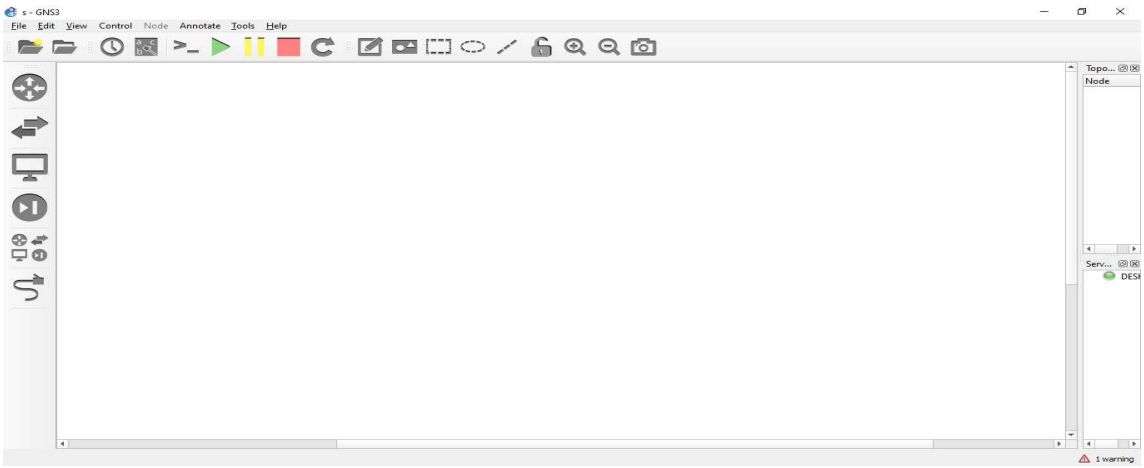

Fig. III.1 : interface du logiciel GNS3

L'interface de GNS3 est à la fois simple et puissante, offrant une expérience utilisateur agréable et efficace pour la conception et la simulation de réseaux.

III.3 Présentation de la Topologie du réseau cœur

Le logiciel **GNS3** nécessite une vraie image **IOS** pour fonctionner, à cet effet nous avons utilisé un routeur **CISCO** de type **7200** de la gamme **C7200**. Nous avons notamment mis en place des interfaces pour interconnecter les routeurs et les switches **L2** et des ordinateurs pour la simulation d'un réseau cœur et pour effectuer des tests.

- **Routeur Cisco C7200** : C'est un routeur prenant en charge une large gamme de densité, de performance et d'exigence de services, il a été conçu pour des performances et services qui font face aux besoins des entreprises, des administrations et des fournisseurs de services ainsi que pour des options de connectivité et de nombreuses fonctionnalités. Notre choix s'est tourné vers ce routeur pour son adaptation avec la norme MPLS, sa flexibilité prenant en charge les liens Fast Ethernet, Gigabit Ethernet et les ports adaptateurs exemple : PA-POS-OC3.
- **Interface** : On a utilisé des interfaces optiques pour les liaisons entre les routeurs P / -PE, et des interfaces Fast Ethernet pour les liaisons entre les routeurs PE-CE.

III.3.1 Présentation de l'architecteur cœur :

Dans ce projet nous avons utilisé l'architecteur du réseau cœur présentée sur la figure (III,2)

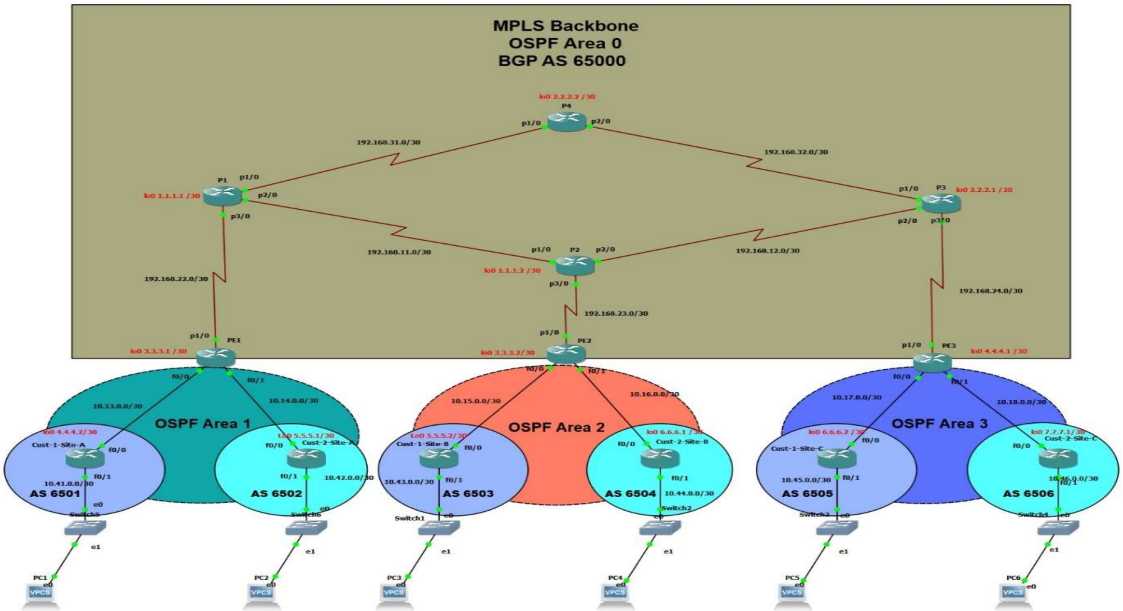

Fig. III.2 : Topologie du réseau cœur

La topologie du réseau cœur est essentielle pour assurer la stabilité et l'efficacité des communications au sein d'une infrastructure. Sa conception intelligente et sa mise en œuvre réfléchie sont des éléments clés pour garantir des performances optimales et une disponibilité continue des services réseau

Architecture du réseau cœur :

Nous avons utilisé dans ce projet 13 routeurs réparties comment suit :

- 4 routeurs provider (P) représentant le cœur MPLS :
  - ✓ P1
  - ✓ P2
  - ✓ P3
  - ✓ P4
- 3 routeurs Provider Edge (PE) représentant l'Edge MPLS :
  - ✓ PE1
  - ✓ PE2
  - ✓ PE3
- 6 routeurs Custemer Edge (CE) représentent les six sites des deux :
  - ✓ Cust-1-Site-A
  - ✓ Cust-1-Site-B
  - ✓ Cust-1-Site-C
  - ✓ Cust-2-Site-A
  - ✓ Cust-2-Site-B
  - ✓ Cust-2-Site-C
- 1 routeur reflecteur RR

Remarque : **Nous avons utilisé le modèle** (C7200-ADVENTERPRISEK9-M), **Version** 12.4(24) T5..

III.4 Configuration de la maquette

III.4.1 Plan d'adressage

Nous avons configurée les adresses IP avec le masque /30 pour les connexions point à point .Aussi nous avons adopté le masque /32 pour les interfaces de bouclage local

(loopback). La répartition des adresses IP attribuées aux interfaces de chaque routeur aussi que les adresses réseaux LAN est fixée dans le tableau III.1 qui suit :

Table III.1 : Adressage d'interface des routeurs

Equipement	Interface	Adresse IPv4	Destination
P1	P1/0	192.168.31.1 /30	**P4**
	P2/0	192.168.11.1 /30	**P2**
	P3/0	192.168.22.1 /30	**PE1**
	Loopback	1.1.1.1 /30	/
P2	P1/0	192.168.11.2 /30	**P1**
	P2/0	192.168.12.1 /30	**P3**
	P3/0	192.168.23.1 /30	**PE2**
	Loopback	1..1.1.2 /30	/
P3	P1/0	192.168.32.2 /30	**P4**
	P2/0	192.168.12.2 /30	**P2**
	P3/0	192.168.24.1 /30	**PE3**
	Loopback	2.2.2.1 /30	/
P4	P1/0	192.168.31.2 /30	**P1**
	P2/0	192.168.32.1 /30	**P3**
	Loopback	2..2.2.2 /30	/
PE1	P1/0	192.168.22.2 /30	**PE1**
	F0/0	10.13.0.1 /30	**CE1**
	F0/1	10.14.0.1 /30	**CE2**
	Loopback	3.3.3.1 /30	/
PE2	P1/0	192.168.23.2 /30	**P2**
	F0/0	10.15.0.1 /30	**CE3**
	F0/1	10.16.0.1 /30	**CE4**
	Loopback	3.3.3.2 /30	/

PE3	P1/0	192.168.24.2 /30	**P3**
	F0/0	10.17.0.1 /30	**CE5**
	F0/1	10.18.0.1 /30	**CE6**
	Loopback	4.4.4.1 /30	/
CE1	F0/0	10.13.0.2 /30	**PE1**
	F0/1	10.41.0.1 /16	**PC1**
	Loopback	4.4.4.2 /30	/
CE2	F0/0	10.14.0.2 /30	**PE1**
	F0/1	10.42.0.1 /16	**PC2**
	Loopback	5.5.5.1 /30	/
CE3	F0/0	10.15.0.2 /30	**PE2**
	F0/1	10.43.0.1 /16	**PC3**
	Loopback	5.5.5.2 /30	/
CE4	F0/0	10.16.0.2 /30	**PE2**
	F0/1	10.44.0.1 /16	**PC4**
	Loopback	6.6.6.1 /30	/
CE5	F0/0	10.17.0.2 /30	**PE3**
	F0/1	10.45.0.1 /16	**PC5**
	Loopback	6.6.6.2 /30	/
CE6	F0/0	10.18.0.2 /30	**PE3**
	F0/1	10.46.0.1 /16	**PC6**
	Loopback	7.7.7.1 /30	/

PC1	Eth0	10.41.0.2 /16	/
PC2	Eth0	10.42.0.2 /16	/
PC3	Eth0	10.43.0.2 /16	/
PC4	Eth0	10.44.0.2 /16	/
PC5	Eth0	10.45.0.2 /16	/
PC6	Eth0	10.46.0.2 /16	/

III.4.2 Configuration de base :

Nous commençons la configuration en utilisant la commande « **enable** » pour avoir le mode d'exécution privilégié. On passe en mode configuration avec la commande « **configure terminal** » puis « **hostname** » pour donner un nom à chaque routeur (Fig. III.3).

```
P#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P(config)#hostname P1
P1(config)#
```

Fig. III.3 : Configuration de base

La configuration de base dans GNS3 est un premier pas essentiel pour créer des réseaux virtuels fonctionnels. Elle permet de définir les paramètres initiaux nécessaires à la communication entre les appareils virtuels, offrant ainsi une plateforme stable pour des expériences réseau plus avancées. (**Fig. III.3**)

III.4.3 Configuration des interfaces :

On configure les interfaces et Loopback des routeurs en indiquant l'interface, puis lui affecter une adresse IP et un masque réseau et enfin la mettre en marche avec la commande « **no shutdown** », toutes les interfaces seront configurées de la même manière (Fig. III.4).

```
P1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P1(config)#inter
P1(config)#interface loo
P1(config)#interface loopback 0
P1(config-if)#ip add
P1(config-if)#ip address 1.1.1.1 255.255.255.252
P1(config-if)#exit
P1(config)#inter
P1(config)#interface p1/0
P1(config-if)#ip add
P1(config-if)#ip address 192.168.31.1 255.255.255.252
P1(config-if)#no shut
P1(config-if)#no shutdown
P1(config-if)#exit
P1(config)#interf
P1(config)#interface p2/0
P1(config-if)#ip add
P1(config-if)#ip address 192.168.11.1 255.255.255.252
P1(config-if)#no shut
P1(config-if)#no shutdown
P1(config-if)#exit
P1(config)#inter
P1(config)#interface p3/0
P1(config-if)#ip add
P1(config-if)#ip address 192.168.22.1 255.255.255.252
P1(config-if)#no shut
P1(config-if)#no shutdown
P1(config-if)#exit
P1(config)#
```

Fig. III.4 : Configuration des interfaces du routeur P1

La configuration des interfaces du routeur P1 dans GNS3 est une étape cruciale pour établir une connectivité efficace au sein de l'infrastructure réseau simulée. En définissant correctement les adresses IP, les masques de sous-réseau et d'autres paramètres, cette configuration assure un fonctionnement fluide des communications entre les périphériques virtuels, formant ainsi la base solide de la topologie réseau.

Remarque : Pour sauvegarder la configuration on exécute la commande « **write** ».

```
P1#wr
Building configuration...
[OK]
P1#
```

Fig. III.5 : Exécution de la Command Write

L'exécution de la commande Write dans GNS3 est une étape cruciale pour sauvegarder les configurations des périphériques virtuels. Cela permet de prévenir la perte de données et de restaurer facilement les configurations en cas de besoin, assurant ainsi la stabilité du réseau simulé. (**Fig. III.5**)

- On refait les mêmes étapes de configuration pour le reste des routeurs.

Pour confirmer la configuration on affiche toues les interfaces de routeurs en utilisant la commande « **show ip interface brief** ». (Fig. III.6)

```
P1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
POS1/0                     192.168.31.1    YES NVRAM  up                    up
POS2/0                     192.168.11.1    YES NVRAM  up                    up
POS3/0                     192.168.22.1    YES NVRAM  up                    up
Loopback0                  1.1.1.1         YES NVRAM  up                    up
P1#
```

Fig. III.6 : Affichage de configuration des interfaces

L'affichage de la configuration des interfaces, tel que présenté dans la figure, est essentiel pour inspecter rapidement et précisément les paramètres de configuration des périphériques réseau dans GNS3. Cela facilite le dépannage, la vérification et la modification des configurations, contribuant ainsi à la fiabilité de l'infrastructure réseau simulée.

La figure III.6 illustre clairement la configuration des interfaces du routeur P1, notamment les interfaces Pos1/0, Pos2/0 et Pos3/0 attribuées

III.4.4 Configuration des PCs

Après le démarrage des nœuds VPCS, l'accès à la console de chaque nœud permet de définir manuellement l'adresse IP, le masque de sous-réseau et la passerelle, comme indiqué à la figure III.7.

```
PC1> ip 10.41.0.2 255.255.255.252 10.41.0.1
Checking for duplicate address...
PC1 : 10.41.0.2 255.255.255.252 gateway 10.41.0.1

PC1>
```

Fig. III.7 : Configuration PC1

La configuration de PC1 dans GNS3 est une étape cruciale pour établir la connectivité et tester les communications au sein de la topologie. En définissant précisément les paramètres réseau comme l'adresse IP, le masque de sous-réseau et la passerelle par défaut, les utilisateurs peuvent simuler des interactions réseau réalistes et valider leurs configurations. Une configuration minutieuse de PC1 est donc essentielle pour des tests efficaces et des résultats cohérents dans l'environnement simule

L'adresse IP configurée sera perdue au redémarrage du router et pour cette raison on va enregistrer la configuration par la commande « **save** » (Fig. III.8).

```
PC1> save
Saving startup configuration to startup.vpc
.  done

PC1>
```

Fig. III.8: enregistrement de configuration du PC1

L'enregistrement de la configuration de PC1 dans GNS3 est crucial pour sauvegarder les paramètres réseau et garantir la cohérence de l'environnement de simulation. Cela permet une restauration rapide des configurations précédentes en cas de besoin, assurant ainsi une gestion efficace et fiable des configurations réseaux

- On effectue les mêmes étapes de configuration pour le reste des PCs.

III.4.5 Configuration du Protocol de routage OSPF :

Nous avons porté notre choix sur le protocole OSPF à cause de ses multiples avantages :

- C'est un protocole de routage à états de liens.
- Il est rapide en termes de convergence

La configuration d'OSPF doit être effectuée sur tous les routeurs du réseau IP/MPLS comme suit :

On active pour chaque routeur le protocole OSPF, qui permet de créer une table de routage dans chaque routeur avec les commandes suivantes (Fig. III.9) :

- « **router ospf 1** » : pour l'activation du processus ospf, le 1 représente l'identifiant du routeur.
- « **network** » : pour déclarer et spécifier le réseau participant au processus OSPF.
- « **e**

```
P1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P1(config)#router ospf 1
P1(config-router)#router-
P1(config-router)#router-id
% Incomplete command.

P1(config-router)#router-id 1.1.1.1
P1(config-router)#network 1.1.1.1 0.0.0.0 area 0
P1(config-router)#network 192.168.11.0 0.0.0.3 area 0
P1(config-router)#network 192.168.22.0 0.0.0.3 area 0
P1(config-router)#network 192.168.31.0 0.0.0.3 area 0
P1(config-router)#exit
P1(config)#exit
P1#
```

Fig. III.9: Activation d'OSPF

Activer OSPF est une étape clé pour permettre le routage dynamique dans un réseau.

On refait les mêmes étapes de configuration pour le reste des routeurs.

Pour visualiser la table de voisinage et vérifier qu'OSPF a établi une contigüité avec ses voisins, on applique la commande « **show ip ospf neighbor** » (Fig. III.10)

```
P1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:34    192.168.31.2    POS1/0
3.3.3.1           0   FULL/  -        00:00:31    192.168.22.2    POS3/0
1.1.1.2           0   FULL/  -        00:00:36    192.168.11.2    POS2/0
P1#
```

Fig. III.10: Affichage des voisins du routeur P1

Afficher les voisins du routeur P1 permet de visualiser les périphériques directement connectés à ce routeur.

La figure III.10 montre le voisinage du router P1sont (P3, PE1, P2)
On exécute la commande « show ip route OSPF » qui nous montre la table de routage de P1.

La lettre « O » représente les liens connectés par le protocole OSPF.La figure III.11 présente la table de routage OSPF.

```
P1#show ip route ospf
     192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/2] via 192.168.11.2, 00:10:25, POS2/0
     1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       1.1.1.2/32 [110/2] via 192.168.11.2, 00:10:25, POS2/0
     2.0.0.0/32 is subnetted, 2 subnets
O       2.2.2.2 [110/2] via 192.168.31.2, 00:09:31, POS1/0
O       2.2.2.1 [110/3] via 192.168.31.2, 00:09:31, POS1/0
                [110/3] via 192.168.11.2, 00:10:25, POS2/0
     3.0.0.0/32 is subnetted, 2 subnets
O       3.3.3.2 [110/3] via 192.168.11.2, 00:10:25, POS2/0
O       3.3.3.1 [110/2] via 192.168.22.2, 00:10:25, POS3/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.1 [110/4] via 192.168.31.2, 00:09:31, POS1/0
                [110/4] via 192.168.11.2, 00:10:25, POS2/0
     192.168.24.0/30 is subnetted, 1 subnets
O       192.168.24.0 [110/3] via 192.168.31.2, 00:09:31, POS1/0
                     [110/3] via 192.168.11.2, 00:10:25, POS2/0
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/2] via 192.168.11.2, 00:10:25, POS2/0
     192.168.32.0/30 is subnetted, 1 subnets
O       192.168.32.0 [110/2] via 192.168.31.2, 00:09:31, POS1/0
P1#
```

Fig. III.11 : Routes OSPF

Les routes OSPF sont les chemins que les paquets de données suivent à travers un réseau

La confirmation se fait à travers un PING de PC1 vers PC2. Pour effectuer cette étape On utilise la commande **PING** et l'adresse IP destination « **10.43.0.2** » (Fig. III.12).

```
PC1> ping 10.43.0.2
*10.41.0.1 icmp_seq=1 ttl=255 time=15.633 ms (ICMP type:3, code:1, Destination host unreachable)
*10.41.0.1 icmp_seq=2 ttl=255 time=19.015 ms (ICMP type:3, code:1, Destination host unreachable)
*10.41.0.1 icmp_seq=3 ttl=255 time=3.497 ms (ICMP type:3, code:1, Destination host unreachable)
*10.41.0.1 icmp_seq=4 ttl=255 time=19.674 ms (ICMP type:3, code:1, Destination host unreachable)
*10.41.0.1 icmp_seq=5 ttl=255 time=23.532 ms (ICMP type:3, code:1, Destination host unreachable)

PC1>
```

Fig. III.12: Ping PC1 vers PC3

Commentaire sur **Fig. III.12** :

Le ping de PC1 vers PC3 vérifie la connectivité entre ces deux appareils.On refait plusieurs Ping vers les différents réseaux pour vérifier la connectivite

III.4.6 Configuration MPLS :

Pour activer MPLS, il est nécessaire de le configurer à la fois globalement et sur chaque interface où son utilisation est requise. Comme cette configuration sur de nombreuses interfaces peut prendre du temps, l'activation automatique de MPLS LDP permet de simplifier ce processus en activant LDP globalement sur chaque interface associée à une instance IGP (**Interior Gateway Protocol**). Actuellement, le seul IGP prenant en charge cette fonctionnalité est OSPF (Open Shortest Path First) L'objectif de la configuration automatique MPLS LDP est de rendre la configuration plus facile, plus rapide et sans erreur. Nous utilisons la commande «**mpls ldp auto config**» pour activer LDP sur chaque interface appartenant à une zone OSPF. (Fig. III.13**)**

```
P1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P1(config)#router ospf 1
P1(config-router)#mpls ldp aut
P1(config-router)#mpls ldp autoconfig
P1(config-router)#end
P1#
```

Fig. III.13 : Configuration de MPLS automatique

La configuration automatique de MPLS simplifie le déploiement et la gestion des réseaux MPLS.

- On refait les mêmes étapes de configuration pour le reste des routeurs Backbone.

On effectue la commande **« show mpls interfaces »** pour lister les interfaces mpls qui ont été activées. (Fig. III.14).

```
P1#show mpls interfaces
Interface              IP           Tunnel   BGP Static Operational
POS1/0                 Yes (ldp)    Yes      No  No     Yes
POS2/0                 Yes (ldp)    Yes      No  No     Yes
POS3/0                 Yes (ldp)    Yes      No  No     Yes
P1#
```

Fig. III.14 : Interfaces MPLS

Les interfaces MPLS permettent le transfert efficace des données dans les réseaux MPLS.

- **Vérification du fonctionnement du MPLS :**

  Vérification des sessions établies par LDP entre les routeurs voisins avec la commande « **show tcp brief** » qui permet de vérifier les sessions LDP (Fig. III.15).

```
P1#show tcp brief
TCB        Local Address               Foreign Address             (state)
6836E73C   1.1.1.1.646                 2.2.2.2.11965               ESTAB
68353980   1.1.1.1.646                 1.1.1.2.55521               ESTAB
6833845C   1.1.1.1.646                 3.3.3.1.58028               ESTAB
P1#
```

Fig. III.15: Vérification des sessions LDP

Vérifier les sessions LDP permet de s'assurer que les appareils IP/ MPLS établissent correctement des liaisons de données.

Pour le test du bon fonctionnement du protocole MPLS/IP on utilise les deux commandes Suivantes :

La premiere commande « **show mpls ldp neighbor** » qui a pour rôle de découvrir les voisins crée par le protocole MPLS (Fig. III.16).

La deuxième commande de test du protocole MPLS est **« show mpls forwardingtable»,** qui permet de voir l'affectation des labels aux adresses qui se trouvent dans la table FEC. (Fig. III.17).

Le résultat de vérification nous indique les labels affectés aux adresses réseau pour qu'ils puissent circuler dans le réseau **IP-MPLS**. A titre d'exemple dans la figure **III.17** le protocole **LDP** affecte le **label 24**, à l'adresse : **192.168.23.0.**

```
P1#show mpls ldp neighbor
    Peer LDP Ident: 3.3.3.1:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 3.3.3.1.58028 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 144/142; Downstream
        Up time: 01:48:56
        LDP discovery sources:
          POS3/0, Src IP addr: 192.168.22.2
        Addresses bound to peer LDP Ident:
          192.168.22.2    3.3.3.1
    Peer LDP Ident: 1.1.1.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 1.1.1.2.55521 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 142/140; Downstream
        Up time: 01:48:55
        LDP discovery sources:
          POS2/0, Src IP addr: 192.168.11.2
        Addresses bound to peer LDP Ident:
          192.168.11.2    192.168.12.1    192.168.23.1    1.1.1.2
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 2.2.2.2.11965 - 1.1.1.1.646
        State: Oper; Msgs sent/rcvd: 139/139; Downstream
        Up time: 01:48:02
        LDP discovery sources:
          POS1/0, Src IP addr: 192.168.31.2
        Addresses bound to peer LDP Ident:
          192.168.31.2    192.168.32.1    2.2.2.2
P1#
```

Fig. III.16 : Résultat du Voisinage MPLS

Le résultat du voisinage MPLS indique les appareils voisins avec lesquels un périphérique MPLS est connecté.

```
P1#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     4.4.4.1 2 [14]   0             PO3/0      point2point
17     16            3.3.3.1 2 [12]   0             PO2/0      point2point
18     18            4.4.4.1/32       0             PO2/0      point2point
       18            4.4.4.1/32       0             PO1/0      point2point
19     19            3.3.3.2/32       0             PO2/0      point2point
20     Pop Label     3.3.3.1/32       13655         PO3/0      point2point
21     21            2.2.2.1/32       0             PO2/0      point2point
       21            2.2.2.1/32       0             PO1/0      point2point
22     No Label      1.1.1.2/32       0             PO2/0      point2point
23     24            192.168.24.0/30  0             PO2/0      point2point
       24            192.168.24.0/30  0             PO1/0      point2point
24     Pop Label     192.168.23.0/30  0             PO2/0      point2point
25     Pop Label     192.168.12.0/30  0             PO2/0      point2point
26     Pop Label     4.4.4.1 1 [20]   0             PO3/0      point2point
27     16            3.3.3.1 1 [16]   0             PO1/0      point2point
28     Pop Label     192.168.32.0/30  0             PO1/0      point2point
29     No Label      2.2.2.2/32       13229         PO1/0      point2point
P1#
```

Fig. III.17 : Correspondance entre les labels et les Adresses IP

La correspondance entre les labels et les adresses IP est essentielle pour le fonctionnement efficace des réseaux MPLS, permettant le routage des paquets de manière rapide et précise.

On peut citer un autre exemple d'affectation de labels pour le réseau **1.1.1.2./32** Avec la commande **« show mpls ldp bindings » (Fig. III.18).**

```
P1#show mpls ldp bindings 1.1.1.2 255.255.255.255
  lib entry: 1.1.1.2/32, rev 18
        local binding:  label: 22
        remote binding: lsr: 3.3.3.1:0, label: 19
        remote binding: lsr: 2.2.2.2:0, label: 22
P1#
```

Fig. III.18 : Allocation des labels pour le réseau 1.1.1.2

L'allocation des labels pour le réseau 1.1.1.2 permet d'identifier de manière unique ce réseau dans le domaine MPLS, facilitant ainsi le routage des paquets à travers le réseau.

La figure III.19 montre l'adresse IP et le label de chaque saut, suite à un traçage de la route emprunté depuis le routeur PE1 vers PE3 avec la commande **« traceroute ».**

```
PE1#traceroute 4.4.4.1

Type escape sequence to abort.
Tracing the route to 4.4.4.1

  1 192.168.22.1 [MPLS: Label 17 Exp 0] 140 msec 112 msec 64 msec
  2 192.168.11.2 [MPLS: Label 16 Exp 0] 88 msec
    192.168.31.2 [MPLS: Label 16 Exp 0] 88 msec 96 msec
  3 192.168.12.2 [MPLS: Label 16 Exp 0] 136 msec
    192.168.32.2 [MPLS: Label 27 Exp 0] 104 msec 96 msec
  4 192.168.24.2 124 msec 100 msec 108 msec
PE1#
```

Fig. III.19 : Traçage de la route entre PE1 et PE3

Le traçage de la route entre PE1 et PE3 permet de suivre le chemin emprunté par les paquets à travers le réseau, facilitant ainsi le dépannage et l'optimisation des performances.

III.4.7 Configuration du MP-BGP L3 VPN Ver4

Le Border Gateway Protocol (BGP):

On utilisé BGP pour échanger des informations de routage entre les différents systèmes autonomes (AS) sur Internet. Il permet de déterminer les meilleurs chemins pour la transmission des données en tenant compte de divers critères, tels que les politiques de routage, la redondance et la fiabilité des chemins. BGP est essentiel pour garantir l'inter connectivité et l'efficacité du routage à l'échelle internet.

Pour commencer la configuration, nous avons désigné le routeur P4 comme routeur réflecteur, et les routeurs PE1, PE2, et PE3 comme des clients RR.

III.4.7.1 Configuration de la partie IBGP

- **Configuration du protocole BGP sur le routeur réflecteur (Fig. 3.20)**

Pour la configuration du protocole BGP, nous avons utilisé les commandes suivantes :

- « **router bgp <as-number> »** : pour l'activation du processus BGP, l'**as-number** représente le numéro de l'AS l'autonome Systeme.
- « **bgp router-id <router-id> »** : pour déterminer ID de routeur BGP.
- « **neighbor <ip-address> remote-as <as-number>**» : pour déclarer le numéro AS distant d'un voisin BGP (dans notre cas nous avons trois voisin **PE1**, **PE2**, **PE3**)
- « **neighbor <ip-address> update-source loopback <number>**» : pour spécifie l'adresse source pour atteindre le voisin (**PE1, PE2, PE3**)
- « **neighbor <ip-address> route-reflector-client** » : pour configure le routeur comme réflecteur de route BGP et le homologue spécifié comme client.

```
P4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P4(config)#router bgp 65000
P4(config-router)#bgp rout
P4(config-router)#bgp router-id 2.2.2.2
P4(config-router)#neigh
P4(config-router)#neighbor 3.3.3.1 remot
P4(config-router)#neighbor 3.3.3.1 remote-as 65000
P4(config-router)#neighbor 3.3.3.1 updt
P4(config-router)#neighbor 3.3.3.1 updat
P4(config-router)#neighbor 3.3.3.1 update-source loo
P4(config-router)#neighbor 3.3.3.1 update-source loopback 0
P4(config-router)#neighbor 3.3.3.1 router
P4(config-router)#neighbor 3.3.3.1 route
P4(config-router)#neighbor 3.3.3.1 route-re
P4(config-router)#neighbor 3.3.3.1 route-reflector-client
P4(config-router)#nei
P4(config-router)#neighbor 3.3.3.2 remo
P4(config-router)#neighbor 3.3.3.2 remote
P4(config-router)#neighbor 3.3.3.2 remote-as 65000
P4(config-router)#neighbor 3.3.3.2 upd
P4(config-router)#neighbor 3.3.3.2 update-source loo
P4(config-router)#neighbor 3.3.3.2 update-source loopback 0
P4(config-router)#neighbor 3.3.3.2 router
P4(config-router)#neighbor 3.3.3.2 route
P4(config-router)#neighbor 3.3.3.2 route-re
P4(config-router)#neighbor 3.3.3.2 route-reflector-client
P4(config-router)#neighbor 4.4.4.1 remote-as 65000
P4(config-router)#neighbor 4.4.4.1 upd
P4(config-router)#neighbor 4.4.4.1 update-source loo
P4(config-router)#neighbor 4.4.4.1 update-source loopback 0
P4(config-router)#neighbor 4.4.4.1 route-reflector-client
P4(config-router)#end
P4#
```

Fig. III.20 : Configuration de BGP sur le Routeur Réflecteur P4

La configuration de BGP sur le routeur réflecteur P4 permet d'établir des sessions BGP et de gérer le routage dans un environnement réseau complexe. (**Fig. III.20)**

- Configuration du protocole BGP sur les routeurs clients RR (**Fig. III.21)**

Pour la configuration du protocole BGP, nous avons exécuté les commandes suivantes :

- « **router bgp <as-number> »** : pour l'activation du processus BGP, l'**as-number** représente l'autonome systeme.
- « **bgp router-id <router-id> »** : pour déterminer ID de routeur BGP.
- **« neighbor <ip-address> remote-as <as-number>**» : pour déclarer le numéro AS distant d'un voisin BGP (dans notre c'est le routeur réflecteur **P4**).
- **« neighbor <ip-address> update-source loopback <number>**» : pour spécifie l'adresse source pour atteindre le voisin (**P4**).

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#router bgp 65000
PE1(config-router)#bgp router
PE1(config-router)#bgp router-id 3.3.3.1
PE1(config-router)#neigh
PE1(config-router)#neighbor 2.2.2.2 remote
PE1(config-router)#neighbor 2.2.2.2 remote-as 65000
PE1(config-router)#neighbor 2.2.2.2 upda
PE1(config-router)#neighbor 2.2.2.2 update-source loo
PE1(config-router)#neighbor 2.2.2.2 update-source loopback 0
PE1(config-router)#end
PE1#
```

Fig. III.21 : Configuration de BGP sur le Routeur client (PE1) de RR

Configurer BGP sur le routeur client (PE1) du routeur réflecteur (RR) permet d'établir des sessions BGP entre le client et le réflecteur, facilitant ainsi la propagation des informations de routage dans le réseau.

- On fait les mêmes étapes de configuration pour le reste des routeurs clients RR (PE2 et PE3).

► **Activation de VPN V4 sur les Neighbors**

Pour le routeur réflecteur :

Pour l'activation du VPN sur le routeur réflecteur P4, nous avons exécuté les commandes suivantes (Fig. 3.22) :

- « **address-family vpnv4 »** : pour créer la famille d'adresses BGP VPNv4 entrez dans sa vue.
- **« neighbor <ip-address> activate** » : pour permettre l'échange d'informations avec un voisin BGP.
- **« neighbor <ip-address> send-community both** » : pour permettre d'envoyer des valeurs communautaires au voisin.

- « **neighbor <ip-address> route-reflector-client** » : pour configure le routeur comme réflecteur de route BGP et le homologue spécifié comme client.

```
P4(config)#router bgp 65000
P4(config-router)#add
P4(config-router)#address-family vpnv4
P4(config-router-af)#neighb
P4(config-router-af)#neighbor 3.3.3.1 activate
P4(config-router-af)#neighbor 3.3.3.1 send
P4(config-router-af)#neighbor 3.3.3.1 send-community both
P4(config-router-af)#neighbor 3.3.3.1 route
P4(config-router-af)#neighbor 3.3.3.1 route-re
P4(config-router-af)#neighbor 3.3.3.1 route-reflector-client
P4(config-router-af)#
P4(config-router-af)#neigh
P4(config-router-af)#neighbor 3.3.3.2 activate
P4(config-router-af)#neighbor 3.3.3.2 send-c
P4(config-router-af)#neighbor 3.3.3.2 send-community both
P4(config-router-af)#neighbor 3.3.3.2 route-reflector-client
P4(config-router-af)#
P4(config-router-af)#neighbor 4.4.4.1 activate
P4(config-router-af)#neighbor 4.4.4.1 send-community both
P4(config-router-af)#neighbor 4.4.4.1 route-reflector-client
P4(config-router-af)#end
P4#
```

Fig. III.22 : L'activation de VPN V4 sur le Routeur Réflecteur

L'activation de VPN V4 sur le routeur réflecteur permet d'étendre les fonctionnalités VPN à travers le réseau, facilitant ainsi la segmentation et la sécurisation du trafic. (**Fig. III.22)**

► **Pour les routeurs Clients RR (PE1, PE2, PE3) :**

Pour l'activation du VPN sur les routeurs clients RR (PE1, PE2, PE3), nous avons exécuté les commandes suivantes (Fig. III.23):

- « **address-family vpnv4 »** : pour créer la famille d'adresses BGP VPNv4 entrez dans sa vue.
- **« neighbor <ip-address> activate** » : pour permettre l'échange d'informations avec un voisin BGP.

- « **neighbor <ip-address> send-community both** » : pour permettre d'envoyer des valeurs communautaires au voisin.

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#router bgp 65000
PE1(config-router)#add
PE1(config-router)#address-family vpnv4
PE1(config-router-af)#neighb
PE1(config-router-af)#neighbor 2.2.2.2 activate
PE1(config-router-af)#neighbor 2.2.2.2 send
PE1(config-router-af)#neighbor 2.2.2.2 send-community both
PE1(config-router-af)#end
PE1#
```

Fig. III.23 : L'activation de VPN V4 sur le Routeur client RR (PE1)

Activer le VPN V4 sur le routeur client RR (PE1) permet d'étendre les fonctionnalités VPN à ce périphérique, facilitant ainsi la gestion sécurisée du trafic dans le réseax

► On refait les mêmes étapes de configuration pour le reste des routeurs clients RR (PE2, PE3).

III.4.7.2 Configuration du Routage Virtuel avec (VRF)

Pour commencer, nous avons défini deux clients, Cust-1 et Cust-2, chacun possédant trois sites : Site A, Site B et Site C. Chaque client utilise des Route Distinguishers (RD) et des Route Targets (RT) différents, comme indiqué dans le tableau III.2.

Table III.2 : Configuration des clients et des sites avec RD et RT

Routeur	Route Target	Route Distinguishers
Cust-1 Site-A	**65000:100**	**65000 :1**
Cust-2 Site-A	**65000:200**	**65000 :2**
Cust-1 Site-B	**65000:100**	**65000 :3**
Cust-2 Site-B	**65000:200**	**65000 :4**
Cust-1 Site-C	**65000:100**	**65000 :5**
Cust-2 Site-C	**65000:200**	**65000 :6**

Pour la configuration des VRF nous avons exécuté les commandes suivantes sur les routeurs PE (Fig. 3.24) :

- « **vrf definition <vrf-name> » :** pour création des instances vrf pour nos clients Cust-1 et Cust-2

- « **adresse-famille ipv4** » : pour initialiser la famille d'adresses. Nous pouvons configurer les adresses IPv4 et IPv6. Pour notre exemple, nous nous en tiendrons à IPv4.
- « **route-distinguisher » :** pour configure un sélecteur de route (RD) pour une famille d'adresses d'instance VPN.
- « **route-target both » :** pour la création d'une liste de cibles de routes d'importation et d'exportation pour le VRF avec les mêmes paramètres.

Cette configuration assure que chaque client dispose de routes distinctes et appropriées pour leurs sites respectifs.

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#vrf def
PE1(config)#vrf definition cust-1
PE1(config-vrf)#add
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-af)#exit
PE1(config-vrf)#rout
PE1(config-vrf)#rd 65000:1
PE1(config-vrf)#route
PE1(config-vrf)#route-target both 65000:100
PE1(config-vrf)#exit
PE1(config)#vrf defe
PE1(config)#vrf def
PE1(config)#vrf definition cust-2
PE1(config-vrf)#add
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-af)#exit
PE1(config-vrf)#rd 65000:2
PE1(config-vrf)#route
PE1(config-vrf)#route-target both 65000:200
PE1(config-vrf)#exit
PE1(config)#
```

Fig. III.24 : Configuration du VRF cust-1 cust-2 sur le routeur PE1

La configuration du VRF cust-1 et cust-2 sur le routeur PE1 permet d'isoler les réseaux des différents clients, assurant ainsi la confidentialité et la sécurité des données dans un environnement partagé.

- On refait les mêmes étapes de configuration pour le reste des routeurs (PE2, PE3).

Après la configuration des VRF, chaque VRF doit être associé à l'interface correspondante de chaque client, pour cela nous avons exécuté les commandes suivantes sur les routeurs PE (Fig. III.25).

III.4.7.3 Configuration de la partie EBGP :

► **Configuration de la publicité conditionnelle compatible BGP VRF sur les routeurs clients RR :**

Pour la configuration du protocole BGP, nous avons exécuté les commandes suivantes (Fig. III.26) :

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#interface fas
PE1(config)#interface fastEthernet 0/0
PE1(config-if)#vrf forw
PE1(config-if)#vrf forwarding cust-1
PE1(config-if)#ip add
PE1(config-if)#ip address 10.13.0.1 255.255.255.252
PE1(config-if)#no shut
PE1(config-if)#no shutdown
PE1(config-if)#end
PE1#
*May 26 12:57:53.071: %SYS-5-CONFIG_I: Configured from console by console
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#interf
PE1(config)#interface fast
PE1(config)#interface fastEthernet 0/1
PE1(config-if)#vrf for
PE1(config-if)#vrf forwarding cust-2
PE1(config-if)#ip add
PE1(config-if)#ip address 10.14.0.1 255.255.255.252
PE1(config-if)#no shut
PE1(config-if)#no shutdown
PE1(config-if)#exit
PE1(config)#exit
PE1#
*May 26 12:58:46.787: %SYS-5-CONFIG_I: Configured from console by console
PE1#
```

Fig. III.25 : Affectation des VRF aux interfaces de routeur PE1

L'affectation des VRF aux interfaces du routeur PE1 permet de spécifier quelles interfaces appartiennent à quel VRF, créant ainsi des domaines de routage virtuels distincts pour chaque client ou application.

```
PE1(config)#router bgp 65000
PE1(config-router)#add
PE1(config-router)#address-family ipv4 vrf cust-1
PE1(config-router-af)#neigh
PE1(config-router-af)#neighbor 10.13.0.2 remote
PE1(config-router-af)#neighbor 10.13.0.2 remote-as 65001
PE1(config-router-af)#exit
PE1(config-router)#address-family ipv4 vrf cust-2
PE1(config-router-af)#neighbor 10.14.0.2 remote-as 65002
PE1(config-router-af)#exit
PE1(config-router)#exit
PE1(config)#exit
PE1#
*May 26 15:12:06.435: %SYS-5-CONFIG_I: Configured from console by console
PE1#
```

Fig. III.26 : Configuration de la publicité conditionnelle compatible BGP VRF sur le routeur PE1

La configuration de la publicité conditionnelle compatible BGP VRF sur le routeur PE1 permet de contrôler la distribution des routes BGP entre les différents VRF, assurant ainsi une gestion efficace du trafic dans un environnement réseau multi-client. (**Fig. III.26)**

- « **router bgp <as-number>** » : pour l'activation du processus BGP, l'**as-number** représente l'autonome système de backbone.

- **«address-family ipv4 [vrf vrf-name] »** : pour initialiser la famille d'adresses. Nous pouvons configurer les adresses IPv4 et IPv6. Pour notre exemple, nous nous en tiendrons à IPv4.
- **« neighbor <ip-address> remote-as <as-number>»** : pour déclarer le numéro AS distant d'un voisin BGP (dans notre c'est l'interface adjacente de routeur CE).

On refait les mêmes étapes de configuration pour le reste des routeurs (PE2, PE3).

► **Configuration de BGP sur les Customer Edge :**

Pour la configuration du protocole BGP, nous avons exécuté les commandes suivantes (Fig. 3.27) :

- « **router bgp <as-number>** » : pour l'activation du processus BGP, l'**as-number** représente l'autonome système de la zone de client.
- « **bgp router-id <router-id>** » : pour déterminer ID de routeur BGP (dans notre cas ID c'est interface f0/0 des routeurs CE).
- **« neighbor <ip-address> remote-as <as-number>»** : pour déclarer le numéro AS distant d'un voisin BGP (dans notre c'est l'interface adjacente de routeur PE).
- **« network <ip-address> mask <adresse-masque>»** : pour inclure l'adresse IP de l'interface loopback dans le processus de routage.

```
Cust-1-Site-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cust-1-Site-A(config)#router bgp 65001
Cust-1-Site-A(config-router)#bgp rout
Cust-1-Site-A(config-router)#bgp router-id 10.13.0.2
Cust-1-Site-A(config-router)#neigh
Cust-1-Site-A(config-router)#neighbor 10.13.0.1 rem
Cust-1-Site-A(config-router)#neighbor 10.13.0.1 remote
Cust-1-Site-A(config-router)#neighbor 10.13.0.1 remote-as 65000
Cust-1-Site-A(config-router)#netw
Cust-1-Site-A(config-router)#network 4.4.4.2 mask 255.255.255.255
Cust-1-Site-A(config-router)#exit
Cust-1-Site-A(config)#
```

Fig. III.27 : Configuration de BGP sur le Cust-1-Site-A

Configurer BGP sur le site A du client 1 (Cust-1-Site-A) permet d'établir des sessions BGP avec d'autres périphériques du réseau, facilitant ainsi l'échange d'informations de routage et la connectivité avec d'autres sites ou clients.

- On refait Mêmes étapes de configuration pour le reste des routeurs Customer Edge.

Remarque : Nous avons procédé au changement du masque de sous-réseau de /30 a /32 pour l'interface loopback0 sur les routeurs Provider Edge et Customer Edge.

III.4.7.4 Vérification de l'état du voisin BGP :

Pour afficher l'état de toutes les connexions (BGP), nous utilisons la commande « **show ip bgp summary** » (Fig. III.28**).**

```
P4#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.1         4        65000       5       9        0    0    0 00:01:20 (NoNeg)
3.3.3.2         4        65000       5       9        0    0    0 00:01:15 (NoNeg)
4.4.4.1         4        65000       5       9        1    0    0 00:01:15        0
P4#
```

Fig. III.28 : Résumé des informations BGP (Border Gateway Protocol) sur le routeur réflecteur P4

Le résumé des informations BGP sur le routeur réflecteur P4 fournit un aperçu des sessions BGP établies, des routes apprises et des états de voisinage BGP dans le réseau, permettant ainsi une surveillance efficace et une gestion du routage dans l'infrastructure.

Pour afficher des informations sur un homologue et toutes les routes reçues de cet homologue, nous utilise la commande « s**how ip bgp neighbor** » (p4)

```
                              Outbound    Inbound
 Local Policy Denied Prefixes:    --------    -------
   Total:                              0          0
 Number of NLRIs in the update sent: max 0, min 0

For address family: VPNv4 Unicast
 BGP table version 7, neighbor version 7/0
 Output queue size : 0
 Index 2, Offset 0, Mask 0x4
 Route-Reflector Client
 2 update-group member
 Community attribute sent to this neighbor
                             Sent       Rcvd
 Prefix activity:            ----       ----
   Prefixes Current:            6          2 (Consumes 136 bytes)
   Prefixes Total:              6          2
   Implicit Withdraw:           0          0
   Explicit Withdraw:           0          0
   Used as bestpath:          n/a          2
   Used as multipath:         n/a          0

                              Outbound    Inbound
 Local Policy Denied Prefixes:    --------    -------
   Total:                              0          0
 Number of NLRIs in the update sent: max 1, min 1

 Address tracking is enabled, the RIB does have a route to 3.3.3.1
 Connections established 1; dropped 0
 Last reset never
 Transport(tcp) path-mtu-discovery is enabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 2.2.2.2, Local port: 179
Foreign host: 3.3.3.1, Foreign port: 24059
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
```

Comme le montre lafigure III.29, le chemin d'accès complet est détaillé ci-dessus.

```
P4#show ip bgp neighbors
BGP neighbor is 3.3.3.1,  remote AS 65000, internal link
  BGP version 4, remote router ID 3.3.3.1
  BGP state = Established, up for 00:53:44
  Last read 00:00:59, last write 00:00:54, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    New ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                6          2
    Keepalives:            54         54
    Route Refresh:          0          0
    Total:                 61         57
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0/0
  Output queue size : 0
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  2 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0
```

```
Event Timers (current time is 0x3390D4):
Timer          Starts    Wakeups            Next
Retrans            61          1             0x0
TimeWait            0          0             0x0
AckHold            58         55             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
ProcessQ            0          0             0x0

iss: 1945487142  snduna: 1945488934  sndnxt: 1945488934     sndwnd:  16308
irs: 1854611141  rcvnxt: 1854612453  rcvwnd:      16175  delrcvwnd:    209

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 44 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
IP Precedence value : 6

Datagrams (max data segment is 536 bytes):
Rcvd: 121 (out of order: 0), with data: 59, total data bytes: 1311
Sent: 119 (retransmit: 1, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 60, total data bytes: 1791
 Packets received in fast path: 0, fast processed: 0, slow path: 0
 fast lock acquisition failures: 0, slow path: 0

BGP neighbor is 3.3.3.2,  remote AS 65000, internal link
  BGP version 4, remote router ID 3.3.3.2
  BGP state = Established, up for 00:55:46
  Last read 00:00:48, last write 00:00:46, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    New ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised
    Address family VPNv4 Unicast: advertised and received
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  2 update-group member
  Community attribute sent to this neighbor
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              6          2 (Consumes 136 bytes)
    Prefixes Total:                6          2
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          2
    Used as multipath:           n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
  Number of NLRIs in the update sent: max 1, min 1

  Address tracking is enabled, the RIB does have a route to 3.3.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 2.2.2.2, Local port: 16820
Foreign host: 3.3.3.2, Foreign port: 179
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x350F7C):
Timer          Starts    Wakeups            Next
Retrans            64          2             0x0
TimeWait            0          0             0x0
AckHold            59         56             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
```

```
KeepAlive           0          0            0x0
GiveUp              0          0            0x0
PmtuAger            1          1            0x0
DeadWait            0          0            0x0
Linger              0          0            0x0
ProcessQ            0          0            0x0

iss: 2081068595  snduna: 2081070425  sndnxt: 2081070425     sndwnd:  16270
irs: 2339393609  rcvnxt: 2339394959  rcvwnd:      16137  delrcvwnd:    247

SRTT: 307 ms, RTTO: 348 ms, RTV: 41 ms, KRTT: 0 ms
minRTT: 72 ms, maxRTT: 360 ms, ACK hold: 200 ms
Status Flags: active open
Option Flags: nagle, path mtu capable
IP Precedence value : 6

Datagrams (max data segment is 536 bytes):
Rcvd: 125 (out of order: 0), with data: 60, total data bytes: 1349
Sent: 124 (retransmit: 2, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 62, total data bytes: 1829
 Packets received in fast path: 0, fast processed: 0, slow path: 0
 fast lock acquisition failures: 0, slow path: 0

BGP neighbor is 4.4.4.1,  remote AS 65000, internal link
  BGP version 4, remote router ID 4.4.4.1
  BGP state = Established, up for 00:57:41
  Last read 00:00:52, last write 00:00:46, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    New ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
```

```
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                6          2
    Keepalives:            57         57
    Route Refresh:          0          0
    Total:                 64         60
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0/0
  Output queue size : 0
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  2 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0

                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Total:                              0          0
  Number of NLRIs in the update sent: max 0, min 0

 For address family: VPNv4 Unicast
  BGP table version 7, neighbor version 7/0
  Output queue size : 0
```

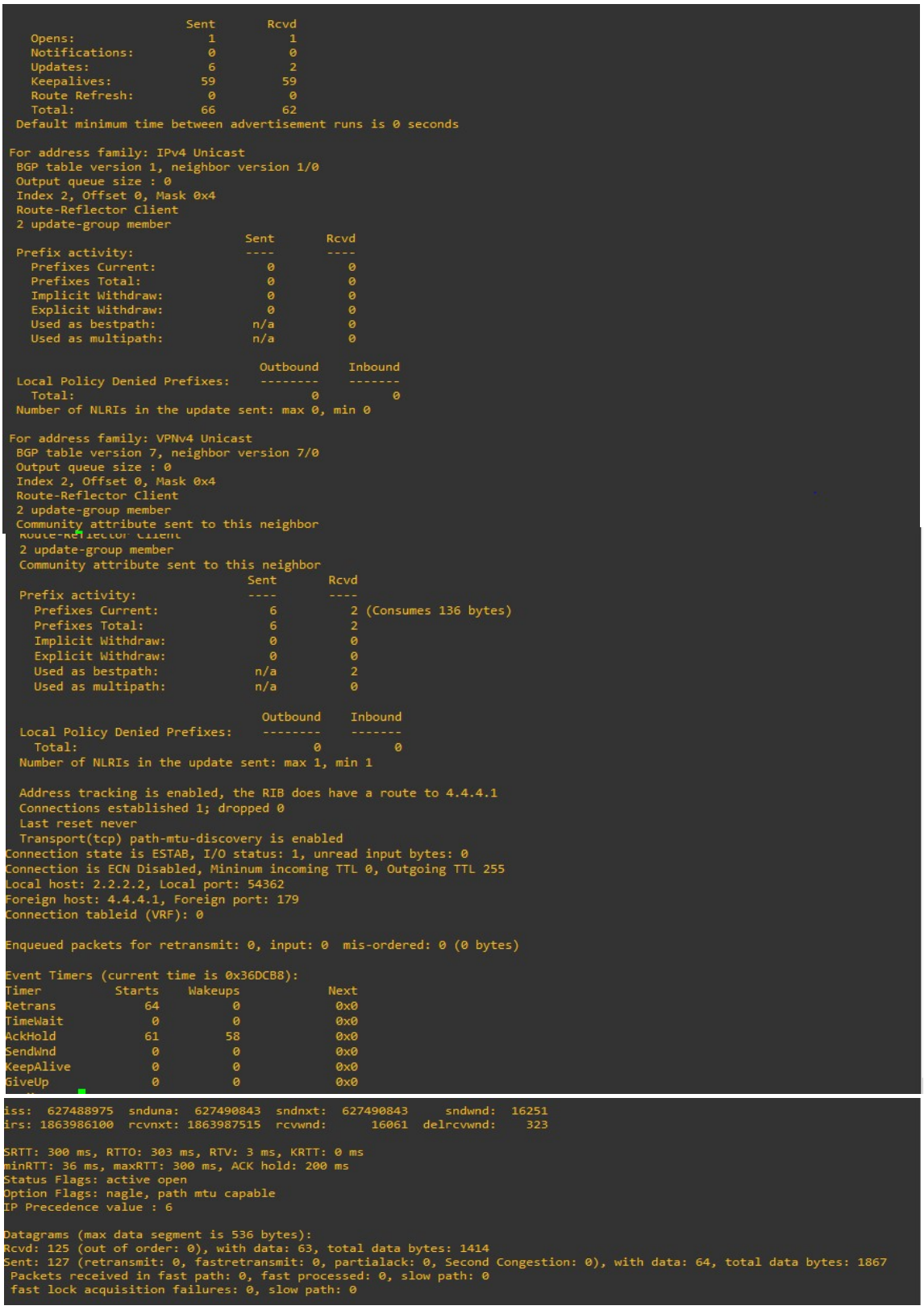

Fig. III.29: Trace route

Trace route est une commande utilisée pour suivre le chemin emprunté par les paquets de données à travers un réseau. Elle permet d'identifier les sauts (hops) successifs effectués par les paquets, en affichant les adresses IP des routeurs intermédiaires traversés. C'est un outil utile pour diagnostiquer les problèmes de connectivité et évaluer les performances du réseau.

Pour afficher une liste détaillée de toutes les routes unicast pour les adresses IPv4 apprises via BGP dans tous les VPN configurés sur l'appareil. « **Show bgp vpnv4 unicast all** » (p4) (Fig. III.30).

```
P4#show bgp vpnv4 unicast all
BGP table version is 1, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:1
* i4.4.4.2/32       3.3.3.1                  0    100      0 65001 i
Route Distinguisher: 65000:2
* i5.5.5.1/32       3.3.3.1                  0    100      0 65002 i
Route Distinguisher: 65000:3
* i5.5.5.2/32       3.3.3.2                  0    100      0 65003 i
* i6.6.6.2/32       4.4.4.1                  0    100      0 65005 i
Route Distinguisher: 65000:4
* i6.6.6.1/32       3.3.3.2                  0    100      0 65004 i
* i7.7.7.1/32       4.4.4.1                  0    100      0 65006 i
P4#
```

Fig. III.30 : Table de routage BGP VPNV4 Unicast

La table BGP VPNv4 Unicast contient les meilleures routes vers les préfixes de réseaux virtuels privés IPv4.

III.4.7.5 Vérification des VRF :

Vérification de configuration des VRF sur le routeur PE, avec la commande « show ip VRF».

```
PE1#show vrf
  Name                             Default RD          Protocols   Interfaces
  cust-1                           65000:1             ipv4        Fa0/0
  cust-2                           65000:2             ipv4        Fa0/1
PE1#
```

Fig. III.31 : Vérification des VRF pour PE

La vérification des VRF pour un routeur PE implique de s'assurer que les instances VRF sont correctement configurées et fonctionnelles sur le périphérique. Cela peut inclure la vérification des interfaces attribuées à chaque VRF, l'affichage des routes apprises dans chaque

instance VRF et la confirmation de la connectivité entre les réseaux appartenant à des VRF différents.

La commande « **ping adresse-destination source loopback 0** » est un outil précieux pour tester la connectivité réseau et isoler les problèmes de réseau locaux (Fig. III.32).

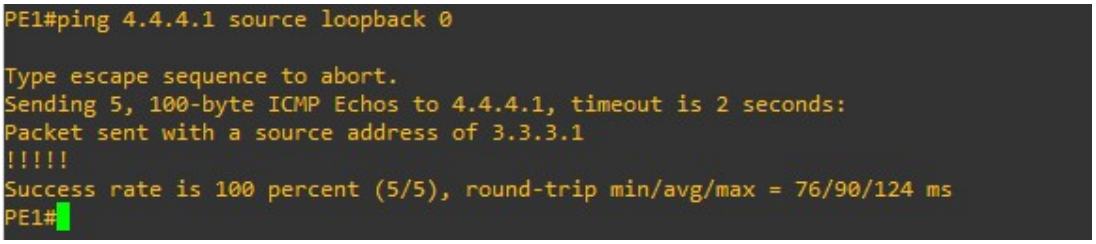

Fig. III.32 : Test de la connectivité

Effectuer des tests de connectivité pour vérifier la disponibilité des réseaux.

Pour tracer le chemin emprunté par les paquets d'un appareil source vers un appareil de destination sur un réseau IP. Elle aide à identifier les problèmes de réseau et les goulots d'étranglement potentiels en affichant les sauts intermédiaires (routeurs) que traversent les paquets le long du chemin en utilisant la command suivant :«**traceroute [options] adresse_source adresse_destination** » **(Fig. III.33).**

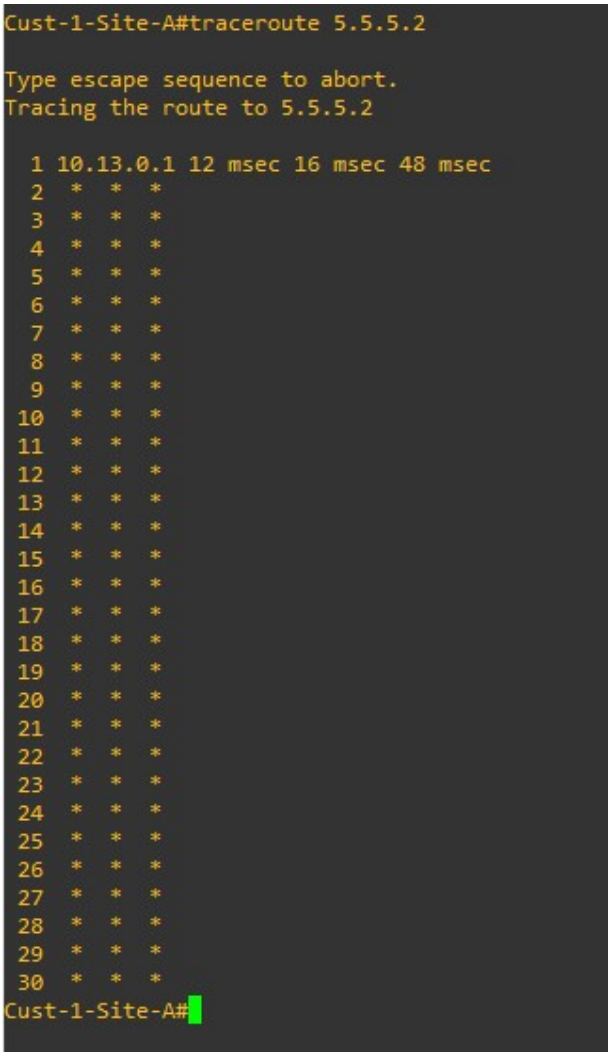

Fig. III.33 : Trace route Cust-1 vers Cust-3

Traceroute de Cust-1 vers Cust-3 permet d'analyser le chemin parcouru par les paquets de données entre ces deux clients, offrant ainsi une visibilité détaillée sur les sauts intermédiaires et les délais rencontrés

III.4.8 optimisation de la maquette par traffic engineering :

On passe en mode OSPF et on active l'ingénierie de trafic MPLS pour la zone OSPF 0, puis on spécifie l'identifiant du routeur d'ingénierie du trafic pour que le nœud soit l'adresse IP du Loopback (Fig. III.34).

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#router ospf 1
PE1(config-router)#mpls tra
PE1(config-router)#mpls traffic-eng area 0
PE1(config-router)#mpls tra
PE1(config-router)#mpls traffic-eng router
PE1(config-router)#mpls traffic-eng router-id loo
PE1(config-router)#mpls traffic-eng router-id loopback 0
PE1(config-router)#exit
PE1(config)#exit
PE1#
```

Fig. III.34 : Configuration d'Ospf pour TE

La configuration OSPF pour TE implique l'activation des extensions Traffic Engineering (TE) dans le protocole OSPF. Cela permet d'optimiser le routage en prenant en compte des métriques supplémentaires telles que la bande passante disponible, la latence, ou d'autres critères de qualité de service (QoS) pour le trafic réseau.

III.4.8.1 Création des tunnels

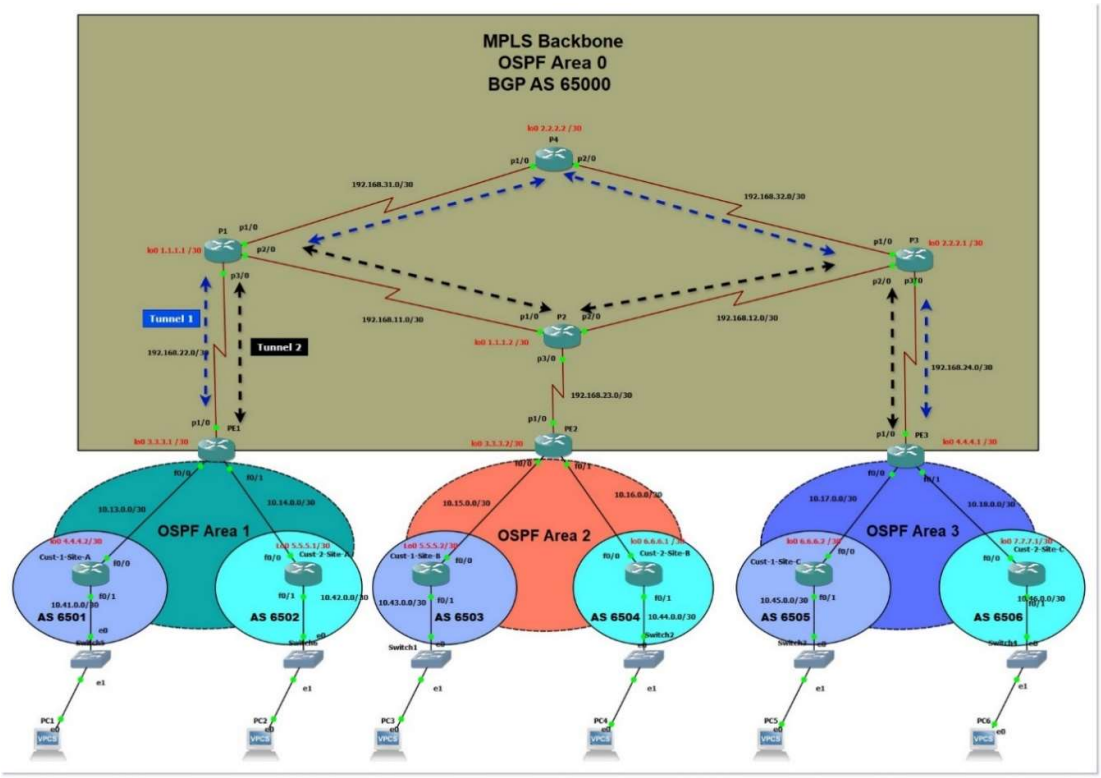

Fig. III.35 : Schéma illustrant la mise en place des tunnels (t1, t2)

Des tunnels seront mis en place entre les routeurs PE1. On a choisi de créer un tunnel pour la voix/vidéo et un tunnel pour le téléchargement. Pour cela, On commence par créer une interface de tunnel sur les routeurs PE, et on lui accorde une adresse IP de Loopback, cette interface est non numéroté car elle représente un lien unidirectionnel. On fixe la destination par la commande « **tunnel destination *ip-adress*** » et on définit le mode d'encapsulation du tunnel à l'ingénierie de trafic MPLS par la commande « **tunnel mode mpls traffic-eng** ». Ensuite, on utilise la commande « **tunnel mpls traffic-eng autoroute announce** » qui permet à l'IGP d'utiliser le tunnel dans son calcul du chemin le plus court. On passe à la priorité de configuration et de maintenance des tunnels par la commande « **tunnel mpls traffic-eng priority** ».

Il y a 8 priorités d'installation et de maintien allant de 0 à 7.0 est le plus préféré, le 7 est le moins (par défaut). La configuration la plus courante consiste à définir la même valeur pour la priorité et le maintien (Tableau III.3).

Table III.3 : Valeur de priorité IP

Valeur	Description
0	Routine or Best Effort
1	Priority
2	Immediate
3	Flash (mainly used for voice signaling or for video)
4	Flash Override
5	Critical (mainly used for voice RTP)
6	Internet
7	Network

La bande passante du tunnel sera déterminée par la commande **« tunnel mpls traffic-eng bandwidth** bandwidth », et le nom du tunnel par la commande *«* **tunnel mpls traffic-eng path-option 1 explicit name name** » (Fig. III.35).

```
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 4.4.4.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 3 3
 tunnel mpls traffic-eng bandwidth 1024
 tunnel mpls traffic-eng path-option 1 explicit name t1
```

Fig. III.36 : Création du Tunnel 1 "t1"

Créer le tunnel 1 (t1) implique de configurer une liaison point à point entre deux périphériques réseau.

```
interface Tunnel2
 ip unnumbered Loopback0
 tunnel destination 4.4.4.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng bandwidth 512
 tunnel mpls traffic-eng path-option 1 explicit name t2
```

Fig. III.37 : Création du Tunnel 2"t2"

Création du tunnel 2 (t2) pour établir une connexion sécurisée et dédiée entre deux points du réseau.

III.4.8.2 Configuration des interfaces :

On précède maintenant à la configuration dès l'interfaces qui supportte la signalisation du tunnel. Pour cela, On active la fonctionnalité de tunnel d'ingénierie de trafic MPLS sur une interface par la commande « **mpls traffic-eng tunnels** », puis on spécifie la quantité de bande passante à réserver sur RSVP par la commande « **ip rsvp bandwidth bandwidth** ».

```
interface FastEthernet0/0
 vrf forwarding cust-1
 ip address 10.13.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 vrf forwarding cust-2
 ip address 10.14.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface POS1/0
 ip address 192.168.22.2 255.255.255.252
 mpls traffic-eng tunnels
 service-policy input in-policy
 ip rsvp bandwidth 2048
```

Fig. III.38: Configuration de l'interface supportant MPLS-TE

Configurer l'interface pour prendre en charge MPLS-TE implique d'activer les fonctionnalités nécessaires sur l'interface pour permettre le trafic étiqueté à être acheminé selon les contraintes de trafic spécifiées par le TE (Traffic Engineering).

III.4.8.3 Vérification de la configuration des tunnels :

La commande utilisée pour visualiser les TE-tunnels sur les routeurs PE1, et PE3 est « **show *MPLS traffic-eng tunnels brief*** »(Fig. III.38) :

```
PE1#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 1571 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 71 seconds
TUNNEL NAME                     DESTINATION     UP IF     DOWN IF   STATE/PROT
PE1_t1                          4.4.4.1         -         PO1/0     up/up
PE1_t2                          4.4.4.1         -         PO1/0     up/up
PE3_t1                          3.3.3.1         PO1/0     -         up/up
PE3_t2                          3.3.3.1         PO1/0     -         up/up
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 2 (of 2) tails
PE1#
```

Fig. III.39: Visualisation des tunnels sur PE1

Visualiser les tunnels sur PE1 permet de surveiller et de gérer les connexions MPLS-TE établies sur ce périphérique, offrant ainsi une visibilité sur les chemins de trafic configurés et leur état actuel.

```
PE2#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 1396 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 196 seconds
Displayed 0 (of 0) heads, 0 (of 0) midpoints, 0 (of 0) tails
PE2#
```

Fig. III.40 : Visualisation des tunnels sur PE2

Visualiser les tunnels sur PE2 permet de surveiller les connexions MPLS-TE établies sur ce périphérique, offrant une visibilité sur les chemins de trafic configurés et leur état actuel.

► **Test des connectivite entre les PE routeurs:**

La figure III.34 montre que la connectivité entre PE1 et PE3 et bien établie

On refait ce test de connectivite entre la différent port du réseau cœur

On effectue un Ping entre le routeur PE1 et les deux autre routeurs PE2 et PE3 (Fig. III.40):

```
PE1#ping 4.4.4.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/91/156 ms
```

Fig. III.41: Ping entre le routeur PE-DP et les routeurs PE1

Effectuer un ping entre le routeur PE-DP et les routeurs PE1 permet de vérifier la connectivité entre ces périphériques, ce qui est essentiel pour assurer le bon fonctionnement du réseau MPLS.

► **Capture de trafic avec le logiciel Wireshark :**

On montre que le protocole RSVP a bien été implémenté, pour cela on prend une capture du trafic avec Wireshark (Fig. III.40).

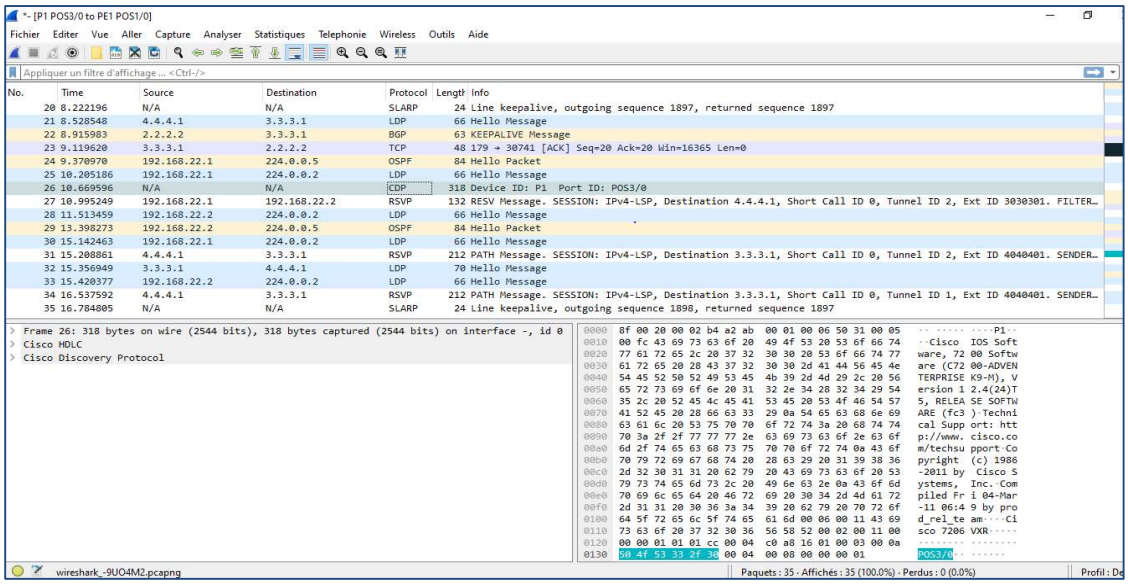

Fig. III.42: Capture de trafic par Wireshark

Commentaire sur **Fig. III.42** :

Capturer du trafic avec Wireshark permet d'analyser le flux de données circulant à travers un réseau, offrant ainsi une visibilité détaillée sur les paquets échangés entre les périphériques et les protocoles utilisés

III.5 Optimisation et implémentation de la qualité de service (QoS)

La classification du trafic permet de catégoriser les différentes données ou flux en fonction des critères imposés par les utilisateurs ou clients MPLS. Pour poursuivre dans l'optimisation de notre déploiement de la technologie MPLS, nous avons créé deux classes de services que

nous avons associés à deux types de flux que nous allons présenter. Pour l'implémentation de la QoS, on suit trois grandes étapes à savoir :

- La classification du trafic basée sur les critères définis par l'utilisateur
- La configuration des stratégies de la QoS pour chacune des catégories définies
- L'association des stratégies /ou d'une stratégie de QoS à une interface.

III.5.1 Configuration basic :

III.5.1.1 Création des class-map

Pour la configuration du QoS, on commence par créer une classe spécifiée pour lui faire correspondre le trafic lié aux critères donnés par l'utilisateur par valeurs de paquets EXP. Cela permet de définir des stratégies de service pour contrôler le trafic EXP par interface en utilisant la commande de la stratégie.

On entre dans le mode de configuration de la classe en spécifiant son nom par la commande « **class-map match-all** *name-class* », cette commande est cependant utilisée lorsque tous les critères d'une classe doivent être remplis pour un paquet, pour faire la correspondance avec la classe du trafic spécifié.

Par la suite, on fait correspondre les paquets à des valeurs dscp par la commande « **match ip dscp** *value* » qui permet de configurer les critères pour une classe basée sur la valeur du champ DSCP, on peut combiner dans une seule déclaration match jusqu'à huit valeurs DSCP qui sont montrés dans (le tableau III.4).

Table III.4 : Valeurs DSCP

Classes	DSCP	EXP	Description
Reserved for control plane trafic	Class Selector 7	7	Routine or Best Effort
Reserved for control plane traffic	Class Selector 6	6	Priority
Class 1 (real-time traffic)	EF	5	Immediate
Class 2 in-profile	AF31	4	Flash (mainly used for voice signaling or for video)
Class 2 out-of-profile	AF32, AF33	3	Flash Override
Class 3 in-profile	AF11	2	Critical (mainly used for voice RTP)
Class 3 out-of-profile	AF12, AF13	1	Internet
Class 4 (best effort)	Default	0	Network

On crée deux classes, la première correspond à la voix/vidéo, on la nomme « Voix-Vid » et on lui affecte les valeurs correspondant au DSCP de la voix/vidéo « af32 af33 ». La deuxième classe nommée « telchrg » correspond aux téléchargements, on lui affecte la valeur du téléchargement « AF ». (**Fig. III.43)**

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#class
*May 25 22:55:45.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
PE1(config)#class
PE1(config)#class-map match
*May 25 22:55:59.555: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Up
PE1(config)#class-map match-all voix-video
PE1(config-cmap)#match ip dscp af32 af33
PE1(config-cmap)#class-map match-all telechargement
PE1(config-cmap)#match ip dscp ef
PE1(config-cmap)#exit
PE1(config)#
```

Fig. III.43: Création des Class-map

Créer des class-maps permet de classifier le trafic réseau en fonction de différents critères, tels que les adresses IP source ou destination, les protocoles utilisés, ou d'autres attributs, afin de pouvoir appliquer des politiques de QoS ou de sécurité spécifiques à ces classes de trafic.

III.5.1.2 Création des policy-map :

On configure une stratégie avant de l'assigner à une classe de trafic particulière en introduisant la commande « **policy-map** *policy-name*», puis on passe en mode de configuration des classes et on introduit enfin la valeur du champ MPLS EXP sur toutes les entrées d'étiquette imposées sur l'interface de sortie. (**Fig. III.44**) :

```
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#policy-map in-policy
PE1(config-pmap)#class voix-video
PE1(config-pmap-c)#set mpls experimental 3
PE1(config-pmap-c)#class telechargement
PE1(config-pmap-c)#set mpls experimental 5
PE1(config-pmap-c)#exit
PE1(config-pmap)#
```

Fig. III.44: Création des Policy-map

La création de policy-maps permet de définir des politiques de traitement du trafic basées sur les class-maps préalablement configurées. Ces politiques peuvent inclure des actions telles que la priorisation, la limitation de bande passante, ou la mise en forme du trafic pour répondre aux exigences de qualité de service (QoS) ou de sécurité du réseau.

III.5.1.3 Configuration des interfaces :

On sélectionne l'interface ayant un lien Ethernet (E1) à configurer, dans notre cas c'est l'interface E1 lié au routeur PE-HMD, on lui introduit l'adresse IP et le masque approprié, puis on associe la policy-map aux paquets entarant à l'interface en tant que politique de service d'entrée par la commande « **service-policy input** *policy_map_name* ».

```
P1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
P1(config)#inter
P1(config)#interface p1/0
P1(config-if)#ip add
P1(config-if)#ip address 198.168.31.1 255.255.255.252
P1(config-if)#no
*Jun  4 10:53:05.851: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on POS1/0 from FULL to DOWN, Neighbor Down: Interface down or d
etached
*Jun  4 10:53:05.959: %LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (3) is DOWN (LDP disabled on interface)
P1(config-if)#no shu
P1(config-if)#no shutdown
```

Fig. III.45 : Configuration de l'interface

Configurer l'interface implique de définir ses paramètres opérationnels, tels que l'adresse IP, le masque de sous-réseau, la vitesse et le mode duplex, ainsi que d'autres options telles que la configuration de la sécurité et des politiques de routage.

III.5.2 Configuration personnalisée

III.5.2.1 Configuration des class-map et des interfaces

La configuration des class-map et des interfaces est exactement la même que dans la configuration basic.

III.5.2.2 Configuration des policy-map personnalisée

On introduit la stratégie en spécifiant que les paquets d'une classe de trafic devraient avoir un taux imposé en bits par seconde, un taux normal en bits par seconde, et un taux maximum en bits par seconde. Les paquets conforme à l'un des taux sont marqués par la valeur du champ MPLS EXP et sont transmis, si ce taux est dépassé, une action immédiate doit être prise comme l'action « drop » qui ne prendra pas le paquet en compte.

La configuration de la policy-map des deux classes voix-ved et telchrg se fait par la commande « **police** bits_per_second [normal_burst_bytes] **conform-action set-mpls-exp-transmit** *exp_value* **exceed-action drop »**

III.4.2.3.4 Vérification de la cofiguration :

On utilise la commande « show policy-map interface X » pour vérifier la stratégie crée sur le routeur PE1 et inséré sur l'interface Gigabits :

```
PE1#show policy-map interface P1/0
 POS1/0

  Service-policy input: in-policy

    Class-map: voix-video (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af32 (28) af33 (30)
      QoS Set
        mpls experimental imposition 3
          Packets marked 0
      police:
          cir 6000000 bps, bc 1000000 bytes, be 1500 bytes
        conformed 0 packets, 0 bytes; actions:
          set-mpls-exp-transmit 3
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: telechargement (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp ef (46)
      QoS Set
        mpls experimental imposition 5
          Packets marked 0
```

Fig. III.46 : Vérification de la stratégie « policy-map » sur le routeur PE1

La vérification de la stratégie "policy-map" sur le routeur PE1 permet de s'assurer que les politiques de traitement du trafic définies dans la "policy-map" sont correctement appliquées à l'interface spécifiée, garantissant ainsi le respect des règles de qualité de service (QoS) ou de sécurité définie dans la stratégie.

III.5 Conclusion

Ce chapitre avait pour but d'optimiser le réseau WAN et améliorer ce dernier par l'implémentation du Traffic-Engineering et la Qualité de service.

La nouvelle architecture offre une QoS nettement meilleure. Le Traffic Engineering améliore la rentabilité du réseau et facilite sa tâche d'administration et sa gestion.

Conclusion générale

Nous avons traité tout au long de ce projet la technologie de communication de type IP/MPLS, avec optimisation par le mécanisme d'ingénierie de trafic et de qualité de services. Notre contribution a commencé par la présentation d'une nouvelle approche des réseaux de nouvelle génération qui doit être mise en place pour permettre une planification et une gestion efficace des ressources dans le but de garantir, de manière continue, la qualité de services tout en minimisant les coûts résultants.

MPLS est donc une technologie qui a su prendre une place prépondérante dans les réseaux longue distance opérateurs. Son but premier, qui était d'optimiser le temps de traitement des paquets au sein du cœur de réseau s'est peu à peu effacé pour laisser placer aux extensions et applications du MPLS.

De nos jours, les quantités de données transportées sur les réseaux sont de plus en plus importantes, et le routage IP actuel ne satisfait pas aux contraintes qui sont désormais de l'ordre de la bande passante et du temps de transmission. MPLS offre indéniablement plusieurs services intéressants à exploiter, et ne nécessite pas forcément d'investissement conséquent lors de sa mise en place. Le développement des technologies à contrainte temporelle telles que la VoIP ou les applications vidéo, sont de plus en plus fréquentes, et requièrent l'utilisation d'un réseau pouvant respecter ces besoins.

Le réseau MPLS qui était créé en besoin de satisfaire la taille des cœurs de réseau des fournisseurs et conçus aussi pour améliorer la gestion du réseau et la qualité de service. A ouvert la porte pour d'autre technologies comme la virtualisation et le cloud computing pour additionner d'autres avantages et en plus facilite la gestion des réseaux de grande taille et donne aux administrateurs de réseau une possibilité de gérée leur réseau à distance.

La technologie SDN (Software Defined Networking) répond à ces besoins et ces objectifs. Le SDN est une approche centralisant la gestion du réseau en établissant le découplage des éléments matériels et des éléments logiciels. Il permet aux ingénieurs d'orchestrer et d'automatiser un réseau informatique sans devoir accéder physiquement aux composants matériels (Routeurs, switchs…etc.).

Enfin, cette expérience nous a permis d'explorer nos connaissances théoriques acquises à l'Université des Science et de la Technologie Mhamed bouguerra durant les deux dernières années.

Au terme de ce projet, nous avons approfondi nos connaissances dans le domaine des réseaux et particulier les réseaux cœurs, nous maitrisons l'outil de simulation GNS3, et les étapes de configuration de créations des VPN.

Aussi nous avons utilisé des techniques d'optimisation des réseaux cœurs. A savoir le TE et la Qos. A la fin de ce projet, et après l'analyse des résultats de configurations on peut dire que les résultats sont satisfaisants et le cahier de charge été satisfaisant.

BIBLIOGRAPHIE

[1] L'évolution du cœur de réseau des opérateurs fixes, par le cabinet Ovum pour le compte de l'Autorité de régulation des Communications électroniques et des Postes, Etude ARCEP, Janvier 2006. https://www.arcep.fr/uploads/tx_gspublication/etd-ovum-ngn-0106.pdf

[2] Recommandation UIT-T Y.2001: Aperçu général des réseaux de prochaine génération. Décembre 2004. https://www.itu.int/rec/T-REC-Y.2001

[3] Site Web de l'UIT-T sur les NGN : https://www.itu.int/en/ITU/gsi/ngn/Pages/definition.aspx

[4] Livre blanc NGN d'Alcatel-Lucent : https://www.al-enterprise.com/

[5] Recommandation UIT-T Y.1303: Glossaire des termes de télécommunication pour les réseaux de prochaine génération (NGN), Février 2012. https://dictionnaire.reverso.net/francais-definition/non+valide

[6] Site Web de Techopedia : https://www.geeksforgeeks.org/classes-of-routing-protocols/

[7] G. Cisco, "Routing Protocols: How the Internet Works", 2005.

[8] J. Doyle, "OSPF Network Design and Implementation" 2012.

[9] RFC 2328 : Définition du protocole OSPFv2, Document par IETF (Internet Engineering Task Force) : https://www.ietf.org/rfc/rfc2328.txt

[10] J. Saladi, "BGP Network Engineering", 2014.

[11] S. Vixie "BGP Internals: Understanding the Routing Protocol for the Internet",2012.

[12] D. Katz et D. Green, "MPLS: The Complete Guide to Multiprotocol Label Switching", 2016.

[13] W. Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", 2011.

[14] J. Palmer, "MPLS Fundamentals", 2011.

[15] W. Stallings, "High-Performance Networking: Traffic Engineering and QoS", 2017.

[16] J. Crowcroft et al., "Quality of Service for Next Generation Networks", 2012.

[17] Network World "Traffic Engineering and QoS: A Comprehensive Guide". https://www.networkworld.com/

Annexe

Présentation de l'organisme d'accueil :

L'Agence Nationale de Valorisation des Ressources en Hydrocarbures « ALNAFT » a été créée en vertu des dispositions de l'article 12 de la loi algérienne n°05-07 du 28 avril 2005 relative aux hydrocarbures, modifiée et complétée, L'Agence ALNAFT est administrée par une Direction Comité composé de six (6) membres dont un président.

Un secrétaire général est nommé pour l'agence ALNAFT pour assister le président du comité de direction dans l'administration et le fonctionnement de l'agence. L'agence ALNAFT dispose d'un Conseil de Surveillance, composé de cinq (5) membres, choisis pour leur expertise dans les domaines technique, économique et juridique du domaine des hydrocarbures.

Le conseil de surveillance assure le suivi et le contrôle de l'exercice des missions de l'agence ALNAFT. A ce titre, il est notamment chargé d'approuver la stratégie, les plans, le budget et le rapport des réalisations de l'Agence ALNAFT :

Missions

- Promouvoir les investissements dans la recherche et l'exploitation des hydrocarbures dans le domaine minier national ;
- Évaluer le secteur minier relatif aux activités en amont, notamment en réalisant des études de bassin et en acquérant des données ;
- Contrôler les activités de prospection, de recherche et d'exploitation des hydrocarbures ;
- Contrôler le respect de la conservation du gisement dans le cadre de l'exploitation des hydrocarbures ;
- Maintenir et mettre à jour un état des réserves d'hydrocarbures ;
- Gérer et préserver le patrimoine des données de recherche et développement sur les hydrocarbures ;
- Assurer la promotion du contenu local dans le cadre des activités en amont.
- Délivrer les certificats de préqualification des personnes et des opérateurs amont,

- Approuver les plans de développement et leurs mises à jour périodiques,
- Encourager les activités de recherche scientifique dans le domaine des activités amont.

Vision

- Promouvoir les activités de recherche et d'exploitation dans le secteur national de l'exploitation des hydrocarbures ;
- Maintenir une dynamique dans le secteur pétrolier amont ;

Valeurs

- Excellence, Transparence et Intégrité ;
- Ecouter et accompagner nos partenaires ;
- Autorité et responsabilité ;