الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière : Télécommunications

Spécialité : Réseaux & Télécommunications

Présenté par :

TEBBAL WIDAD

RT17

VPN IPSec multipoint dynamiques (Utilisation de GRE Multipoint/NHRP pour étendre les VPN IPsec)

Promoteur : Mme AMIROUCHE Nesrine

Co-promoteur : Mr Boughera abderrahim

Année Universitaire 2024-2025

Remerciement

En premier lieu, je remercie Dieu Tout-Puissant pour Son succès et Son aide, sans lesquels ce travail n'aurait pas pu être achevé. Louange et gratitude Lui soient rendus pour Ses innombrables bienfaits.

J'adresse mes plus sincères remerciements et ma profonde gratitude à mes chers encadrants, Monsieur BOUGHERA ABDERRAHIM et Madame AMIROUCHE NESRINE, pour leurs grands efforts et leurs précieuses orientations tout au long de la réalisation de ce mémoire. Leur soutien et leurs connaissances ont eu un impact considérable sur le succès de ce travail.

J'exprime ma gratitude et mes remerciements aux membres honorables du jury pour avoir bien voulu évaluer ce travail, et pour le temps précieux qu'ils y ont consacré.

Pour conclure, je ne saurais oublier de présenter mes plus vifs remerciements et ma reconnaissance à mes chers parents et à mes chers frères et sœurs, pour leur soutien moral continu et leurs encouragements constants qui ont eu un impact profond sur mon parcours. Et enfin, je remercie toutes les personnes qui m'ont apporté leur aide et leur soutien, de près ou de loin, dans l'achèvement de ce mémoire.

Dédicace

Je dédie ce modeste travail à :

À mes très chers parents (TEBBAL DJAMALE ; OGABE HADJIRA), les mots ne suffisent pas pour exprimer l'étendue de ma gratitude et de mes profonds remerciements pour tous vos nobles sacrifices et votre soutien illimité qui m'a toujours enveloppé. Votre amour, votre dévouement et votre présence ont été un pilier essentiel à toutes les étapes de ma vie.

À mes chers frères, (ABDEL MADJID, ABDEL SATAR, ABDEL WADOUD, ABOUBAKER) et à mes deux sœurs bien-aimées, (ASMA, YOUSRA), ainsi qu'à tous les membres de ma grande famille, qui ont toujours été une source d'aide et de soutien, me prodiguant conseils, encouragements et un amour inépuisable.

À l'entreprise SONTRACH, j'adresse mes sincères remerciements et ma profonde gratitude pour m'avoir donné l'opportunité de réaliser ce travail dans un environnement professionnel, et pour le soutien et les précieuses facilités que vous avez offerts, qui ont enrichi mon expérience.

À tous mes amis sans exception, qui ont toujours été à mes côtés, semant l'espoir en moi et m'apportant soutien et encouragements, leur souhaitant un succès continu et durable.

Résumé

Ce mémoire examine la technologie DMVPN (Dynamic Multipoint VPN), une combinaison d'IPsec, mGRE et NHRP, qui facilite le déploiement de VPN IPsec fiables, sécurisés et évolutifs. Basée sur une architecture centralisée, la Cisco DMVPN prend en charge divers utilisateurs (mobiles, télétravailleurs, extranet) et intègre la Voix sur IP (VoIP) sans connexion VPN permanente, réduisant ainsi la latence et optimisant la bande passante.

Mon projet chez SONATRACH a démontré comment cette architecture a significativement amélioré la connectivité, la sécurité et l'optimisation des ressources pour les sites distants. Les résultats confirment l'efficacité de l'automatisation des tunnels IPsec via GRE multipoint et NHRP.

Cependant, malgré sa robustesse, le DMVPN présente des limites notables, notamment l'absence d'équilibrage de charge dynamique et de basculement instantané en cas de défaillance, des points forts des technologies plus récentes comme le SD-WAN.

Ce mémoire vise à offrir une vue d'ensemble de l'application pratique du DMVPN chez SONATRACH, en soulignant ses atouts et ses limites face aux solutions modernes, afin d'éclairer les entreprises dans l'optimisation de leur infrastructure réseau.

Mots-clés : DMVPN, IPsec, mGRE, NHRP, SONATRACH, VoIP, Équilibrage de charge, Basculement, SD-WAN, Infrastructure réseau.

Abstract

This paper examines DMVPN (Dynamic Multipoint VPN), an integrated set of technologies including IPsec, mGRE, and NHRP. This combination significantly streamlines VPN IPsec deployment, offering a reliable, secure, and scalable solution for flexible tunnel creation and management. Cisco DMVPN uses a centralized architecture and supports various users like mobile workers, teleworkers, and extranet users. It also enables Voice over IP (VoIP) between connected sites without requiring permanent VPN links, substantially reducing latency and jitter while optimizing bandwidth usage.

My project at SONATRACH clearly demonstrated how this architecture vastly improved connectivity, security, and resource utilization for the company's remote sites. The results confirmed the effectiveness of automating IPsec tunnel creation via GRE multipoint and NHRP.

However, despite its robustness, DMVPN faces notable challenges, primarily the lack of dynamic load balancing capabilities and instantaneous failover. These aspects are key strengths of newer technologies like SD-WAN.

This research aims to provide a comprehensive overview of DMVPN's practical application within an environment like SONATRACH, highlighting its advantages and limitations compared to modern solutions. The goal is to offer valuable insights to businesses seeking to optimize their network infrastructure.

Keywords: DMVPN, IPsec, mGRE, NHRP, SONATRACH, VoIP, Load Balancing, Failover, SD-WAN, Network Infrastructure.

ملخص

يتناول هذا البحث تقنية(DMVPN (Dynamic Multipoint VPN ، وهي مزيج من التقنيات المتكاملة IPsec :و mGRE و .NHRPيسهل هذا المزيج بشكل كبير نشر شبكات VPN IPsec الموثوقة والآمنة والقابلة للتطوير. تعتمد Cisco DMVPN على بنية مركزية وتدعم مختلف المستخدمين (المتنقلين، عن بُعد، الشبكات الخارجية) وتدمج الصوت عبر IP (VoIP) دون الحاجة لاتصال VPN دائم، مما يقلل زمن الاستجابة ويحسن عرض النطاق الترددي.

لقد أظهر مشروعي في سوناطراك كيف ساهمت هذه البنية في تحسين الاتصال والأمان واستخدام الموارد للمواقع البعيدة بشكل كبير. تؤكد النتائج فعالية أتمتة أنفاق IPsec عبر GRE multipoint و.NHRP

لكن، على الرغم من قوتها، تواجه DMVPN تحديات بارزة، أبرزها غياب موازنة التحميل الديناميكية والتحويل الفوري عند الفشل، وهي نقاط قوة كبيرة للتقنيات الأحدث مثل.SD-WAN

يهدف هذا البحث إلى تقديم لمحة عامة عن التطبيق العملي لـ DMVPN في بيئة مثل سوناطراك، مسلطًا الضوء على مزاياها وقيودها مقارنة بالحلول الحديثة، وذلك لتزويد الشركات بمعلومات قيمة لتحسين بنيتها التحتية للشبكات.

الكلمات الرئيسيةDMVPN ، IPsec، mGRE، NHRP، SONATRACH، VoIP، موازنة التحميل، الفشل، SD-WAN، البنية التحتية للشبكة.

Sommaire

Chapitre IV : VPN IPSec multipoint dynamiques

Chapitre V : Implémentation du la maquette

Table des figures

Introduction Générale

Les réseaux informatiques modernes font face à des défis de sécurité croissants, notamment avec l'expansion de la connectivité et le besoin des entreprises, comme SONATRACH, d'interconnecter leurs sites multiples de manière sécurisée et efficace. Si les solutions de couche 2 telles que RNIS et Frame Relay étaient utilisées par le passé, elles s'avéraient coûteuses et complexes à déployer.

L'adoption d'Internet et l'utilisation de tunnels IPsec pour garantir l'authentification, l'intégrité des données et la confidentialité sont devenues essentielles. Cependant, les solutions VPN IPsec traditionnelles présentent des limites claires en termes de maintenance et d'évolutivité ; chaque nouvel ajout de site entraîne des modifications de configuration complexes, une difficulté qui s'accentue considérablement dans les réseaux entièrement maillés.

SONATRACH dispose d'un réseau de données à couverture nationale de type SH-WAN comportant des routeurs de marque de gamme qui permettent les services d'acheminement TCP/IP et supportent plusieurs protocoles de la couche liaison IPv4/IPv6, ainsi que les protocoles de routage EIGRP, OSPF, BGP.

Pour la sécurité, ces routeurs permettent l'implémentation des ACL, NAT et VPN.

Les liens sont en fibre optique avec des redondances, mais aussi avec des liaisons de secours via VSAT en cas de nécessité ou encore via des VPN dynamiques (DMVPN), ce qui est l'objet de notre travail

Le problème qui se pose est : Comment pouvons-nous construire un réseau VPN sécurisé, multipoint et dynamique qui s'adapte aux exigences changeantes de la connectivité ?

Pour répondre à ces limites, le VPN multipoint dynamique (DMVPN) est apparu comme une solution avancée, combinant la sécurité d'IPsec, la flexibilité de GRE multipoint, et le dynamisme de NHRP.

Ce travail vise à proposer une solution open source à cette problématique. Le rapport est structuré comme suit :

- **Chapitre 1 :** Présentation de l'organisme d'accueil /Présentation de la SONATRACH

- **Chapitre 2 :** Généralités sur les réseaux informatiques

Nous présenterons une vue d'ensemble des fondamentaux des réseaux, incluant leurs types, leurs composants et leurs protocoles de base, afin d'établir une compréhension commune des concepts.

- **Chapitre 3 :** Les réseaux privés virtuels

Nous approfondirons le concept des réseaux privés virtuels (VPN), en expliquant leurs principes de fonctionnement, leurs différentes typologies, et les avantages sécuritaires qu'ils offrent.

- **Chapitre 4 :** VPN IPsec multipoint dynamiques

Nous explorerons en détail les techniques qui combinent IPsec avec GRE multipoint et NHRP. Nous expliquerons comment ces composants interagissent pour créer une solution VPN multipoint dynamique et discuterons des avantages qu'offre cette approche.

- **Chapitre 5 :** Implantation de la maquette

Dans ce chapitre, nous passerons de la théorie à la pratique. Nous décrirons les outils et les étapes concrètes que nous avons suivis pour concevoir et mettre en œuvre un réseau VPN sécurisé, multipoint et dynamique.

Cette implémentation a été réalisée en utilisant GNS3 (Graphical Network Simulator-3) dans un environnement Windows.

Ce chapitre vous fournira des directives détaillées sur la manière de configurer et de tester ce prototype, avec des exemples clairs pour garantir son bon fonctionnement et valider l'efficacité de notre solution.

Chapitre I : Présentation de l'organisme d'accueil

Introduction :

Notre projet de fin d'études s'est déroulé à « **SONATRACH** » « **Société Nationale pour la Recherche, la Production, le Transport, la Transformation, et la Commercialisation des Hydrocarbures** » cette société occupe une place incontournable dans l'économie de notre pays, pour bien comprendre le contexte de notre projet, nous donnerons dans ce chapitre une vue globale sur cette entreprise**,** sa structure, son objectif et ses diverses activités.

1. Présentation de la SONATRACH :

SONATRACH ; un acteur majeur de l'industrie pétrolière en Algérie et en Afrique créée en 1963 pour exploiter les ressources en hydrocarbures du pays. Elle se présente actuellement sous l'aspect d'une entreprise intégrée intervenant directement dans l'ensemble des activités du secteur des hydrocarbures.

Adoptant une stratégie de diversification, SONATRACH se développe dans les activités de génération électrique, d'énergies nouvelles et renouvelables, de dessalement d'eau de mer, de recherche et exploitation minière. Poursuivant sa stratégie d'internationalisation, SONATRACH opère en Algérie et plusieurs régions du monde : en Afrique (Mali, Niger, Libye, Egypte), en Europe (Espagne, Italie, Portugal, Grande Bretagne), En Amérique Latine (Pérou) et aux USA.

Avec un chiffre d'affaires à l'exportation de près de 56.1 milliards de US$ réalisé en 2010, SONATRACH est classée 1ère compagnie en Afrique et 12ème compagnie dans le monde. Elle est également 4ème exportateur mondial de GNL (Gaz Naturel Liquéfié), 3ème exportateur mondial de GPL, et 5ème exportateur de Gaz Naturel.

Ses activités de base sont **l'exploitation**, **la production, le transport par canalisation**, **les premières transformations, la commercialisation et la maintenance lourde**, représentant les activités de base. Elles sont considérées prioritaires, donc bénéficient d'une affectation prioritaire des ressources de l'entreprise.

2. Organigramme :

Voici ci-dessous l'organigramme qui représente la structure de l'entreprise :

- Le schéma de la macrostructure s'articule autour :
    - De la Direction Générale,
    - Des Activités Opérationnelles
    - Des Directions Fonctionnelles.

La Direction Générale du groupe est assurée pas un Président Directeur Général, assisté du Comité Exécutif.

Les Activités Opérationnelles exercent les métiers du groupe et développent son potentiel d'affaires tant en Algérie qu'en international.

Il s'agit de l'activité Exploration et Production (E&P), de l'Activité Aval (AVL), de l'activité Transport par Canalisation (TRC) et de l'Activité commercialisation (COM).

Les directions fonctionnelles élaborent les politiques et stratégies du groupe, et veillent à leur application. Elles fournissent l'expertise et l'appui nécessaires aux Activités Opérationnelles du groupe.

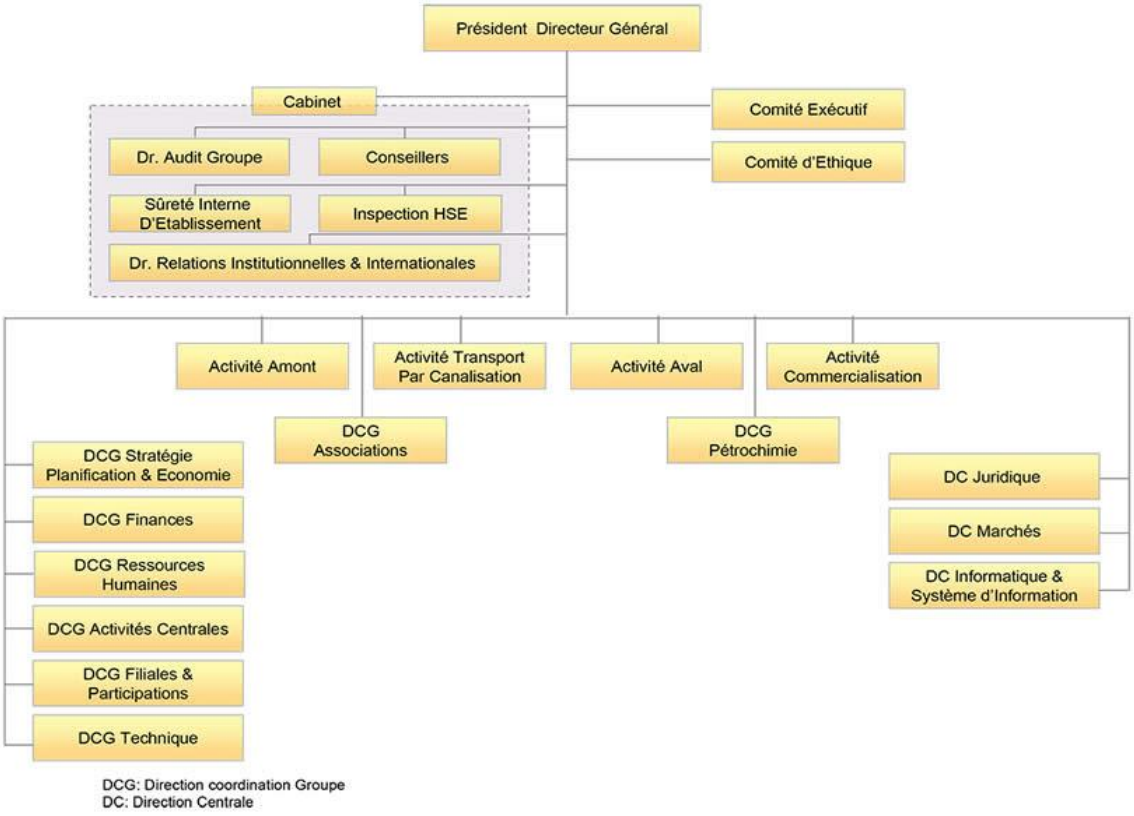

Figure 1.1 : Organigramme de la SONATRACH.

Pour notre étude, on intervient au sein de la division P.E.D « Petroleum Engineering & Développement » qui fait partie de l'activité E&P (ex- Amont).

3. Présentation de l'activité Exploration et Production :

L'activité Exploration et production (E&P) a en charge la recherche, l'exploration, l'exploitation et la production des hydrocarbures. Ses missions sont principalement axées sur le développement des gisements découverts, l'amélioration du taux de récupération et la mise à jour des réserves.

L'activité E&P est organisée en huit (8) divisions, dont la division PED.

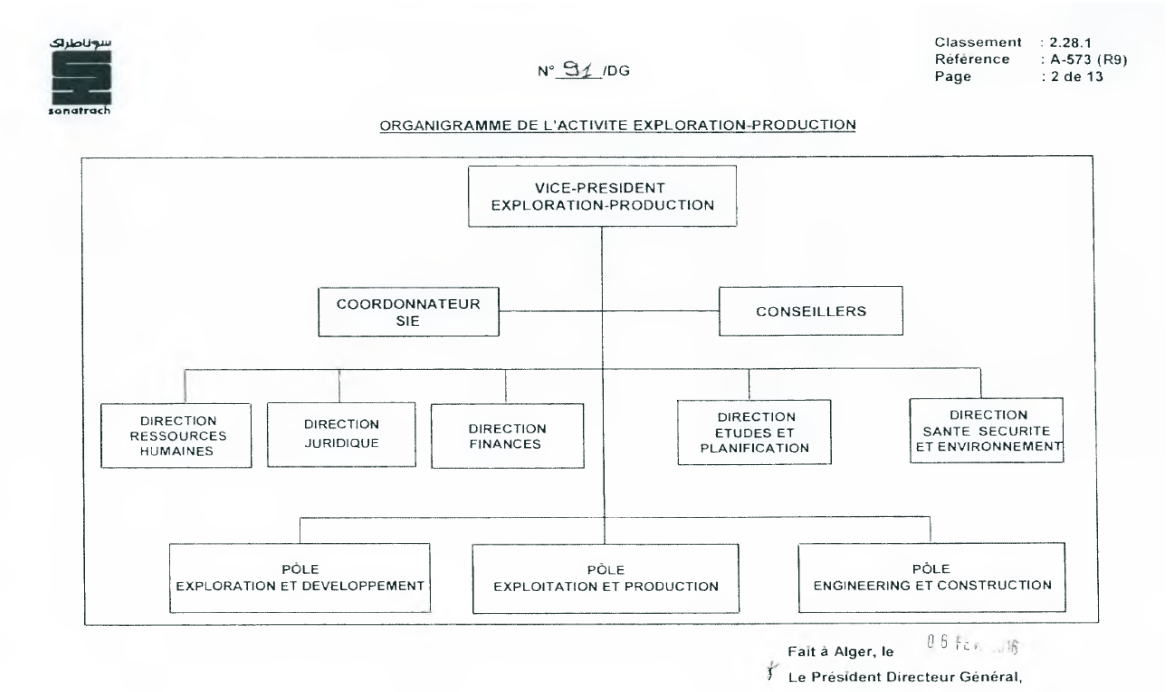

Figure 1.2 : Organigramme de la division Exploration– Production (ex- AMONT)

4. Présentation de la division production :

Orientation de la division production :

La division production (SH/DP) est organisée en un siège regroupant des directions à Alger et onze régions réparties dans le sud du pays.

Elle a pour mission le développement et l'exploitation des gisements d'hydrocarbures ainsi que l'optimisation de la production par l'utilisation des méthodes de récupération, l'entretien et la conservation des réserves en place.

La division production emploi actuellement plus de 16.000 agents répartis entre le siège et les régions et structures de :

Six (06) directions qui sont :

- Direction Finance et Comptabilité (DFC)
- Direction Ressources Humaines (DRH)
- Direction Opérations.
- Direction Approvisionnement et Transport (DAT)
- Direction Moyens Généraux (DMG)
- Direction Informatique (DINF)

Onze (11) directions régionales qui sont :

- Hassi- messaoud (HMD).
- Hassi- R'mel (HR).
- Haoud- Berkaoui (HBK).
- Gassi- Touil (GT).
- Ohanet (OHT).
- Stah (STH).
- In Aménas (INA).
- Rhoudes Nouss (RNS).
- Rhoudes El Baguel (BER).
- Tin Fouyé Tbankourt (TFT).
- Hors régions (Oued Guetteni + Djebel Onk).

Les activités de la division production « DP » :

Les activités de la division production consistent :

- Au développement et à l'exploitation des gisements d'hydrocarbures, situé dans leur quasi-totalité dans le Sud-Est de l'Algérie et qui sont actuellement au nombre de 66 gisements.
- A la production d'hydrocarbures liquides et gazeux (pétrole brut, condensat, GPL et Gaz).
- A l'exploitation et maintenance des installations et équipements de production d'hydrocarbures de pression des gisements.
- A la gestion et l'exploitation des raffineries de Hassi-Messaoud et d'Ain Amenas

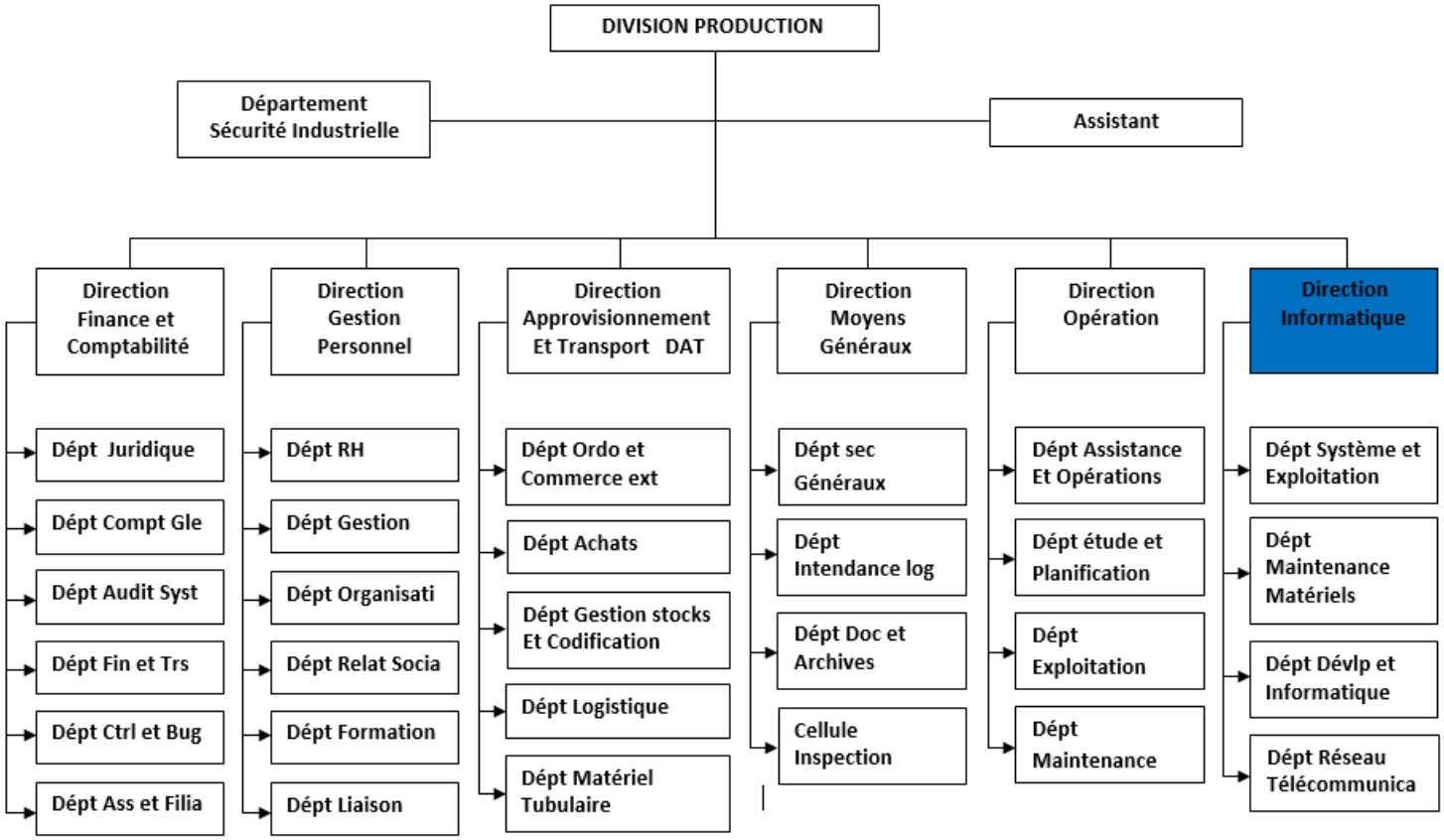

Figure 1.3 : Organigramme de la Division Production

5. Présentation de la division PED

Le rôle de la division PED (Petroleum Engineering et Développement) est de suivre et d'optimiser le développement et l'exploitation des gisements de pétrole qui se trouve dans le Sahara Algérien.

La Division PED est organisée en quatre (4) directions, chacune étant constituée de départements, et trois départements directement rattachés à la direction de la Division PED :

- La Direction « Gisements » dont le rôle est de définir les caractéristiques des réservoirs, telles que leurs limites et la quantité de pétrole qu'ils recèlent.
- La Direction « Développement » dont les ingénieurs de cette direction analysent les données obtenues par les différentes compagnies de service afin de déterminer les informations telles que les cotes de perforation, la saturation en eau, huile et gaz, la porosité et la perméabilité des roches…etc,

- La Direction « Techniques de Production » qui a pour objectif le suivi de comportement des réservoirs, l'établissement des prévisions annuelles de production, la détermination des installations de surface, la programmation des interventions sur puits ainsi que la production et la détermination des moyens de production.
- La Direction « Stratégie Planification & Reporting » dont l'objectif principal est la recherche et l'identification des opportunités de développement.
- Le Département « Gestion du Personnel » qui assure la gestion des ressources humaines du personnel PED.
- Le Département « Finances et Juridique » qui assure le suivi juridique et financier des contrats avec les prestataires.
- Le Département « Technologies de l'Information » qui assure le soutient à la Division PED en matière d'infrastructures et de systèmes informatiques.

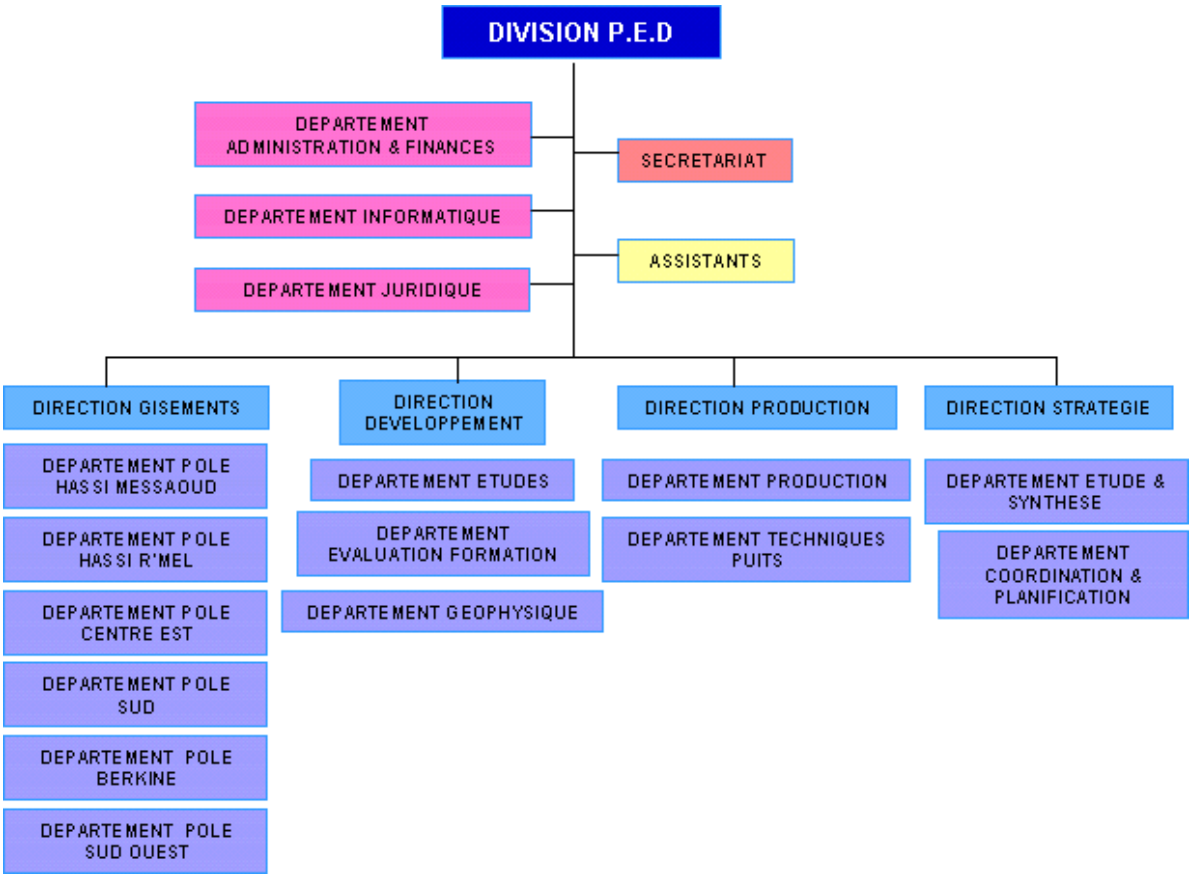

Figure 1.4 : Organigramme de la division P.E.D

6. Département informatique :

La division production a créé le département informatique au siège pour ses besoins informatiques.

Ce département contient quatre services :

- Service réseaux et télécommunications.
- Service systèmes et exploitations.
- Service maintenances.
- Service développement.

Le service réseaux a pour missions :

- Tout ce qui est branchement et maintenance des réseaux.
- L'intégration des microordinateurs des employés au réseau local de l'entreprise.
- La mise en place d'un réseau reliant les différents sites de la DP.
- La dotation d'un accès à internet à tous les utilisateurs de l'outil informatique.
- Conception du réseau.
- Evaluation de la charge du réseau.
- Contrôle des performances du réseau.
- Protection du réseau (sauvegarde, anti-virus, accès…)

Chapitre II : Généralité sur les réseaux informatiques

1. Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'équipements informatiques (ordinateurs, imprimantes, scanners etc.) reliées entre eux par des médias (câbles, Fibre optique, ……) pour échanger des informations et partager des ressources matériels et logiciels dans un certain domaine géographique.

Voici trois composants clés de la définition d'un réseau informatique : l'interconnexion, le partage de ressources et l'échange d'informations.

- **Interconnexion :** les appareils du réseau sont connectés à l'aide de divers moyens : câblage, fibres optiques, Wi-Fi et Bluetooth.
- **Partage de ressources :** dont l'objectif est de mettre des ressources à la disposition de plusieurs utilisateurs.
- **Échange d'informations entre les appareils :** accès total ou partiel au contenu et informations stockées sur les appareils du réseau.

Figure 2.1 : Réseau informatique [1]

2. Le modèle OSI :

OSI (Open Systems Interconnexion)

Pour faire circuler l'information sur un réseau on peut utiliser principalement deux stratégies. L'information est envoyée de façon complète ou l'information est fragmentée en petits morceaux (paquets).

La première stratégie base sur l'envoyer les informations de façon complète sur le réseau, cette stratégie n'est pas utilisée en raison de la complexité des erreurs de transmission et des problèmes sous-jacents. Ces erreurs sont difficiles à gérer et à corriger.

La deuxième stratégie, c'est la commutation de paquets, un système où les données sont divisées en petits paquets qui sont envoyés indépendamment sur un réseau. Ces paquets sont ensuite réassemblés à destination pour reconstruire l'information originale. Cette méthode permet une utilisation plus efficace de la bande passante et une meilleure résilience en cas de panne, car les paquets peuvent être acheminés par différents chemins.

Le modèle OSI est un modèle à 7 couches qui décrit le fonctionnement d'un réseau à commutations de paquets. Chacune des couches de ce modèle représente une catégorie de problème que l'on rencontre dans un réseau. Découper les problèmes en couche présente des avantages. Lorsque l'on met en place un réseau, il suffit de trouver une solution pour chacune des couches,

L'utilisation de couches permet également de changer de solution technique pour une couche sans pour autant être obligé de tout repenser, Chaque couche garantit à la couche qui lui est supérieur que le travail qui lui a été confié a été réalisé sans erreur.

Le modèle OSI mettre en place une architecture commun pour que chaque appareil, quelle que soit sa marque, puisse communiquer entre eux.

Le modèle OSI est divisé en 7 couches (7 layers)

Voici les 7 Couche du modèle OSI, de la couche la plus basse à la couche la plus haute :

1. Couche Physique (Physical Layer)
2. Couche Liaison de données (Data Link Layer)
3. Couche Réseau (Network Layer)
4. Couche Transport (Transport Layer)
5. Couche Session (Session Layer)
6. Couche Présentation (Présentation Layer)
7. Couche Application (Application Layer)

Le but de ce modèle est d'analyser la communication en découpant les différentes étapes en 7 couches chacune de ces couches remplissant une tache bien spécifique.

Les avantages de ce modèle sont :

- Une division de la communication réseau en éléments plus petits et plus simple pour une meilleure compréhension
- L'uniformisation des éléments afin de permettre le développement multi constructeur
- La possibilité de modifier un aspect de la communication réseau sans modifier le reste (Exemple : un nouveau média)

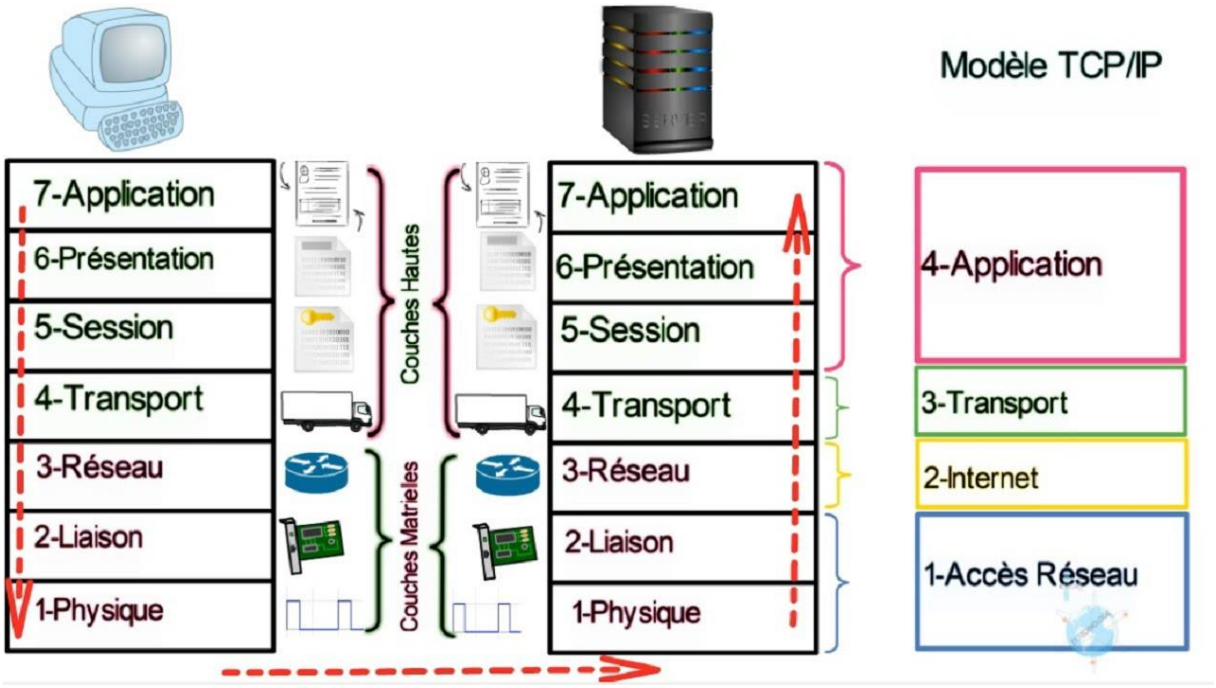

Figure 2.2 : Archetecture du standard OSI [2]

3. L'Adressage IP :

IP (Internet Protocol)

L'adresse IP est le processus d'attribution à des appareils connectés par un réseau de communications utilisant Internet Protocol des identifiants correspondants. Son objectif principal est la numérotation des appareils connectés en tant qu'ID final glue de route pour garantir que les paquets de données de base de connaissances atteignent leur destination physiologique.

Est un numéro unique attribué à chaque appareil connecté à un réseau informatique.

Versions d'adresses IP : il existe deux versions principales de protocole IP :

- ✓ **IPv4 :** (internet Protocol version 4) utilise 32 bites, 2^{32} =4,3 baléares d'adresse unique

Exprimées sous la forme de 4 nombres décimaux (octets) séparés par des points

Exemple : 192.168.1.1

- ✓ **IPv6 :** (internet Protocol version 6) utilise 128 bites, un nombre pratiquement illimité

Exprimées à 8groupe de 4 chiffres hexadécimaux sépares par deux-points

Exemple : 2001 : odb8 :85a3 :0000 :0000 :8a2e :0370 :7334

Une adresse IPv4 se compose de deux parties principales : l'ID de réseau et l'ID d'hôte. L'ID de réseau identifie le réseau auquel l'appareil est connecté, tandis que l'ID d'hôte identifie l'appareil spécifique sur ce réseau. La manière dont ces parties sont divisées dépendait autrefois de la classe de l'adresse IP (A, B, C, D et E), chaque classe ayant une taille de réseau et d'hôte différente.

Cependant, le CIDR (Classless Inter-Domain Routing) a largement remplacé ce système de classes.

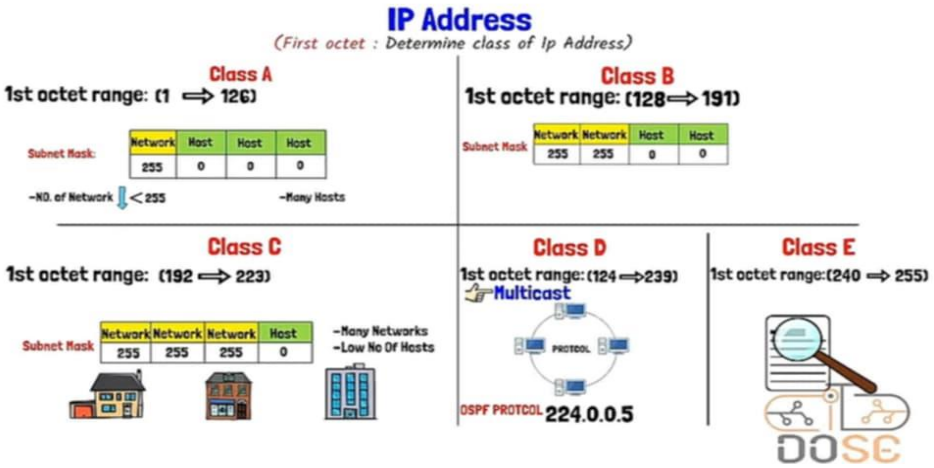

Figure 2.3 : Classes d'adresses IP [3]

CIDR et Masque de Sous-Réseau :

CIDR : permet une allocation plus flexible des adresses IP en utilisant une notation qui spécifie le nombre de bits utilisés pour l'ID de réseau à l'aide d'un suffixe (par exemple, 192.168.1.0/24). Le "/24" indique que les 24 premiers bits de l'adresse identifient le réseau.

Le masque de sous-réseau : est un nombre de 32 bits qui, lorsqu'il est combiné avec une adresse IP, détermine quelle partie de l'adresse identifie le réseau et quelle partie identifie l'hôte. En notation décimale pointée, un masque de sous-réseau correspondant à /24 serait 255.255.255.0. Les bits à '1' dans le masque correspondent à la partie réseau, et les bits à 'O' correspondent à la partie hôte.

Il existe deux types d'adresses IP : publiques et privées.

Les adresses IP publiques sont uniques au monde et servent à communiquer sur Internet. Elles sont attribuées par les fournisseurs d'accès à Internet (FAI).

Les adresses IP privées, quant à elles, sont réservées à l'usage interne des réseaux locaux (LAN) et ne sont pas routables sur Internet. Elles sont réparties en trois classes :

- ✓ Classe A : 10.0.0.0 - 10.255.255.255
- ✓ Classe B : 172.16.0.0 - 172.31.255.255
- ✓ Classe C : 192.168.0.0 - 192.168.255.255

Pour permettre aux appareils utilisant des adresses IP privées d'accéder à Internet, un mécanisme appelé NAT (Network Address Translation) est utilisé.

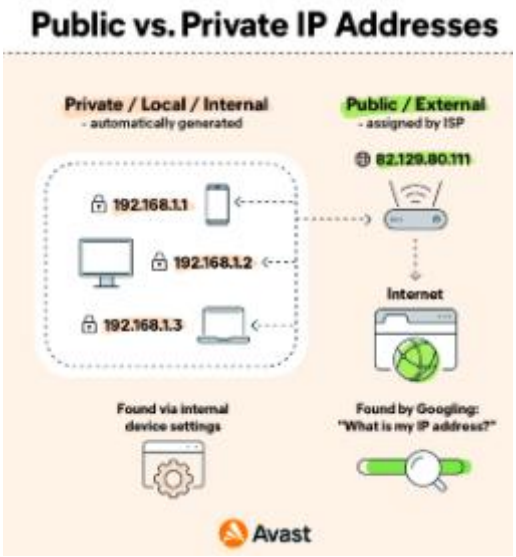

Figure 2.4: Public vs privet IP addres [4]

4. Les Topologies de Réseau :

C’est la maniéré dont les ordinateurs et les équipements du réseau sont reliés entre eux. Le choix de la topologie dépend de plusieurs facteurs, comme la taille du réseau, le budget, la fiabilité souhaitée et les performances attendues.

Il y'a trois topologies des réseaux informatiques qui sont les plus reconnus et les plus utilisés. [5]

4 .1. Topologie en BUS :

Dans cette topologie, toutes les stations sont connectées en série le long d'un seul câble désigné par Bus. **[5]**

Avantages : Simple à mettre en place et économique en termes de câblage.

Inconvénients : Si le câble principal tombe en panne, tout le réseau est hors service. Il est difficile d'identifier les problèmes et le trafic peut ralentir si de nombreux appareils sont connectés.

Cette topologie est de moins en moins utilisée.

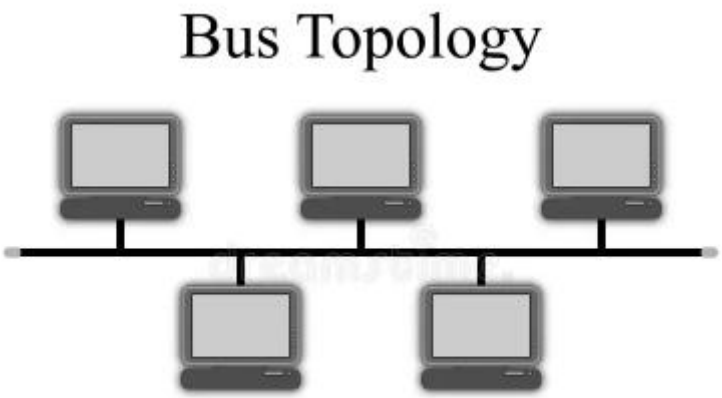

Figure 2.5 : Topologie en BUS [6]

4.2. Topologie en étoile :

Dans cette topologie, toutes les stations sont reliées à un nœud central HUB ou switch. **[5]**

Avantages : Facile à installer et à dépanner. La défaillance d'un appareil n'affecte pas le reste du réseau. Ajout et suppression d'appareils faciles. Gestion centralisée.

Inconvénients : Nécessite plus de câblage que la topologie en bus. Si le nœud central tombe en panne, tout le réseau est hors service. Le coût peut être plus élevé en raison du matériel central.

C'est la topologie la plus couramment utilisée aujourd'hui pour les réseaux locaux (LAN).

Figure 2.6 : Topologie en étoile [7]

4.3. Topologie en anneau :

C'est une topologie de type bus mais en circuit fermé, elle repose une boucle de câblage fermée**. [5]**

Avantages : Nécessite moins de câblage que la topologie en étoile. Fonctionne bien pour les réseaux avec un trafic régulier.

Inconvénients : La défaillance d'un seul appareil peut interrompre tout le réseau. Il est difficile d'ajouter ou de supprimer des appareils sans perturber le réseau.

Le dépannage peut être complexe. Cette topologie est moins courante aujourd'hui pour les LAN traditionnels.

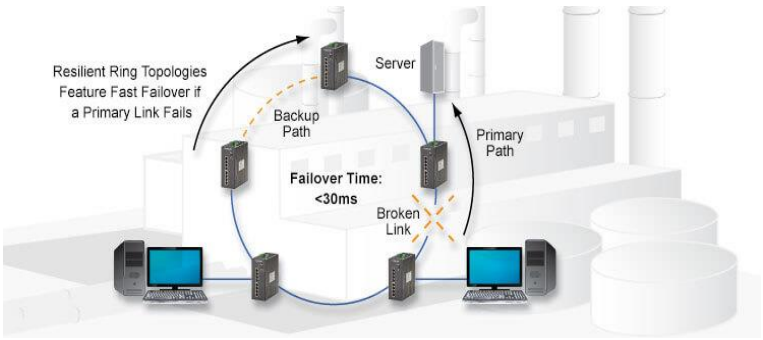

Figure 2.7 : Topologie en Anneau [8]

5. Les Technologies Réseau :

La technologie des réseaux combine du matériel, des logiciels et des techniques de communication pour développer et entretenir des réseaux informatiques. Elle garantit un flux fluide d'informations numériques, un partage de ressources et une accessibilité aux applications entre les ordinateurs.

Aujourd'hui, les entreprises s'appuient largement sur ces technologies pour une communication transparente au bureau sans être liées à un emplacement spécifique. Des configurations personnelles aux systèmes d'entreprise complexes, les technologies de réseau imprègnent de multiples facettes de notre vie quotidienne.

Ils ont non seulement rationalisé mais également accéléré de nombreux processus, rendant notre monde interconnecté plus efficace.

La technologie réseau est une famille de technologies utilisées pour envoyer et recevoir des données sur un réseau informatique. Elle permet la transmission de données entre deux ou plusieurs ordinateurs, leur permettant de communiquer entre eux via Internet ou d'autres réseaux.

Quelques technologies réseau :

- **Câblage physique :** Ethernet, Fibre optique, Câble coaxial, DSL, Câble téléphonique
- **Transmission sans fil :** Wi-Fi, Bluetooth, Réseau cellulaire (3G, 4G, 5G), Satellite
- **Logiciels et protocoles :** TCP/IP, HTTP, DNS, VPN, Firewall, Routage, Commutation

6. Les équipements d'interconnexion du réseau :

Les équipements d'interconnexion du réseau sont les composants matériels essentiels qui permettent de connecter différents segments de réseau ou des réseaux entiers entre eux, assurant ainsi la communication et le partage de ressources entre les appareils situés sur ces réseaux distincts.

On les classe principalement en fonction de leur couche d'opération dans le modèle OSI :

- ✓ **Couche physique (Couche 1) :** Répéteurs (étend la portée du signal) et Concentrateurs (Hubs) (point de connexion central diffusant le signal).
- ✓ **Couche liaison de données (Couche 2) :** Ponts (connectent des segments de LAN et filtrent par adresse MAC) et Commutateurs (Switches) (ponts multiports intelligents dirigeant le trafic vers des adresses MAC spécifiques).
- ✓ **Couche réseau (Couche 3) :** Routeurs (connectent différents réseaux et déterminent le meilleur chemin via les adresses IP) et Brouteurs (combinaison des fonctionnalités des couches 2 et 3).
- ✓ **Couches supérieures (Couche 4 et au-delà):** Passerelles (connectent des réseaux avec des protocoles différents en effectuant des conversions) et Pare-feu (contrôlent le trafic réseau pour la sécurité).

D'autres équipements importants incluent les Modems (pour la connexion WAN via diverses technologies) et les Points d'accès sans fil (WAPs) (pour connecter des appareils Wi-Fi aux réseaux câblés).

Le type d'équipement utilisé dépend des besoins spécifiques du réseau en termes de taille, de complexité et de fonctionnalités requises.

7. Routage :

Le routage est un processus décentralisé, c'est-à-dire que chaque routeur possède des informations sur son voisinage. Chaque routeur maintient une liste des réseaux connus, chacun de ces réseaux étant associé à un ou plusieurs routeurs voisins à qui le message peut être passé.

Le routage dans la couche réseau assure l'acheminement optimal des paquets à travers des réseaux interconnectés grâce à deux fonctions distinctes mais complémentaires :

- ✓ **Fonction de Routage :** Détermine le meilleur chemin vers le réseau de destination en consultant la table de routage et en utilisant une métrique pour évaluer la qualité des différents chemins.
- ✓ **Fonction de Commutation :** Permet au routeur de recevoir un paquet sur une interface d'entrée et de le transmettre vers une interface de sortie.

Pour optimiser la transmission des paquets, des méthodes de mise en cache des décisions de routage existent, notamment :

- ✓ **Fast Switching :** Met en cache la décision de routage (interface de sortie) et l'en-tête de trame généré pour la première destination rencontrée. Les paquets suivants vers la même destination sont traités plus rapidement en utilisant les informations mises en cache. C'est le mode par défaut sur les routeurs Cisco.
- ✓ Silicon Switching
- ✓ Autonomous Switching
- ✓ CEF (Cisco Express Forwarding)

Cependant, à l'exception de CEF, ces méthodes ont l'inconvénient de ne mettre en cache que la première décision de routage, ce qui empêche le partage de charge sur plusieurs liens pour une même destination.

L'administrateur doit donc choisir entre la rapidité de transmission et la répartition de charge.

La commande [no] IP route-cache permet d'activer ou de désactiver le Fast Switching sur une interface spécifique. Il est activé par défaut. **[9]**

8. Types de routage :

Il existe deux types de routage (Statique, Dynamique)

8.1. Routage statique :

Statique, Tout est géré manuellement par un administrateur réseau qui enregistre toutes les informations dans la configuration d'un routeur. **[9]**

Il doit mettre à jour manuellement les entrées de route statique chaque fois qu'une modification de la topologie le nécessite. Le routage statique offre plusieurs applications utiles. **[9]**

8.2. Routage dynamique :

Dynamique. Une fois qu'un administrateur réseau a entré les commandes de configuration pour lancer le routage dynamique, les informations relatives aux routes sont mises à jour automatiquement, par un processus de routage chaque fois que l'inter réseau envoie de nouvelles informations.

Il possède comme avantage principal de s'adapter automatiquement aux modifications topologiques. **[9]**

La mise en œuvre du routage dynamique dépend de deux fonctions de base :

- La gestion d'une table de routage (liste des chemins et des interfaces connus)
- La distribution opportune des informations aux autres routeurs sous la forme de mises à jour du routage.

Lorsqu'un réseau n'est accessible que par un seul chemin, une route statique vers ce réseau peut s'avérer suffisante. Ce type de réseau est appelé réseau d'extrémité. La configuration d'une route statique vers un réseau d'extrémité permet d'éviter la surcharge liée au routage dynamique.

Il évite d'avoir une perte en bande passante due aux mises à jour envoyées par les protocoles de routage.

Le routage dynamique possède comme avantage principal de s'adapter automatiquement aux modifications topologiques.

9. Table de routage :

La table de routage est l'élément central d'un routeur. C'est cette table qui est utilisée par la fonction de routage pour déterminer le meilleur chemin pour chaque destination connue du routeur. **[9]**

Il existe une seule table de routage par protocole routé, sachant que cette table de routage peut être complétée manuellement (routage statique) ou dynamiquement (protocoles de routage).

Voici les éléments clés que l'on trouve généralement dans une table de routage :

- ✓ **Adresse de destination :** L'adresse IP du réseau ou de l'appareil de destination.
- ✓ **Masque de sous-réseau :** Il définit la partie de l'adresse de destination qui identifie le réseau.
- ✓ **Passerelle (Gateway) :** L'adresse IP du prochain routeur (saut suivant) sur le chemin vers la destination. Pour les destinations directement connectées, la passerelle peut être l'interface locale.
- ✓ **Interface :** L'interface réseau locale par laquelle le trafic doit être envoyé pour atteindre la passerelle ou la destination.
- ✓ **Métrique :** Une valeur qui indique le coût ou la distance pour atteindre la destination. Les routeurs utilisent les métriques pour déterminer le meilleur chemin lorsqu'il existe plusieurs routes possibles.
- ✓ **Flags (Indicateurs) :** Des codes qui fournissent des informations supplémentaires sur la route (par exemple, si la route est active, une passerelle, un hôte, etc.)

Fonctionnement d'une table de routage :

Lorsqu'un routeur reçoit un paquet de données, il examine l'adresse de destination du paquet. Ensuite, il consulte sa table de routage pour trouver la meilleure correspondance entre l'adresse de destination et une des entrées de la table.

Une fois la route correspondante trouvée, le routeur transfère le paquet vers l'interface et la passerelle spécifiées dans cette entrée.

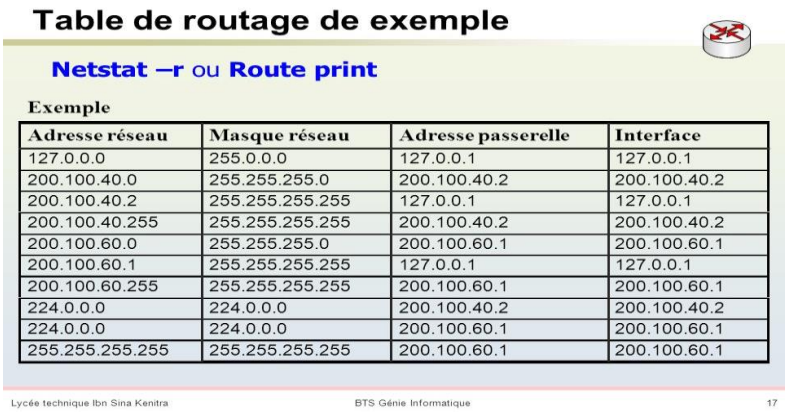

Figure 2.8 : Table de routage [10]

10. Les protocoles de routage :

Les protocoles de routage sont des ensembles de règles qui permettent aux routeurs de communiquer entre eux afin d'établir les meilleurs chemins pour acheminer les données à travers un réseau. Ils sont essentiels pour le bon fonctionnement d'Internet et des réseaux d'entreprise.

On distingue principalement deux types de protocoles de routage :

- ✓ **Protocoles de routage statique :** Les routes sont configurées manuellement par l'administrateur réseau sur chaque routeur. Ce type de routage est simple à mettre en place pour les petits réseaux, mais il devient complexe et difficile à maintenir pour les réseaux plus importants ou dynamiques.
- ✓ **Protocoles de routage dynamique :** Les routeurs découvrent automatiquement les réseaux et les chemins disponibles, et ils mettent à jour leurs tables de routage en conséquence. Ces protocoles sont plus adaptés aux grands réseaux car ils s'adaptent aux changements de topologie.

Parmi les protocoles de routage dynamique, on trouve deux grandes catégories :

- ✓ **Protocoles à vecteur de distance :** Ces protocoles, comme RIP (Routing Information Protocol), diffusent périodiquement leur table de routage complète à leurs voisins. Ils déterminent le meilleur chemin en se basant sur le nombre de sauts (le nombre de routeurs traversés).
- ✓ **Protocoles à état de liens :** Ces protocoles, comme OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System), diffusent des informations sur l'état de leurs propres liens (interfaces et voisins). Chaque routeur construit alors une carte complète du réseau et calcule les meilleurs chemins en utilisant un algorithme comme Dijkstra.

Il existe également des protocoles hybrides, comme EIGRP (Enhanced Interior Gateway Routing Protocol) de Cisco, qui combinent des caractéristiques des protocoles à vecteur de distance et à état de liens.

Les protocoles de routage peuvent aussi être classés en fonction de leur utilisation au sein d'un système autonome (un réseau sous une administration unique) ou entre différents systèmes autonomes :

- ✓ **Protocoles de routage interne (IGP - Interior Gateway Protocols) :** Utilisés au sein d'un même système autonome, par exemple RIP, OSPF, EIGRP, IS-IS.
- ✓ **Protocole de routage externe (EGP - Exterior Gateway Protocol) :** Utilisé pour échanger des informations de routage entre différents systèmes autonomes, le principal exemple étant BGP (Border Gateway Protocol), qui est le protocole de routage utilisé sur Internet.

Le choix d'un protocole de routage dépend de plusieurs facteurs, tels que la taille du réseau, la topologie, les exigences de performance et les fonctionnalités souhaitées.

Chapitre III : Les réseaux privés virtuels

1. La définition de VPN :

Un VPN, qui signifie réseau privé virtuel, établit une connexion numérique entre un ordinateur et un serveur distant appartenant à un fournisseur VPN, créant un tunnel point à point qui crypte vos données personnelles, masque votre adresse IP et vous permet de contourner les blocages de sites Web et pare-feu sur Internet.

Cela garantit que vos expériences en ligne sont privées, protégées et plus sécurisées.

Par sa définition même, une connexion VPN est :

- ✓ Virtuel : car aucun câble physique n'est impliqué dans le processus de connexion.
- ✓ Privé : car grâce à cette connexion, personne d'autre ne peut voir vos données ou votre activité de navigation.
- ✓ En réseau : car plusieurs appareils—votre ordinateur et le serveur VPN—travaillent ensemble pour maintenir un lien établi.

Dans la suite nous explorons les nombreux avantages d'un VPN et pourquoi il pourrait être avantageux d'en utiliser un pour aborder notre problématique.

Figure 3.1 : Schéma global d'un réseau VPN [11]

Pourquoi devrais-je utiliser un service VPN ?

Pour tous ceux qui recherchent une expérience en ligne plus sûre, plus libre et plus sécurisée, les avantages de l'utilisation d'un VPN sont innombrables. Un VPN protège ses utilisateurs en cryptant leurs données et en masquant leur adresse IP, laissant leur historique de navigation et leur localisation introuvables.

Cet anonymat permet une plus grande confidentialité, ainsi qu'une plus grande liberté pour ceux qui souhaitent accéder au contenu bloqué ou lié à une région.

2. Le principe fonctionnement de VPN : [12]

La création d'un VPN nécessite la création d'un tunnel. Un tunnel est un canal de communication dans lequel circulerons les données cryptées.

Le principe du VPN est donc basé sur la technique du tunneling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. La source peut ensuite éventuellement chiffrer les données (on parle alors de VPN chiffrés) et les achemine en empruntant ce chemin virtuel.

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunneling encapsule les données en rajoutant un entête permettant le routage des trames dans le tunnel.

Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulassions.

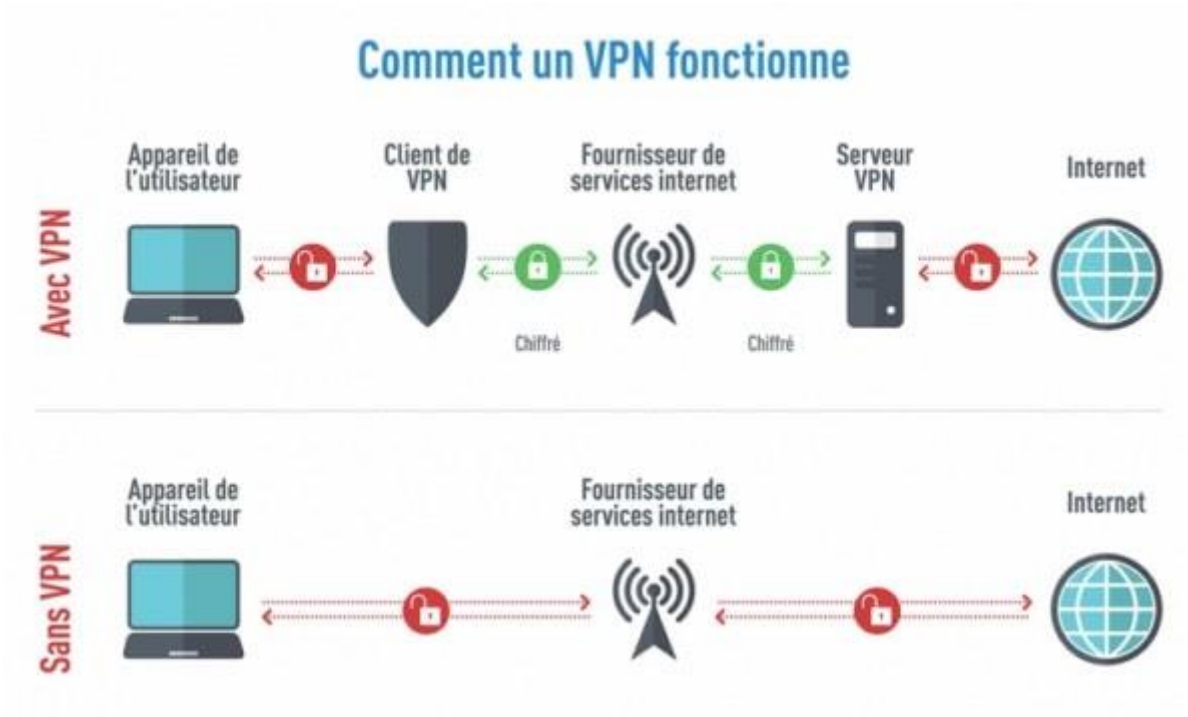

Figure 3.2 : Fonctionnement de VPN [13]

3. Les types de VPN :

Il existe différents types de VPN, chacun conçu pour répondre à des besoins spécifiques, que ce soit pour un usage personnel, pour connecter des bureaux distants ou pour sécuriser l'accès à des ressources d'entreprise.

Pour illustrer cela, nous allons examiner de plus près deux types fondamentaux :

3.1. Les VPN utilisateur à site :

Un VPN utilisateur à site fait référence à une connexion temporaire configurée entre un ou plusieurs utilisateurs et un emplacement central. Dans la plupart des cas, un VPN utilisateur à site est utilisé pour donner à chaque emplacement l'accès à un centre de données. Dans certaines situations, une connexion qui utilise la sécurité IPsec (Internet Protocol Security) est suffisante.

Cependant, il est également courant pour une organisation d'utiliser un VPN, qui lui permet de bénéficier de la sécurité positionnée aux passerelles à chaque extrémité du VPN.

Un VPN utilisateur à site est un outil utile pour les entreprises avec des travailleurs distants, que ce soit en déplacement ou à domicile. Si ces travailleurs doivent accéder à des informations privées ou sensibles hébergées dans les serveurs de l'entreprise, ils peuvent se connecter à un VPN utilisateur à site.

De cette manière, chaque employé peut accéder aux ressources dont il a besoin pour faire son travail.

Ce type de VPN peut être utilisé pour offrir aux travailleurs de différents endroits une expérience similaire à celle de ceux du bureau principal qui peuvent se connecter au serveur à leur bureau à l'aide d'un câble Ethernet. Dans un sens, le VPN utilisateur à site étend un câble sur de nombreux kilomètres, et même aux frontières internationales, jusqu'au poste de travail de chaque employé, qui comprend les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles.

3.2. Les VPN site à site (site à multisite) :

Un VPN Site-à-Site est une solution permettant de connecter deux ou plusieurs réseaux locaux (LAN) situés à des emplacements géographiques différents via un tunnel sécurisé sur Internet.

Il crée un tunnel chiffré qui permet la transmission sécurisée de données entre ces réseaux. Cela permet aux entreprises ou aux organisations d'étendre leur réseau interne en toute sécurité entre plusieurs sites distants, comme si tous les sites étaient connectés au même réseau local.

Ce type de VPN est particulièrement utile pour interconnecter différents bureaux ou succursales d'une entreprise.

4. Les protocoles utilisés pour réaliser une connexion VPN :

Les protocoles VPN sont des ensembles de règles qui déterminent comment les données sont transmises via le tunnel VPN. Différents protocoles offrent différents niveaux de sécurité, de vitesse et de compatibilité. Voici quelques protocoles courants :

4.1. Le protocole PPTP :

PPTP (Point-to-Point Tunneling Protocol) : C'est l'un des plus anciens protocoles de tunneling VPN. Il est facile à configurer mais est aujourd'hui considéré comme peu sécurisé en raison de vulnérabilités connues. Il est généralement déconseillé pour les applications nécessitant une forte protection des données.

4.2. Le protocole l2tp :

L2TP (Layer 2 Tunneling Protocol) : Ce protocole de tunneling crée une connexion entre deux points. En lui-même, il ne fournit pas de chiffrement. C'est pourquoi il est très souvent utilisé en combinaison avec un autre protocole de sécurité, comme IPsec (on parle alors de L2TP/IPsec).

4.3. Le protocole IPSec :

IPsec (Internet Protocol Security) : Il s'agit d'une suite de protocoles qui sécurise les communications IP en authentifiant et en cryptant chaque paquet de données d'une session. IPsec peut être utilisé seul ou en combinaison avec d'autres protocoles de tunneling comme L2TP pour offrir une solution VPN robuste et sécurisée.

4.4. Le protocole MPLS :

MPLS (Multi Protocol Label Switching) : Ce n'est pas un protocole VPN au sens strict, mais plutôt une technique de routage haute performance utilisée dans les réseaux de télécommunications. MPLS achemine les données en utilisant des étiquettes au lieu des adresses IP, ce qui permet un routage plus rapide et offre des capacités de qualité de service (QoS) et d'ingénierie de trafic.

Les entreprises l'utilisent souvent pour créer des VPN MPLS, qui sont des réseaux privés virtuels sécurisés et performants gérés par un fournisseur de services.

4.5. Le protocole SSL :

SSL (Secure Sockets Layer): C'est un protocole cryptographique qui fournit une communication sécurisée sur un réseau, notamment sur Internet. Bien qu'il ait été largement remplacé par son successeur, TLS (Transport Layer Security), le terme SSL est encore couramment utilisé.

SSL/TLS chiffre les données entre un client (comme un navigateur web) et un serveur, et est également utilisé pour l'authentification. Dans le contexte des VPN, SSL/TLS est utilisé par le protocole SSTP et pour les VPN basés sur navigateur.

Chapitre IV : VPN IPSec multipoint dynamiques

1. Introduction : [14]

De plus en plus d'entreprises expriment le besoin d'interconnecter leurs différents sites et d'utiliser un moyen de chiffrement afin de protéger leurs communications. Dans le passé, la seule solution à ce problème était l'utilisation des réseaux Layer-2 tels que RNIS ou Frame Relay.

La mise en place et le cout étant fastidieux, le déploiement de ces derniers serait sans doute moins cher si tous les sites avaient accès à internet afin de faciliter la sécurité des communications IP par l'utilisation des tunnels IPsec pour assurer l'authentification, l'intégrité et la confidentialité des données (VPN IPsec).

Le VPN IPsec est une solution fiable de communication sécurisée, mais il présente un certain nombre de limités à savoir :

- ➤ Une limite de maintenance et d'échelle : chaque ajout d'un nouveau site conduit à une modification totale de la configuration du site central. La configuration du site central peut facilement devenir illisible au bout d'une dizaine de sites.

- ➤ Pour interconnecter n sites, il faut configurer n (n-1) /2 tunnels et n routeurs ; une équation qui devient difficile à résoudre quand le nombre de sites augmente notamment dans le cas des réseaux Full Meshed ou complètement maillés.

Ces principales limites ont poussé les auteurs du VPN IPsec à se tourner vers une technologie beaucoup plus avantageuse : le DMVPN (Dynamic Multipoint VPN). Il s'agit d'un mécanisme qui permet d'établir les tunnels IPsec + GRE (Generic Routing Encapsulation), directement entre les routeurs qui veulent dialoguer ensemble avec une simplicité et une scalabilité déconcertante et surtout de façon totalement dynamique.

Son avantage majeur est qu'il permet de garder la configuration des routeurs statiques en cas d'ajout d'un nouveau site et la création des tunnels entre les sites distants est entièrement automatique. Déployer cette solution logicielle Cisco IOS pour la construction poussée IPsec des réseaux privés virtuels (VPN) sera l'objectif de notre exposé.

2. Présentation des DMVPN (Dynamic multipoint VPN) : [14]

Le DMVPN (Dynamic Multipoint VPN) est une solution de réseau privé virtuel (VPN) développée par Cisco qui simplifie la création et la gestion de réseaux VPN à grande échelle, en particulier pour interconnecter de nombreux sites distants à un site central (hub-and-spoke) ou entre eux (full mesh ou partial mesh).

En termes simples, le DMVPN permet de construire des tunnels VPN IPsec de manière dynamique et automatisée entre des routeurs, réduisant considérablement la complexité de configuration et de maintenance par rapport aux VPN IPsec traditionnels.

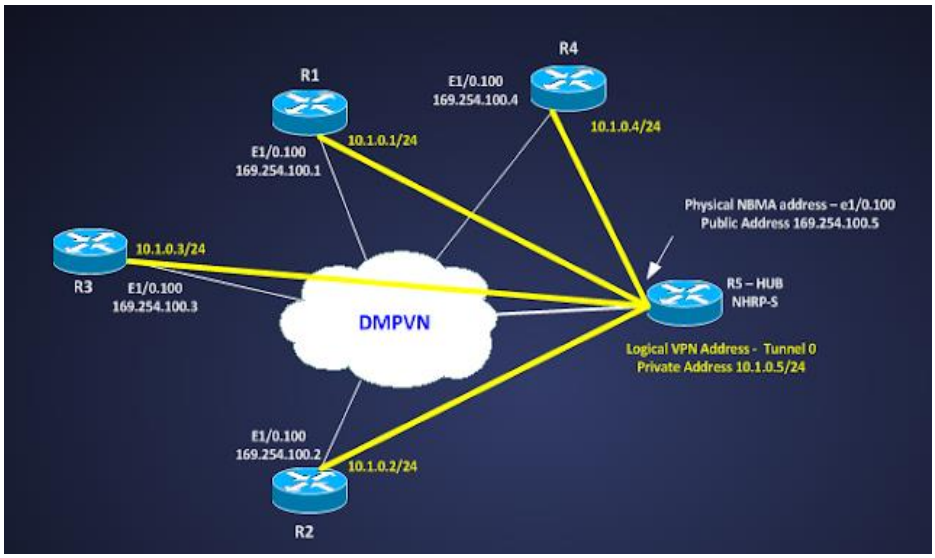

Figure 4.1 : Dynamique multipoint VPN [15]

3. Les composants et les terminologies :

Pour fonctionner, DMVPN s'appuie sur une combinaison de plusieurs technologies de base : GRE (Generic Routing Encapsulation), IPsec pour la sécurité, et surtout NHRP (Next Hop Resolution Protocol), qui joue un rôle central dans la découverte dynamique des routes entre les sites.

L'architecture DMVPN repose généralement sur une structure hub-and-spoke, où un routeur central (Hub) sert de point de coordination, tandis que les routeurs distants (Spokes) peuvent établir des connexions directes entre eux après une résolution initiale via le hub. Cela permet des communications efficaces de type spoke-to-spoke, réduisant la latence et la charge sur le hub.

Enfin, plusieurs phases de DMVPN (Phase 1, 2 et 3) existent, chacune introduisant des niveaux croissants de dynamisme et de complexité, notamment dans la gestion du routage et la redirection des flux.

Dans les sections suivantes, nous allons explorer en détail les principaux composants (Hub and Spoke, NHRP, mGRE, IPsec, OSPF) ainsi que les termes techniques associés, afin de mieux comprendre le fonctionnement interne et les avantages de cette technologie.

3.1. IPsec : [14]

IPsec (Internet Protocol Security) : protocole de chiffrement permettant de chiffrer le trafic entre deux sites, par l'utilisation des clés pré-partagées. Il n'est sans doute pas le protocole le mieux sécurisé mais permet une mise en œuvre simple et rapide.

3.2. mGRE (Multipoint Generic Routing Encapsulation) : [14]

mGRE (multipoint GRE) : protocole permettant de créer des tunnels multipoints entres différents sites ; c'est-à-dire créer plusieurs tunnels à partir d'un seul pseudo interface Tunnel.

3.3. NHRP (Next Hope Resolution Protocol): [14]

NHRP (Next Hope Resolution Protocol): protocole permettant aux routeurs distants de faire connaitre leur adresse IP servant à monter le tunnel GRE avec le serveur. Le serveur, de son coté, stocke les adresses IP pour permettre à chaque routeur de connaitre l'adresse de son voisin et ainsi établir un tunnel direct avec lui.

3.4. OSPF (Open Shortest Path First): [14]

OSPF (Open Shortest Path First) : protocole de routage permettant au routeur du site central de propager les différentes routes aux sites distants. Il permet aussi aux routeurs des sites distants d'annoncer leur réseau local au site central.

3.5. Hub and Spoke : [14]

Hub and Spoke : les deux termes désignent respectivement le routeur central et les routeurs distants. Le site central desservi par le routeur central fait office de serveur NHRP.

4. Les Modèles de déploiement :

Les modèles de déploiement de DMVPN (Dynamic Multipoint VPN) offrent différentes manières de connecter des sites distants de manière sécurisée et flexible sur un réseau non fiable comme Internet. Voici les modèles de déploiement les plus courants :

- ✓ **Le modèle Hub-and-spoke :** chaque spoke possède une interface GRE permettant de monter le tunnel vers le HUB. Tout trafic entre les spoke passe par le HUB. Ce modèle ne prend pas en compte les liaisons entre les spoke. **[14]**

    - **Avantages :** Configuration centralisée et simplifiée du hub, idéal pour les scénarios où la plupart du trafic est destiné au site central (par exemple, accès aux serveurs du siège).
    - **Inconvénients :** La communication entre les spoke nécessite un double saut via le hub, ce qui peut introduire une latence supplémentaire et potentiellement créer un point de congestion unique

- ✓ **Le modèle Spoke-to-Spoke :** chaque spoke doit disposer d'une interface mGRE permettant aux tunnels dynamiques de transiter vers les autres spoke. Ce modèle prend en compte les liaisons entre différents spoke et offre une grande évolutivité de la configuration pour les périphériques. **[14]**

    - **Avantages :** Réduction de la latence et de la charge sur le hub pour le trafic inter-sites, amélioration de l'efficacité pour la communication fréquente entre les branches.
    - **Inconvénients :** Configuration plus complexe, nécessite l'utilisation de NHRP (Next Hop Resolution Protocol) pour la résolution dynamique des adresses IP des tunnels.

5. Les Avantages du DMVPN :

- ➢ **Scalabilité accrue :** L'ajout de nouveaux sites distants nécessite une configuration minimale, voire nulle, sur le site central. Les nouveaux spoke se configurent pour se connecter au hub, et la création des tunnels spoke-to-spoke est automatisée.

- ➢ **Gestion simplifiée :** La configuration centralisée sur le hub réduit la complexité administrative et facilite la gestion des politiques de sécurité et de routage.

- ➢ **Réduction des coûts :** En simplifiant la configuration et la gestion, le DMVPN peut réduire les coûts opérationnels associés au déploiement et à la maintenance des réseaux VPN.

- ➢ **Flexibilité accrue :** Le DMVPN prend en charge différentes topologies, notamment le hub-and-spoke, le full mesh et le partial mesh, offrant une grande flexibilité pour répondre aux besoins spécifiques de l'entreprise.

- **Optimisation du trafic :** La possibilité d'établir des tunnels spoke-to-spoke permet d'optimiser le routage du trafic en évitant le transit inutile par le hub pour les communications directes entre les sites distants, réduisant ainsi la latence et la charge sur le hub.

- **Déploiement rapide :** La simplicité de la configuration permet un déploiement plus rapide des nouveaux sites et des modifications du réseau VPN.

6. La solution DMVPN : [16]

La solution de routage DMVPN emploie le multipoint GRE (mGRE) et le protocole de résolution de sauts successifs (NHRP), avec IPsec et quelques nouvelles améliorations, pour résoudre les problèmes de routage ci-dessus d'une manière évolutive.

7. Démarrage automatique du cryptage Ipsec : [16]

Quand la solution DMVPN n'est pas utilisée, le tunnel de cryptage IPsec n'est pas lancé jusqu'à ce qu'il y ait du trafic de données qui requiert l'utilisation de ce tunnel IPsec.

Il peut falloir entre 1 et 10 secondes pour terminer le démarrage du tunnel IPsec et le trafic de données est stoppé pendant ce temps. En utilisant GRE avec IPsec, la configuration de tunnel GRE inclut déjà l'adresse de l'homologue de tunnel GRE (destination du tunnel...), qui est également l'adresse d'homologue IPsec. Chacune des deux adresses est préconfigurée.

Si vous utilisez le Tunnel Endpoint Discovery (TED) et des cartes de chiffrement dynamique sur le routeur concentrateur, alors vous pouvez éviter de devoir préconfigurer les adresses d'homologue IPsec sur le concentrateur, mais un probe and réponse de TED doit être envoyé et reçu avant que la négociation ISAKMP puisse commencer.

Ceci ne devrait pas être nécessaire puisque, en utilisant GRE, les adresses d'origine et de destination d'homologue sont déjà connues. Elles sont en configuration ou résolues avec le NHRP (pour les tunnels GRE multipoints).

Avec la solution de routage DMVPN, IPsec est déclenché immédiatement pour les tunnels GRE point par point et multipoints. En outre, il n'est pas nécessaire de configurer une ACL de cryptage, puisque ceux-ci seront automatiquement dérivés des adresses d'origine et de destination du tunnel GRE.

Les commandes suivantes sont utilisées pour définir les paramètres de cryptage IPsec. Notez qu'il n'y a aucune commande set Peer... ou match adresse... requise parce que ces informations sont dérivées directement des mappages du tunnel GRE ou du NHRP associés.

8. Création dynamique de tunnel pour les trafics « Spoke-to-Spoke » : [16]

Comme indiqué plus tôt, actuellement dans un réseau maillé, tous les tunnels point à point IPsec (ou IPsec + GRE) doivent être configurés sur tous les routeurs, même si certains/la plupart de ces tunnels ne sont pas nécessaires à tout moment.

Avec la solution DMVPN, un routeur est le concentrateur, et tous les autres routeurs (rayons) sont configurés avec des tunnels vers le concentrateur. Les tunnels de rayon-à-concentrateur sont continuellement en ligne, et les rayons n'ont pas besoin de la configuration pour les tunnels directs aux autres rayons.

Au lieu de cela, quand un rayon veut transmettre un paquet à un autre rayon (tel que le sous-réseau derrière un autre rayon), elle emploie NHRP pour déterminer dynamiquement l'adresse de destination requise du rayon cible.

Le routeur concentrateur agit en tant que serveur NHRP et traite cette demande pour le rayon source. Les deux rayons créent alors dynamiquement un tunnel IPsec entre eux (par l'intermédiaire de l'interface simple mGRE) et des données peuvent être directement transférées.

Ce tunnel dynamique de rayon à rayon sera automatiquement démoli après une période d'inactivité (configurable).

9. Prise en charge des protocoles de routage dynamiques : [16]

La solution DMVPN est basée sur les tunnels GRE qui prennent en charge des paquets de multicast/diffusion IP de transmission tunnel. Ainsi, la solution DMVPN prend en charge également les protocoles de routage dynamiques s'exécutant au-dessus des tunnels IPsec + mGRE. Précédemment, le NHRP vous obligeait à configurer explicitement le mappage diffusion/multicast pour que les adresses IP du tunnel de destination pour prendre en charge la transmission tunnel GRE des paquets IP multicast et de diffusion.

Par exemple, au niveau du concentrateur vous auriez besoin de la ligne de configuration ip nhrp map multicast <spoke-n-addr> pour chaque rayon. Avec la solution DMVPN, les adresses des rayons ne sont pas connues à l'avance et cette configuration n'est donc pas possible.

Au lieu de cela, NHRP peut être configuré pour ajouter automatiquement chaque rayon à la liste de destination multicast sur le concentrateur avec la commande ip nhrp map multicast dynamic.

Avec cette commande, quand les routeurs en étoile enregistrent leur mappage de NHRP de monodiffusion avec le serveur NHRP (concentrateur), NHRP créera également un mappage diffusion/multicast pour ce rayon. Ceci élimine le besoin de connaître les adresses des rayons à l'avance.

10. Commutation rapide de Cisco Express Forwarding pour mGRE : [16]

Actuellement, le trafic dans une interface de mGRE est commuté par processus, ce qui entraîne des performances médiocres. La solution DMVPN ajoute la commutation de Cisco Express Forwarding pour le trafic mGRE, ce qui entraîne des performances bien meilleures.

Il n'y a aucune commande de configuration nécessaire pour activer cette fonctionnalité. Si la commutation de Cisco Express Forwarding est autorisée sur l'interface de tunnel GRE et sur les interfaces physiques sortantes/entrantes, alors les paquets du tunnel GRE multipoints seront commutés par Cisco Express Forwarding.

11. Utilisation du routage dynamique sur les VPN protégés par Ipsec : [16]

Cette section décrit la situation actuelle (antérieure à la solution DMVPN). IPsec est mis en application sur les routeurs Cisco par l'intermédiaire d'un ensemble de commandes qui définissent le cryptage, puis une commande crypto map <map-name> appliquée sur l'interface externe du routeur.

En raison de cette conception et du fait qu'il n'y a actuellement aucune norme pour l'usage d'IPsec pour crypter des paquets IP multicast/diffusion, les paquets du protocole de routage IP ne peuvent pas <<< être transférés >> par le tunnel IPsec et aucune modification du routage ne peut être dynamiquement propagée de l'autre côté du tunnel IPsec.

Remarque : Tous les protocoles de routage dynamiques excepté le BGP utilisent des paquets IP de diffusion ou de multicast. Les tunnels GRE sont utilisés en combinaison avec IPsec pour résoudre ce problème de routage.

Les tunnels GRE sont mis en application sur les routeurs Cisco à l'aide d'une interface de tunnel virtuel (interface tunnel<#>). Le protocole de transmission tunnel GRE est conçu pour prendre en charge les paquets IP multicast/diffusion pour qu'un protocole de routage dynamique puisse être <<<< exécuté >>> sur un tunnel GRE.

Les paquets de tunnel GRE sont des paquets de monodiffusion IP qui encapsulent le paquet IP multicast/monodiffusion original. Vous pouvez alors utiliser IPsec pour crypter le paquet du tunnel GRE.

Vous pouvez également exécuter IPsec en mode transport et économiser 20 octets puisque GRE a déjà encapsulé le paquet des données originales. Vous n'avez donc pas besoin qu'lPsec encapsule le paquet IP GRE dans un autre en-tête IP.

En exécutant IPsec en mode de transport, il y a une restriction qui fait que les adresses IP d'origine et de destination du paquet à chiffrer doivent correspondre aux adresses d'homologue IPsec (le routeur lui-même).

Dans ce cas, ceci signifie juste que le point de destination du tunnel GRE et des adresses de l'homologue IPsec doivent être identiques. Ce n'est pas un problème puisque les mêmes routeurs sont à la fois les points de destination d'IPsec et du tunnel GRE.

En combinant des tunnels GRE avec le cryptage IPsec, vous pouvez utiliser un protocole de routage dynamique IP pour mettre à jour les tables de routage aux deux extrémités du tunnel crypté.

Les entrées de la table de routage IP pour les réseaux qui ont été appris via le tunnel crypté auront l'autre extrémité du tunnel (adresse IP de l'interface de tunnel GRE) comme prochain saut d'IP. Ainsi, si les réseaux changent d'un côté ou de l'autre du tunnel, alors l'autre côté apprendra dynamiquement la modification et la connectivité continuera sans aucune modification de configuration des routeurs.

12. Mise en place de tunnel GRE au sein de la maquette en routage statique sous GNS3 puis de l'algorithme de routage NHRP :

La mise en place d'un tunnel GRE (Generic Routing encapsulation) consiste à configurer une liaison point-à-point virtuelle entre deux routeurs au pare-feu via une liaison logique, qui permet de connecter plusieurs sites distants via un tunnel unique au lieu de tunnels point à point individuels.

Elle utilise une topologie en étoile (hub and spoke) où un hub centralise les connexions avec plusieurs sites, permettant d'encapsuler et de transmettre des paquets réseau, y compris des paquets de diffusion et de multicast, à travers un réseau public comme Internet.

Le mGRE (Multipoint GRE), permet lui de créer des tunnels multipoints entre les sites (Rx-Ry et Rr-Rz), c'est à dire de créer plusieurs tunnels par une seule pseudo-interface 'Tunnel'.

Le mGRE est dynamique et utilise le Next Hop Resolution Protocol (NHRP) pour établir les tunnels. Cela simplifie la configuration et la maintenance des VPN, en particulier pour les réseaux avec un grand nombre de sites.

Chapitre V : Implémentation du la maquette

1. Introduction :

Dans ce chapitre, nous aborderons l'implémentation de la technologie DMVPN (Dynamic Multipoint VPN). Cette technologie permet de connecter des réseaux distants de manière sécurisée et efficace.

Pour ce faire, nous commencerons par une démonstration pratique de sa mise en œuvre en utilisant le simulateur GNS3. Nous créerons une topologie de réseau appropriée pour faciliter la compréhension de cette implémentation. Une fois cette étape terminée, nous nous concentrerons sur la manière d'appliquer cette technologie dans l'environnement de l'entreprise SONATRACH.

2. Environnement de travail :

Matériel et Logiciel utilisés lors de l'implémentation :

- Simulateur : GNS3
- Routeur Cisco IOS : C3745
- Ordinateur portable : Avec un minimum de 4 Go de RAM (idéalement 8 Go de RAM).

Architecture du réseau :

- Version d'IOS : 12.4 et plus (utilisation d'un routeur C3745 pour disposer de la fonctionnalité DMVPN).
- RAM : 512 Mo.
- Flash : 125 Mo.

3. Contexte :

Quelques précisions avant de commencer :

- ✓ Que la politique IKE (crypto isakmp Policy) soit identique sur chacun des routeurs.
- ✓ Que la politique IPSec (crypto ipsec transform-set) soit identique sur chacun des routeurs.
- ✓ Que le protocole de routage EIGRP soit configuré de façon cohérente, c'est à dire que le réseau soit déclaré dans une area différente des réseaux LAN (10.160.x.0/24) et du réseau utilisé pour les tunnels VPN (172.16.200.0/24). En effet, si cette condition n'est pas remplie, vos tunnels VPN risquent d'avoir une connexion instable.

4. Installation de GNS3 Windows :

4.1. Présentation de GNS3 :

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.

GNS3 est utilisé l'émulateur Dynamics pour simuler Cisco IOS, et utilise par des centaines de milliers d'ingénieurs réseau dans le monde entier pour émuler, configurer, tester et dépanner des réseaux virtuels et réels.

Figure 5.1 : Dynamique multipoint VPN [17]

4.2. Téléchargement :

L'installation de GNS3 nécessite la création d'un compte sur le site internet GNS3. Une fois le compte créer nous nous rendrons à l'adresse suivante pour nous connecter : Site GNS3.

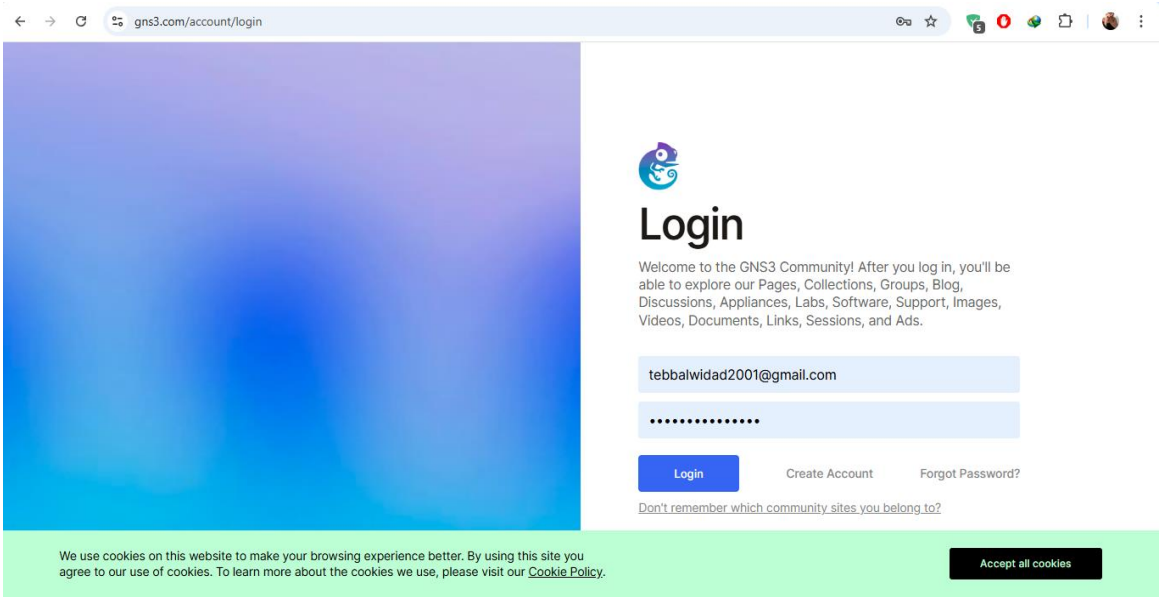

Figure 5.2: Interface de connexion au site web GNS3

Une fois identifié, nous avons accès aux liens pour télécharger l'exécutable.

Après vous être connecté, vous serez invité à sélectionner la version de GNS3 à télécharger. Dans ce guide, nous sélectionnerons l'installation Windows. Cliquez sur le bouton Télécharger pour télécharger le package GNS3 tout-en-un.

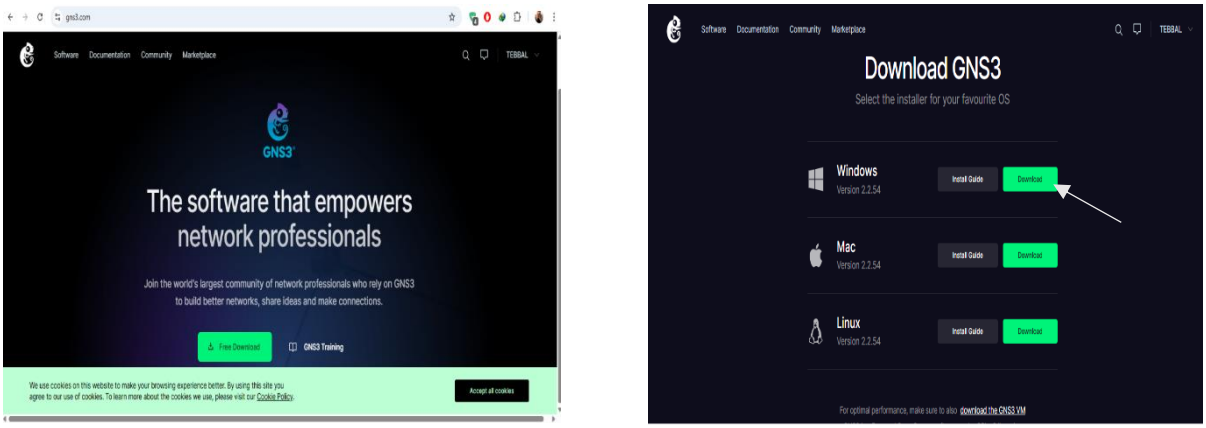

Figure 5.3: Page de téléchargement de GNS3

Quand le téléchargement est terminé, nous nous rendons dans le dossier « Téléchargements » et nous double-cliquerons sur l'exécutable que nous venons de télécharger, cela aura pour effet, de lancer l'assistant d'installation.

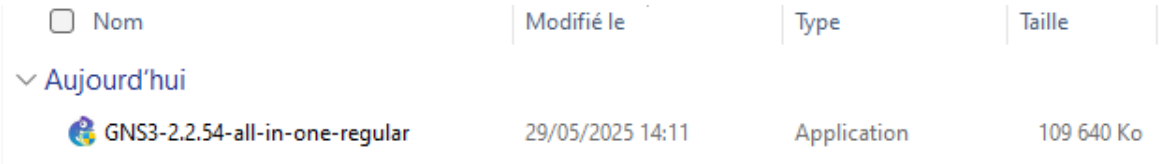

Figure 5.4 : Fichier d'installation GNS3 dans le dossier de téléchargement

L'assistant d'installation de GNS3 s'affiche. Cliquez sur Next > pour lancer l'installation

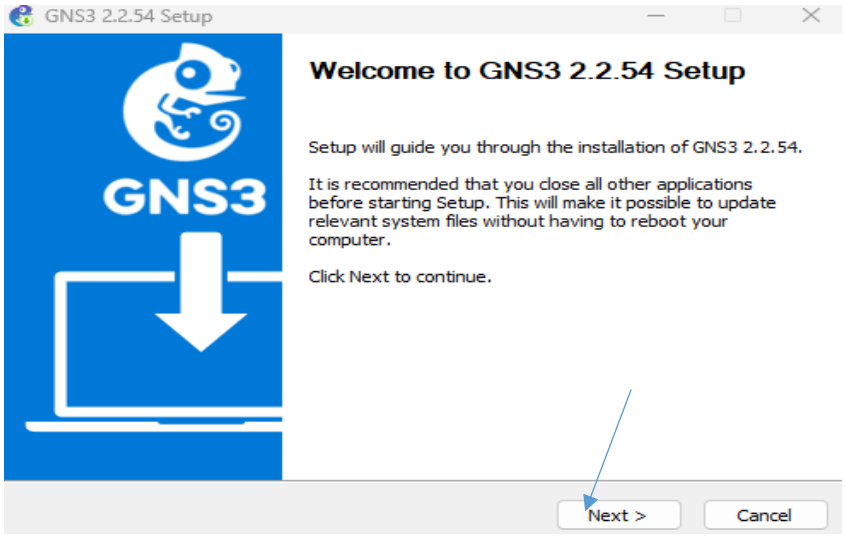

Figure 5.5: Assistant d'installation de GNS3 – écran de bienvenue

À l'étape suivante, nous avons accès à la licence d'utilisation que nous devons accepter pour nous permettre de poursuivre l'installation. Nous cliquerons sur le bouton « I Agree ».

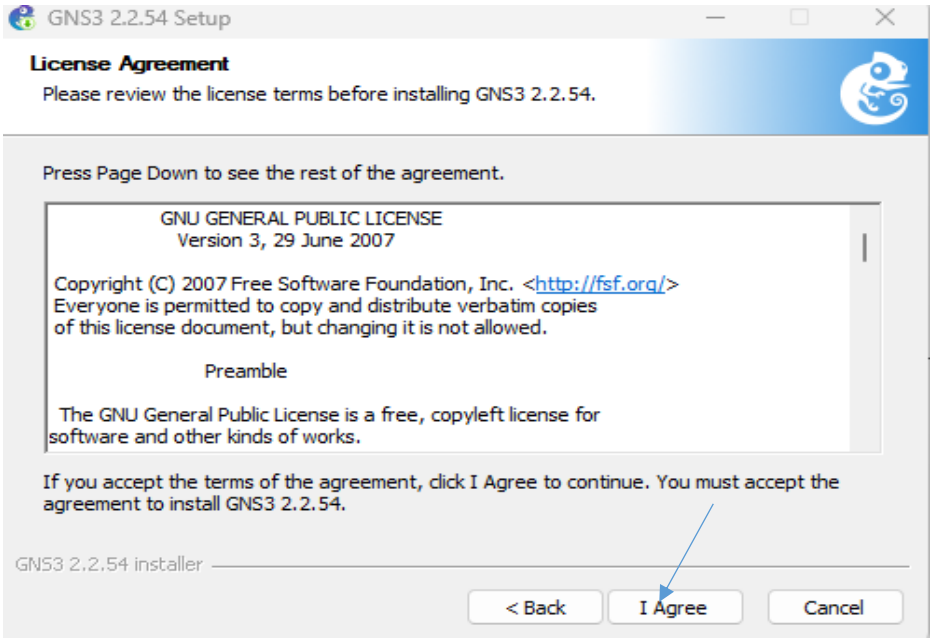

Figure 5.6: Assistant d'installation de GNS3 – Contrat de licence

Sélectionnez le dossier du menu Démarrer pour le raccourci GNS3. Le dossier par défaut est GNS3. Cliquez sur Next > pour poursuivre l'installation

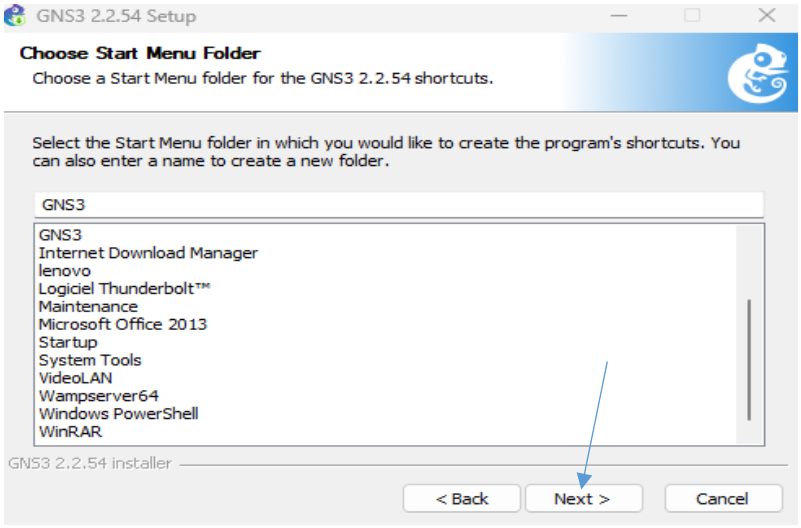

Figure 5.7: Assistant d'installation de GNS3 -Sélection du dossier du menu Démarrer

GNS3 est fourni avec divers logiciels prérequis et optionnels. Par défaut, la plupart des logiciels sont sélectionnés pour l'installation, mais vous pouvez choisir de n'installer que certains d'entre eux.

Si vous n'êtes pas sûr, laissez toutes les sélections de logiciels à leur sélection par défaut et cliquez sur Next > pour continuer l'installation

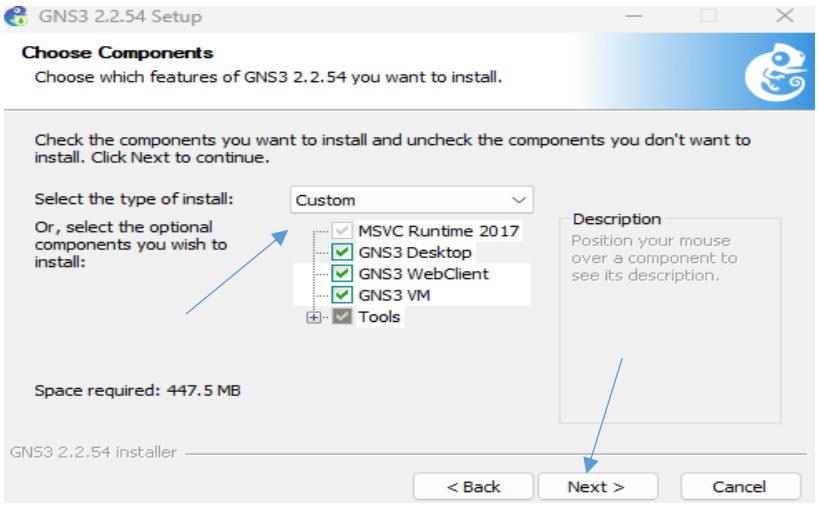

Figure 5.8: Assistant d'installation de GNS3 - Sélection des composants à installer

Nous sélectionnerons ensuite l'emplacement où nous voulons installer les composants. Pour des raisons de performances, il peut s'avérer très intéressant d'installer sur un disque dur SSD. Une fois l'emplacement sélectionné, nous pouvons cliquer sur le bouton « Next ».

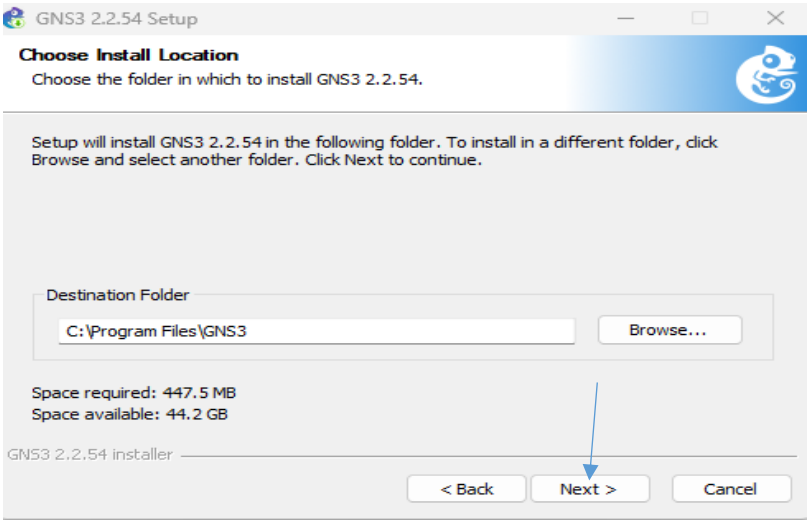

Figure 5.9: Assistant d'installation de GNS3 - Choix du dossier d'installation

Vu que précédemment nous avons sélectionné « GNS3 VM », il nous ai demandé de sélectionner l'hyperviseur qui sera utilisé pour exécuter la VM. Pour cet article, VMWare Workstation sera utilisé, c'est donc « VMWARE Workstation » qui sera choisi.

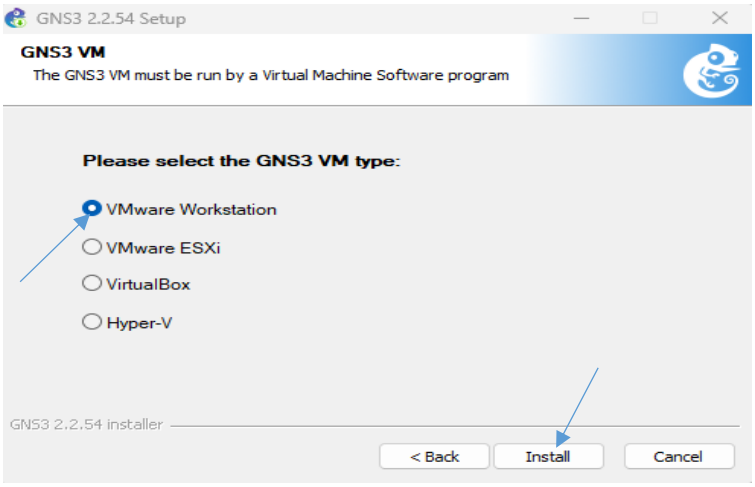

Figure 5.10: Assistant d'installation de GNS3 - Sélection du type de machine virtuelle

Le processus d'installation démarre en y intégrant le téléchargement de la machine virtuelle.

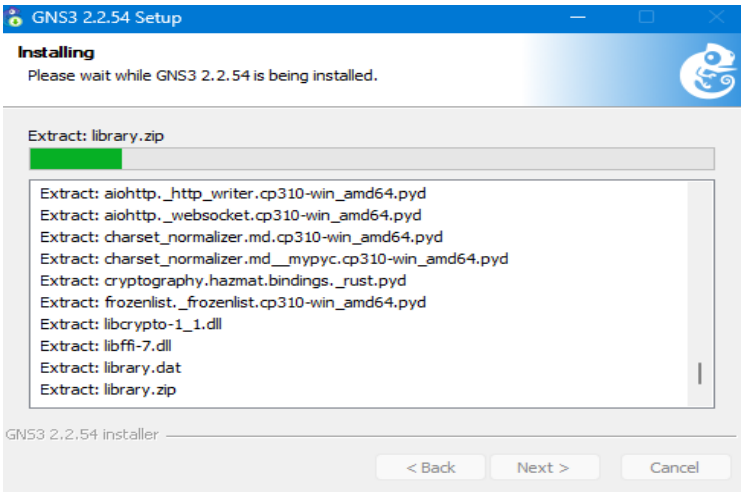

Figure 5.11 : Assistant d'installation de GNS3 - Progression de l'installation

Puis, nous installerons NPCAP qui permet de faire de la capture de trame. Nous laisserons également les valeurs par défaut.

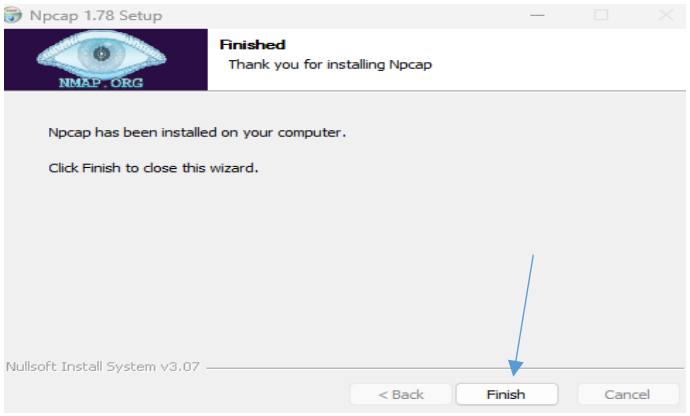

Figure 5.12 : Assistant d'installation Npcap - Fin de l'installation

Ensuite, nous passons à l'installation de Solar-Putty qui est un terminal qui nous permettra de paramétrer les équipements des maquettes réalisées avec GNS3. Acceptez les conditions d'utilisation puis cliquez sur le bouton « Accept ».

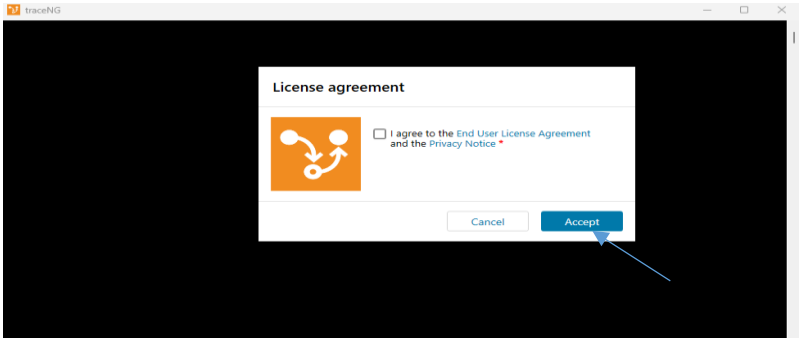

Figure 5.13 : Accord de licence de l'utilisateur final (SolarWinds/Solar-PuTTY)

Une fois l'installation de solar-putty installé, nous passerons à la suite, une proposition d'installation d'un autre outil de SolartWinds est proposée, n'ayant jamais eu besoin de cet outil, nous cocherons « No », puis nous cliquerons sur « Next ».

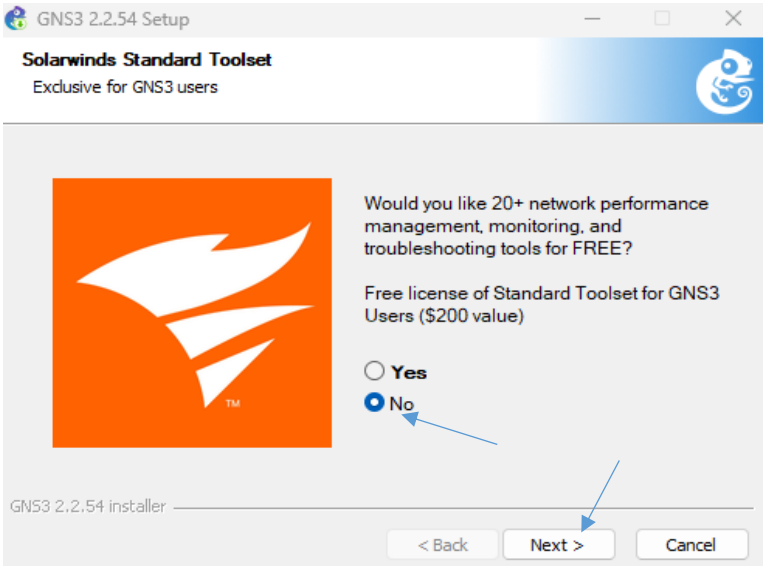

Figure 5.14 : Assistant d'installation GNS3 - Offre d'outils SolarWinds

Nous en avons fini avec l'installation à proprement parler de GNS3, nous pouvons continuer en cliquant sur le bouton « Finish ».

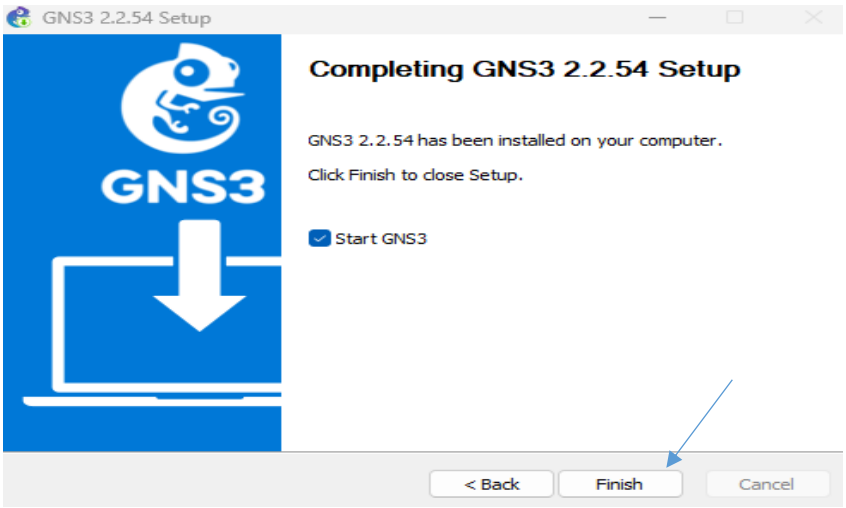

Figure 5.15 : Assistant d'installation GNS3 - Installation terminée

Nous avons ainsi terminé l'installation de GNS3.

Après avoir finalisé la configuration de la machine virtuelle requise et téléchargé les outils utilisés dans GNS3, nous pouvons maintenant le configurer pour son utilisation. Dans GNS3, cette fenêtre qui apparaît sur l'image, nous permet soit de créer un nouveau projet en lui donnant un nom et en spécifiant son emplacement de sauvegarde, soit d'ouvrir un projet existant depuis le disque dur ou à partir de la liste des projets récents.

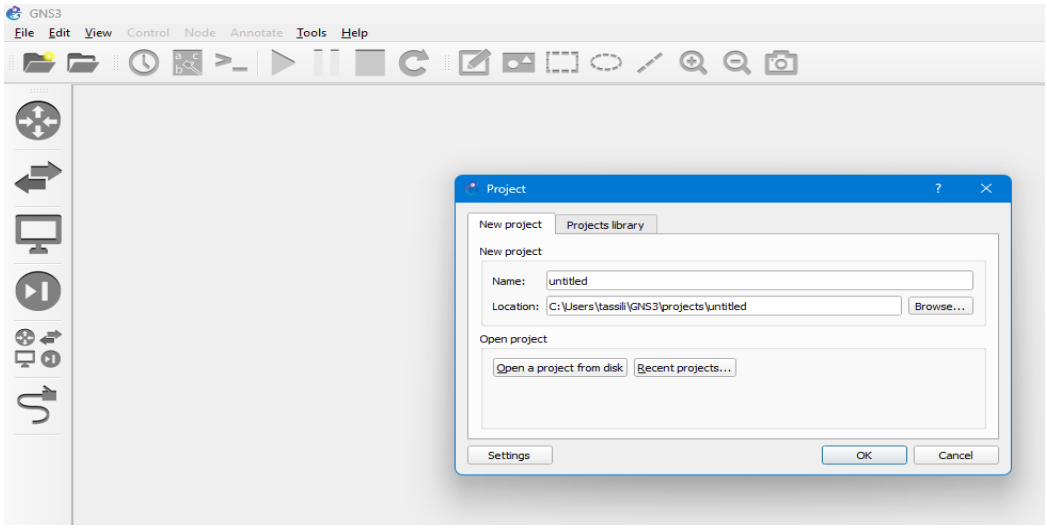

Figure 5.16: Fenêtre de gestion des projets GNS3.

Après avoir ouvert la fenêtre des préférences dans GNS3, une liste latérale apparaît, nous permettant d'accéder à divers paramètres. Sur cette image, l'option "IOS routers" est sélectionnée dans la section "Dynamips" sur le côté gauche. Cette fenêtre principale vide indique que nous sommes en train d'ajouter des modèles (templates) de routeurs IOS, ce qui est une étape essentielle pour permettre la simulation de réseaux utilisant ces dispositifs dans GNS3.

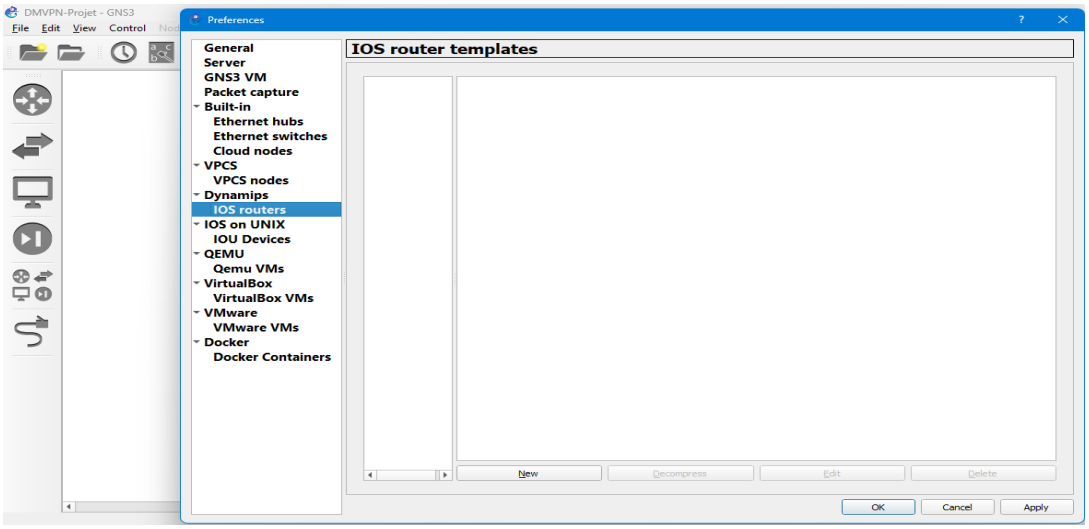

Figure 5.17: Configuration des modèles de routeurs IOS dans GNS3.

Après avoir sélectionné 'IOS routers' dans le menu latéral des préférences de GNS3, une fenêtre pop-up intitulée 'New IOS router template' apparaît. Cette fenêtre est dédiée à l'ajout d'un nouveau modèle de routeur IOS. Sur l'image, l'option 'Existing image' est sélectionnée, et le chemin ou le nom du fichier d'image IOS spécifié est affiché, indiquant que l'utilisateur est en train d'importer une image de système d'exploitation Cisco IOS existante pour l'utiliser dans la simulation, avant de passer aux étapes suivantes en cliquant sur 'Next'.

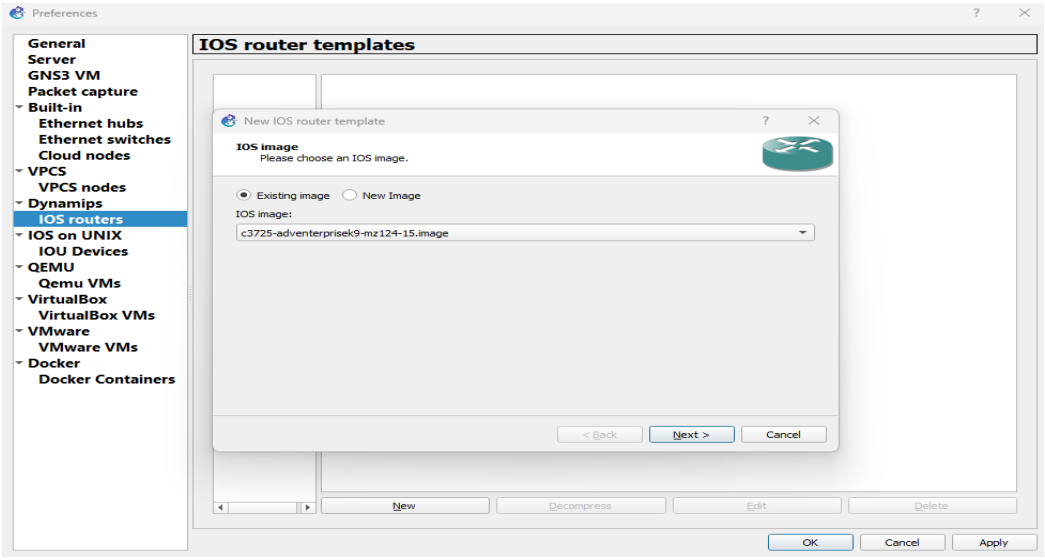

Figure 5.18: Ajout d'un nouveau modèle de routeur IOS dans GNS3.

Après la sélection de l'image IOS, la fenêtre 'Network adapters' apparaît dans GNS3 pour définir les adaptateurs réseau par défaut du nouveau modèle de routeur. L'image montre deux slots activés : 'slot 0' configuré en 'C1700-100 PE' et 'slot 1' en 'NM-16ESW', déterminant ainsi les ports par défaut du périphérique simulé.

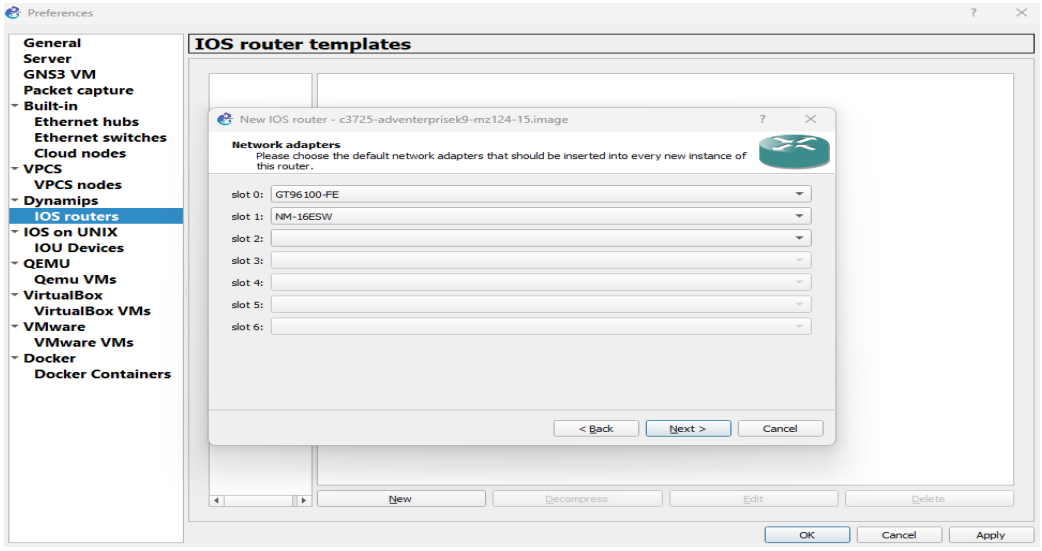

Figure 5.19: Choix des slots d'interface pour le routeur IOS dans GNS3

Après la configuration des adaptateurs réseau, nous passons dans GNS3 à l'étape cruciale du réglage de la valeur Idle-PC. Une fenêtre pop-up confirme que GNS3 a trouvé une valeur appropriée (0x60f9f8a0) pour l'image IOS, ce qui l'empêche de consommer toutes les ressources du processeur et assure la stabilité de la simulation.

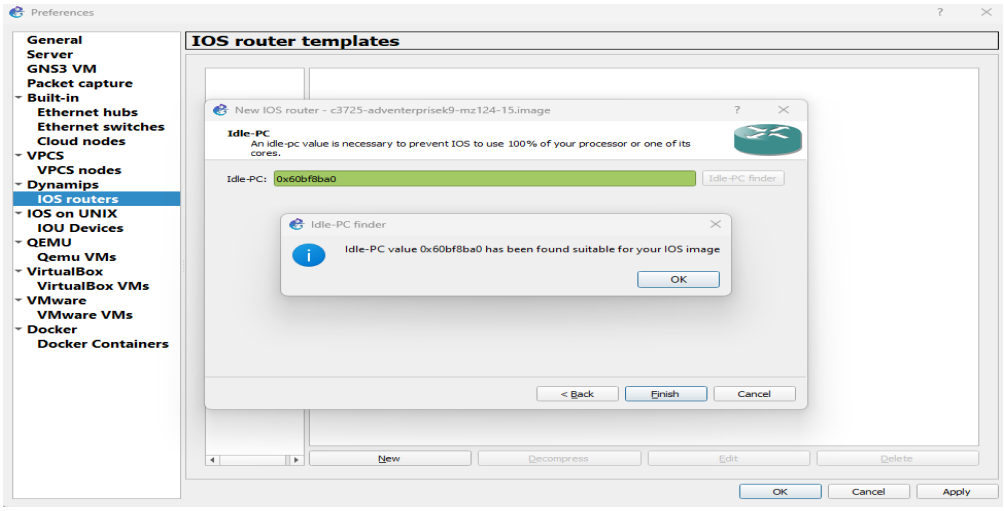

Figure 5.20: Réglage de la valeur Idle-PC pour le routeur IOS dans GNS3

Une fois les paramètres du modèle de routeur IOS et la valeur Idle-PC configurés, les détails du nouveau modèle sont affichés dans la fenêtre 'IOS router templates' de GNS3. L'écran présente un résumé complet des réglages tels que le nom du modèle ('c3725'), l'image, la valeur Idle-PC, les allocations de mémoire et les détails des adaptateurs (comme C1700-100 PE et NM-16ESW), confirmant ainsi que le modèle est prêt à l'emploi.

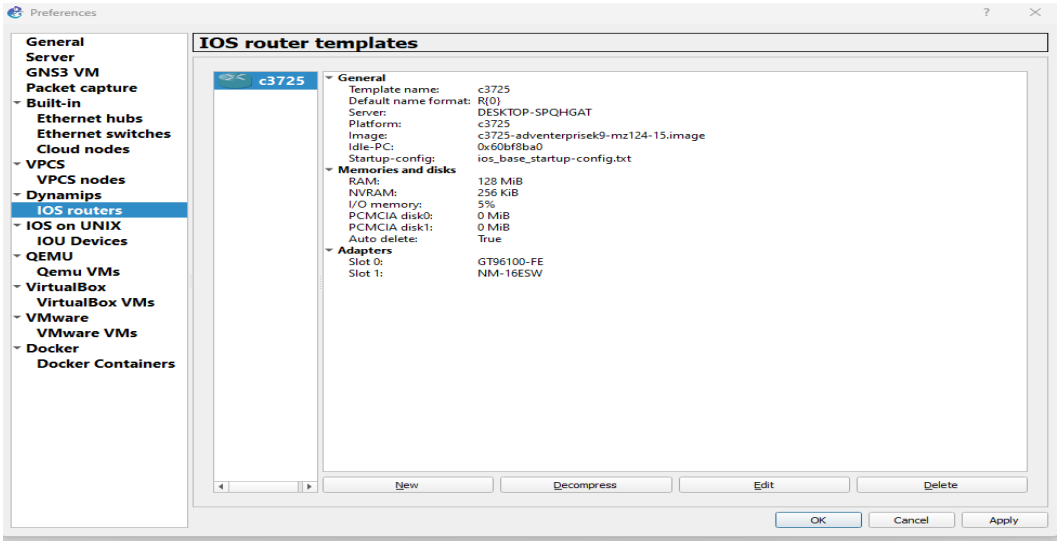

Figure 5.21 : Confirmation des propriétés du routeur c3725 dans GNS3

Après avoir terminé l'ajout des modèles (templates) d'appareils dans GNS3, nous revenons à l'interface principale du projet. L'image montre la liste latérale des appareils disponibles (Installed & Available appliances), plus précisément la section 'Routers'. On peut observer qu'une longue liste de routeurs différents, tels que '6WIND Turbo Router', 'Alcatel 7750', et 'Cisco 3725' (qui a été configuré précédemment), est désormais disponible pour être utilisée dans la conception et le test de réseaux. Cette liste offre à l'utilisateur une large gamme d'appareils virtuels qui peuvent être glissés-déposés dans l'espace de travail pour construire la topologie réseau souhaitée.

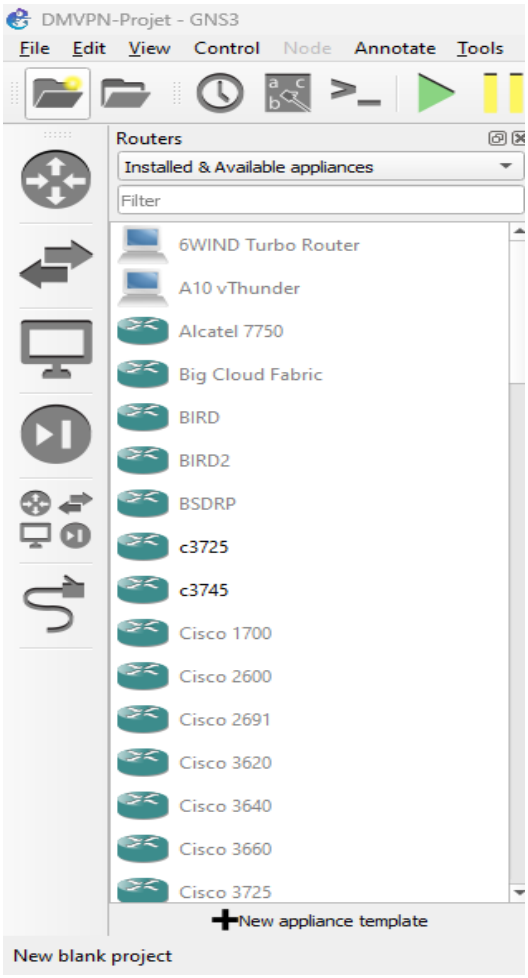

Figure 5.22: Liste des routeurs disponibles et installés dans GNS3

GNS3 est à présent configuré avec succès, ce qui nous permet d'utiliser les appliances virtuelles dédiées à la topologie du projet.

5. Déploiement du DMVPN au niveau de GNS3 :

Dans cette partie nous allons voir l'implémentation du DMVPN via ces étapes

5.1. Topologie du réseau DMVPN :

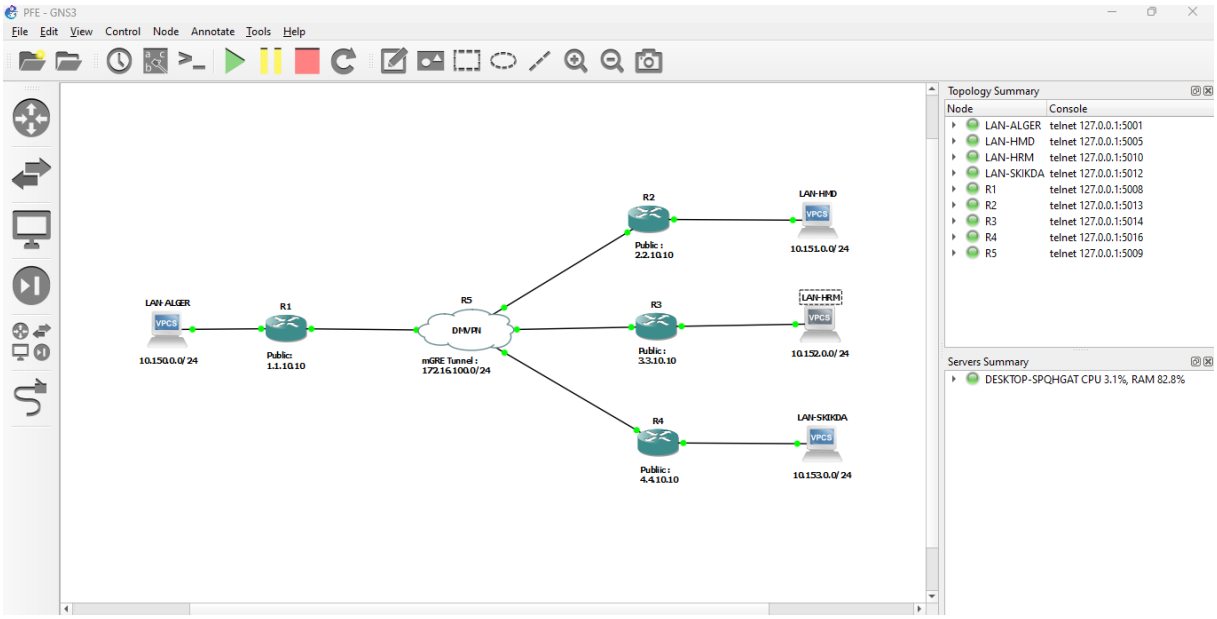

Figure 5.23 : Topologie DMVPN sur GNS3

5.1.1. Explication de topologie DMVPN :

Cette topologie présente une conception de réseau DMVPN (Dynamic Multipoint VPN) créée à l'aide du simulateur GNS3. L'objectif principal de cette topologie est de démontrer comment connecter plusieurs sites distants (Spokes (R2, R3, R4)) à un siège central (Hub (R1)) de manière sécurisée et efficace, avec la possibilité d'établir des connexions directes entre les sites distants (Spoke-to-Spoke) si nécessaire.

Analysons les composants de la topologie :

1. Composants Principaux :

R1 (Hub - Siège Central) :

- ✓ Représente le routeur central (Hub Router) qui connecte tous les sites distants.
- ✓ Possède une interface publique avec l'adresse IP : 1.1.10.10.
- ✓ Connecté au réseau LAN-ALGER (réseau local d'Alger) avec l'adresse 10.150.0.0/24 via un appareil virtuel (VPC - Virtual PC) qui représente les appareils utilisateurs de cette branche.

R2 (Spoke - Première Branche) :

- ✓ Représente un routeur de branche (Spoke Router).
- ✓ Possède une interface publique avec l'adresse IP : 2.2.10.10.
- ✓ Connecté au réseau LAN-HMD (réseau local de Hassi Messaoud) avec l'adresse 10.151.0.0/24 via un appareil virtuel (VPC).

R3 (Spoke - Deuxième Branche) :

- ✓ Représente un autre routeur de branche.
- ✓ Possède une interface publique avec l'adresse IP : 3.3.10.10.
- ✓ Connecté au réseau LAN-HRM (réseau local de Hassi RMel) avec l'adresse 10.152.0.0/24 via un appareil virtuel (VPC). (Remarque : "LAN-HRM" semble être dupliqué pour R2 et R3, il pourrait y avoir une erreur typographique dans la légende du diagramme, mais la description ici fait référence à des sites distants différents).

R4 (Spoke - Troisième Branche) :

- ✓ Représente un troisième routeur de branche.
- ✓ Possède une interface publique avec l'adresse IP : 4.4.10.10.
- ✓ Connecté au réseau LAN-SKIKDA (réseau local de Skikda) avec l'adresse 10.153.0.0/24 via un appareil virtuel (VPC).

2. Le Réseau DMVPN :

Tunnel mGRE (Multipoint GRE Tunnel) :

- ✓ C'est l'élément central du DMVPN. Un seul tunnel GRE est créé sur le routeur central (Hub) et peut accepter des connexions de plusieurs routeurs de branche (Spokes).
- ✓ Ce réseau de tunnel est indiqué par le réseau 172.16.100.0/24. C'est la plage d'adresses IP interne (overlay) qui sera utilisée pour les interfaces de tunnel sur le Hub et les Spokes.
- ✓ Ces tunnels sont établis au-dessus des connexions publiques (adresses IP publiques) entre les routeurs.

Connexions Réseau Publiques :

- ✓ Les lignes reliant R1 à R2, R3 et R4 via l'Internet (ou un réseau public simulé) représentent les connexions sous-jacentes (underlay) utilisées pour transporter le trafic DMVPN.
- ✓ Les adresses IP publiques affichées (par exemple, 1.1.10.10, 2.2.10.10, etc.) sont les adresses accessibles via le réseau public.

3. Fonctionnalités DMVPN dans cette Topologie :

Connectivité Hub-and-Spoke :

- ✓ Initialement, des tunnels VPN (généralement IPsec sur mGRE) sont établis entre chaque routeur Spoke et le Hub. Cela permet à toutes les branches de se connecter au centre et d'échanger des informations.

Connectivité Spoke-to-Spoke Dynamique:

- ✓ La principale caractéristique du DMVPN est sa capacité à permettre aux branches de communiquer directement entre elles sans avoir à faire transiter le trafic par le Hub.
- ✓ Lorsqu'un Spoke a besoin de communiquer avec un autre Spoke, il envoie une requête au Hub.
- ✓ Le Hub utilise le protocole NHRP (Next Hop Resolution Protocol) pour informer le Spoke demandeur de l'adresse IP publique du Spoke cible.
- ✓ Ensuite, le Spoke demandeur peut établir un tunnel VPN direct (tunnel dynamique) avec le Spoke cible, réduisant la latence et améliorant les performances en évitant le Hub comme point de passage unique.

Sécurité :

- ✓ Les tunnels DMVPN sont généralement sécurisés à l'aide d'IPsec (Internet Protocol Security), qui fournit le chiffrement et l'authentification des données transitant par les tunnels, rendant la communication sécurisée sur le réseau public.

Routage :

- ✓ Un protocole de routage dynamique (tel qu'EIGRP, comme mentionné dans le contexte précédent) est utilisé à l'intérieur des tunnels DMVPN pour permettre aux routeurs d'échanger des informations de route et d'accéder aux réseaux locaux de chacun (tels que 10.150.0.0/24, 10.151.0.0/24, etc.).

5.2. Configuration :

5.2.1. Configuration du Hub DMVPN - Routeur R1 :

- Configuration de l'interface physique pour le réseau LAN :

```
R1
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)# description LAN-Network
R1(config-if)# ip address 10.150.0.1 255.255.255.0
R1(config-if)# duplex auto
R1(config-if)# speed auto
R1(config-if)#!
R1(config-if)#
```

Figure 5.24 : Implémentation de l'interface pour le réseau LAN sur le router Hub

Analyse de la figure 5.24 :

Interface FastEthernet0/0 : Cette ligne définit l'interface FastEthernet0/0 qui sera utilisée pour la connexion au réseau local (LAN) du site Hub (LAN-ALGER dans la topologie).

Description LAN-Network : C'est une description pour aider à identifier le but de l'interface.

IP addresse 10.150.0.1 255.255.255.0 : Attribue l'adresse IP 10.150.0.1 et le masque de sous-réseau 255.255.255.0 (soit /24) à cette interface. C'est l'adresse IP de la passerelle par défaut pour les appareils du réseau local.

Duplex auto et speed auto : Ces commandes permettent la négociation automatique du mode duplex et de la vitesse de l'interface.

! : Indique la fin de la section de configuration de l'interface.

- Configuration de l'interface physique pour le réseau WAN (public) :

```
R1
R1(config-if)#interface FastEthernet0/1
R1(config-if)# description WAN-Network
R1(config-if)# ip address 1.1.10.10 255.255.255.0
R1(config-if)# duplex auto
R1(config-if)# duplex auto
R1(config-if)# speed auto
R1(config-if)#
```

Figure 5.25 : Implémentation de l'interface pour le réseau LAN sur le router Hub

Analyse de la figure 5.25 :

Interface FastEthernet0/1 : Cette ligne définit l'interface FastEthernet0/1 qui sera utilisée pour la connexion au réseau WAN public (Internet), à travers lequel les tunnels DMVPN seront établis.

Description WAN-Network : Description de l'interface.

ip address 1.1.10.10 255.255.255.0 : Attribue l'adresse IP publique 1.1.10.10 et le masque de sous-réseau 255.255.255.0 à cette interface. C'est l'adresse IP source du tunnel DMVPN.

Duplex auto et speed auto : Négociation automatique du mode duplex et de la vitesse.

- Configuration de l'interface tunnel mGRE (Tunnel DMVPN) :

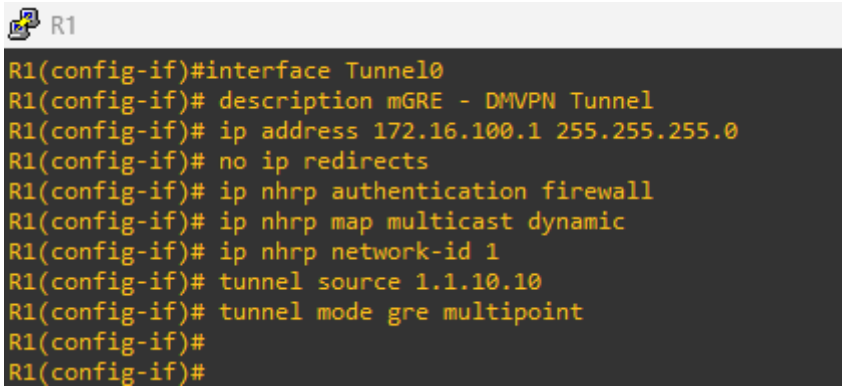

Figure 5.26 : Implémentation de tunnels mGRE sur le routeur HUB.

Analyse de la figure 5.26 :

Interface Tunnel0 : Crée et définit une interface de tunnel virtuelle nommée Tunnel0.

Description MGRE DMVPN Tunnel : Description du tunnel.

ip address 172.16.100.1 255.255.255.0: Attribue l'adresse IP 172.16.100.1 et le masque de sous-réseau 255.255.255.0 (soit/24) à l'interface du tunnel. C'est l'adresse IP "interne" ou "overlay" du Hub au sein du réseau DMVPN.

no ip redirects : Empêche le routeur d'envoyer des messages de redirection. C'est important pour éviter les problèmes dans les environnements VPN.

ip nhrp authentication firewall : Cette ligne fait référence à l'authentification NHRP. Dans une configuration standard, cela devrait être une clé secrète qui doit correspondre sur tous les routeurs participant au DMVPN. Il semble que le mot firewall ici soit la clé secrète, ou qu'il s'agisse d'un nommage non standard ou d'une erreur de frappe. La clé doit correspondre exactement sur le Hub et les Spokes.

ip nhrp map multicast dynamic : Cette commande permet au Hub d'envoyer dynamiquement le trafic multicast aux Spokes qui s'enregistrent auprès du Hub. Ceci est essentiel pour les protocoles de routage comme EIGRP ou OSPF qui s'appuient sur le multicast.

ip nhrp network-id 1: Attribue un identifiant unique à ce réseau DMVPN. Cet identifiant doit être identique sur tous les routeurs (Hub et Spokes) appartenant au même réseau DMVPN logique.

tunnel source 1.1.10.10: Cette ligne spécifie l'interface source pour le tunnel GRE. Dans ce cas, c'est l'adresse IP publique 1.1.10.10 de l'interface FastEthernet0/1.

tunnel mode gre multipoint: Spécifie que le tunnel est un tunnel GRE multipoint (mGRE). Cela permet à un seul tunnel sur le Hub de gérer les connexions de plusieurs Spokes et permet ensuite aux Spokes de construire des tunnels dynamiques entre eux.

5.2.2. Configuration des spokes DMVPN -R2 :

- Configuration de l'interface physique pour le réseau LAN :

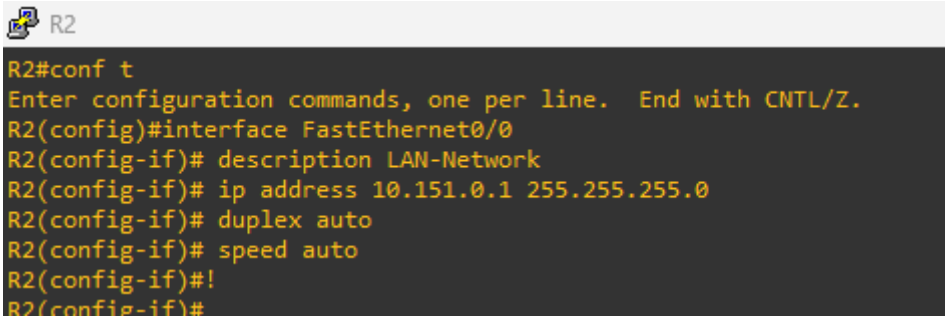

Figure 5.27 : Implémentation de l'interface pour le réseau LAN sur le router Spoke

Analyse de la figure 5.27 :

interface FastEthernet0/0: Cette commande identifie l'interface physique qui se connectera au réseau local (LAN) du site Spoke R2.

description LAN-Network: Un texte descriptif indiquant que cette interface est dédiée au réseau local. C'est très utile pour la documentation et pour faciliter le dépannage.

ip address 10.151.0.1 255.255.255.0: Attribue l'adresse IP 10.151.0.1 et le masque de sous-réseau /24 à cette interface. C'est l'adresse IP du réseau local sur le site Spoke, et elle servira généralement de passerelle par défaut pour les périphériques connectés à ce réseau.

duplex auto: Permet la négociation automatique du mode duplex (Half-Duplex ou Full-Duplex).

speed auto: Permet la négociation automatique de la vitesse de l'interface (par exemple, 10 Mbps ou 100 Mbps).

- Configuration de l'interface physique pour le réseau WAN (public) :

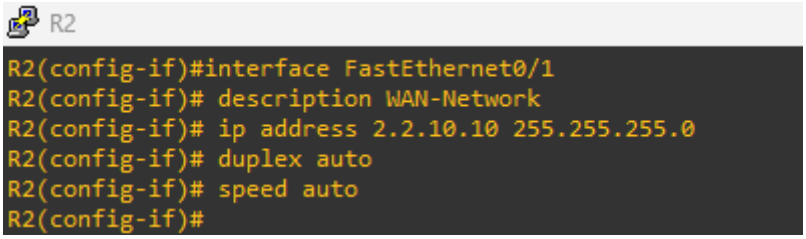

Figure 5.28 : Implémentation de l'interface pour le réseau WAN sur le router spoke

Analyse de la figure 5.28 :

Interface FastEthernet0/1 : Cette commande identifie l'interface physique qui se connectera au réseau étendu (WAN), c'est-à-dire l'Internet ou le réseau dorsal sur lequel le tunnel DMVPN transitera.

Description WAN-Network : Un texte descriptif indiquant que cette interface est dédiée au réseau WAN. C'est l'adresse "publique" ou "visible" du routeur sur Internet à laquelle le Hub se connectera.

ip address 2.2.10.10 255.255.255.0 : Attribue l'adresse IP 2.2.10.10 et le masque de sous-réseau /24 à cette interface. C'est l'adresse IP "publique" ou "externe" du routeur Spoke R2.

Duplex auto et speed auto : Fonctionnent de la même manière que pour l'interface FastEthernet0/0, facilitant la négociation automatique du mode et de la vitesse avec l'équipement WAN connecté.

- Configuration de l'interface tunnel mGRE (Tunnel DMVPN) :

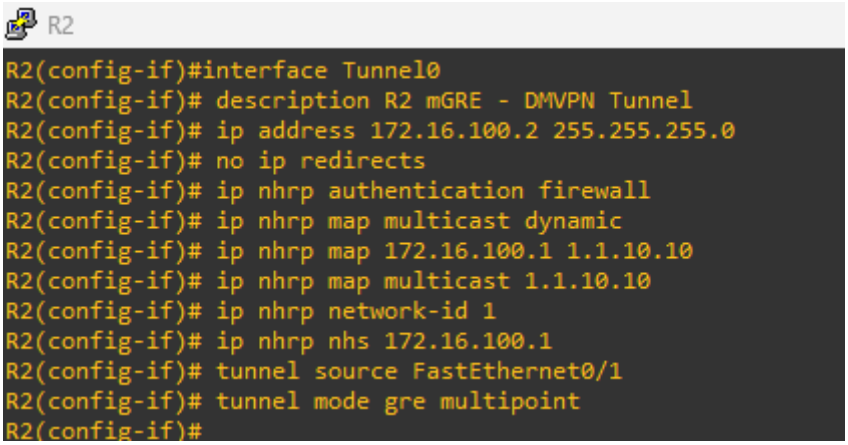

Figure 5.29 : Implémentation de tunnels mGRE sur le routeur Spoke

Analyse de la figure 5.29 :

Interface Tunnel0 : Identifie l'interface de tunnel virtuelle qui sera utilisée pour configurer le tunnel DMVPN.

Description R2 mGRE - DMVPN Tunnel : Un texte descriptif indiquant que ce tunnel est le tunnel DMVPN de Spoke R2.

ip address 172.16.100.2 255.255.255.0: Attribue l'adresse IP 172.16.100.2 et le masque de sous-réseau /24 à l'interface de tunnel. C'est l'adresse IP "interne" du tunnel de Spoke R2, et elle doit faire partie du même réseau logique que le Hub et les autres Spokes (par exemple, le réseau 172.16.100.0/24).

no ip redirects: Empêche le routeur d'envoyer des messages de redirection ICMP. C'est toujours recommandé sur les interfaces de tunnel pour éviter les problèmes de routage.

ip nhrp authentication firewall: Spécifie un mot de passe pour l'authentification entre les membres du réseau NHRP (Hubs et Spokes). Ce mot doit correspondre sur tous les périphériques DMVPN pour maintenir la sécurité. Ici, le mot est firewall.

ip nhrp map multicast dynamic: Permet au routeur de gérer dynamiquement le trafic multicast à travers le tunnel. Ceci est crucial pour les protocoles de routage comme EIGRP ou OSPF qui utilisent le multicast pour la découverte des voisins et l'échange d'informations de routage.

ip nhrp map 172.16.100.1 1.1.10.10: Il s'agit du seul mappage NHRP statique requis sur le Spoke. Il associe l'adresse IP interne du tunnel du Hub (172.16.100.1) à l'adresse IP externe/publique du Hub (1.1.10.10). Cela indique au Spoke où trouver le Hub.

ip nhrp map multicast 1.1.10.10: Dirige le trafic multicast vers l'adresse IP externe/publique du Hub (1.1.10.10).

ip nhrp network-id 1: Spécifie l'identifiant du réseau NHRP. Cet identifiant doit être identique sur tous les routeurs Hub et Spoke appartenant au même nuage DMVPN pour permettre la communication entre eux.

ip nhrp nhs 172.16.100.1: Désigne le routeur Hub comme serveur NHRP (Next Hop Server). Cette commande indique au Spoke que le Hub, dont l'adresse est 172.16.100.1, est responsable de la résolution des adresses IP des autres Spokes en leurs adresses IP publiques correspondantes.

tunnel source FastEthernet0/1: Spécifie l'interface physique FastEthernet0/1 comme source du tunnel. Cela signifie que le routeur utilisera l'adresse IP de cette interface comme adresse IP publique (externe) du tunnel DMVPN.

tunnel mode gre multipoint: Spécifie le type de tunnel comme GRE multipoint (mGRE). C'est la base du DMVPN, car cela permet à une seule interface de tunnel (sur le Hub) d'établir des connexions avec plusieurs Spokes, et permet aux Spokes de communiquer directement entre eux (Spoke-à-Spoke) avec l'aide du Hub.

5.2.3. Configuration des spokes DMVPN –R3 :

- Configuration de l'interface physique pour le réseau LAN :

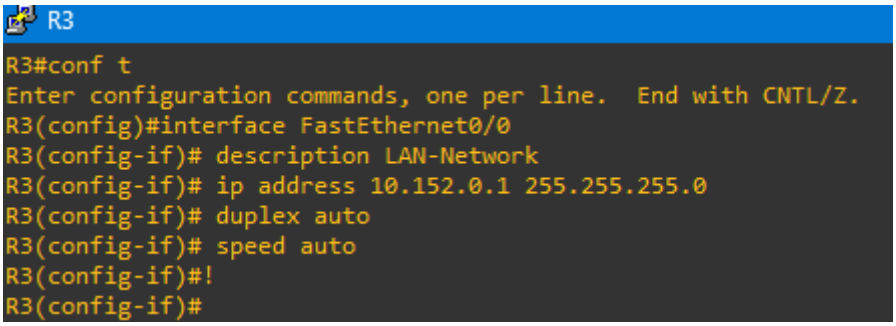

Figure 5.30: Implémentation de l'interface pour le réseau LAN sur le router Spoke

Analyse de la figure 5.30 :

interface FastEthernet0/0 : Cette ligne identifie l'interface FastEthernet0/0 qui est sélectionnée pour la configuration. C'est l'interface qui sera utilisée pour connecter le routeur R3 (désigné comme "Spoke" dans la topologie) au réseau local (LAN).

description LAN-Network: Cette commande ajoute une description à l'interface, ce qui est une bonne pratique pour documenter la configuration. Elle indique que cette interface est dédiée au "réseau LAN".

ip address 10.152.0.1 255.255.255.0 : Cette commande attribue l'adresse IP 10.152.0.1 avec un masque de sous-réseau 255.255.255.0 (ce qui correspond à un /24) à l'interface FastEthernet0/0. Cette adresse IP servira de passerelle par défaut pour tous les périphériques connectés à ce réseau local.

duplex auto et speed auto: Ces deux commandes configurent l'interface pour qu'elle négocie automatiquement le mode de communication (duplex intégral ou semi-duplex) et la vitesse de la connexion. Cela assure une compatibilité et une performance optimales avec l'équipement réseau auquel elle est connectée.

!: Ce symbole indique la fin du bloc de configuration pour l'interface spécifique et le retour au mode de configuration globale du routeur.

- Configuration de l'interface physique pour le réseau WAN (public) :

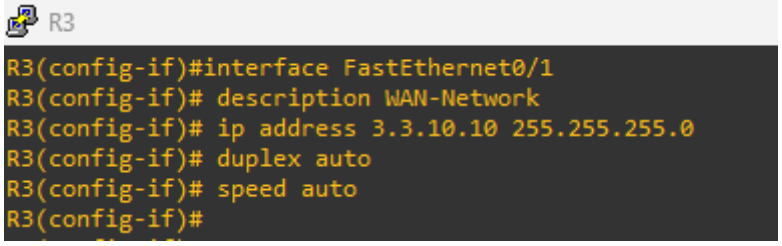

Figure 5.31: Implémentation de l'interface pour le réseau WAN sur le router spoke

Analyse de la figure 5.31 :

interface FastEthernet0/1: Cette commande identifie l'interface physique qui se connectera au réseau étendu (WAN).

description WAN-Network: Un texte descriptif indiquant que cette interface est dédiée au réseau WAN. C'est très utile pour la documentation et pour faciliter le dépannage.

ip address 3.3.10.10 255.255.255.0: Attribue l'adresse IP 3.3.10.10 et le masque de sous-réseau /24 à cette interface. C'est l'adresse IP du routeur sur le réseau WAN.

duplex auto: Permet la négociation automatique du mode duplex (Half-Duplex ou Full-Duplex).

speed auto: Permet la négociation automatique de la vitesse de l'interface (par exemple, 10 Mbps ou 100 Mbps).

- Configuration de l'interface tunnel mGRE (Tunnel DMVPN) :

R3

```
R3(config-if)#interface Tunnel0
R3(config-if)# description R3 mGRE - DMVPN Tunnel
R3(config-if)# ip address 172.16.100.3 255.255.255.0
R3(config-if)# no ip redirects
R3(config-if)# ip nhrp authentication firewall
R3(config-if)# ip nhrp map multicast dynamic
R3(config-if)# ip nhrp map 172.16.100.1 1.1.10.10
R3(config-if)# ip nhrp map multicast 1.1.10.10
R3(config-if)# ip nhrp network-id 1
R3(config-if)# ip nhrp nhs 172.16.100.1
R3(config-if)# tunnel source FastEthernet0/1
R3(config-if)# tunnel mode gre multipoint
R3(config-if)#
```

Figure 5.32: Implémentation de tunnels mGRE sur le routeur Spoke

Analyse de la figure 5.32 :

interface Tunnel0: Cette commande identifie l'interface de tunnel virtuelle, nommée "Tunnelo", qui sera utilisée pour configurer le tunnel DMVPN. C'est une interface logique créée spécifiquement pour encapsuler et transporter le trafic à travers le réseau physique sous-jacent.

description R3 mGRE - DMVPN Tunnel : Un texte descriptif est ajouté à l'interface pour indiquer clairement que ce tunnel est un tunnel DMVPN et qu'il est configuré sur le routeur R3. C'est une bonne pratique pour faciliter la gestion et le dépannage.

ip address 172.16.100.3 255.255.255.0 : Cette commande attribue l'adresse IP 172.16.100.3 avec un masque de sous-réseau 255.255.255.0 (soit/24) à l'interface Tunnelo. Cette adresse IP est l'adresse "interne" du tunnel pour le Spoke R3 et fait partie du sous-réseau logique que tous les routeurs (Hub et Spokes) du DMVPN partagent (par exemple, le réseau 172.16.100.0/24).

ip nhrp map multicast dynamic: Cette commande permet à l'interface du routeur de gérer dynamiquement le trafic multicast à travers le tunnel DMVPN via NHRP. C'est crucial car les protocoles de routage dynamique (tels qu'OSPF ou EIGRP), souvent utilisés sur les tunnels DMVPN, dépendent du multicast pour découvrir leurs voisins et échanger des informations de routage.

ip nhrp map multicast 1.1.10.10: Cette commande crée un mappage NHRP statique spécifique pour le trafic multicast. Elle associe le trafic multicast à l'adresse IP externe/publique du Hub (1.1.10.10). Cela garantit que le trafic multicast initié par le Spoke (R3) est dirigé vers le Hub, qui est ensuite responsable de le distribuer aux autres Spokes.

ip nhrp network-id 1: Cette commande spécifie l'identifiant unique du réseau NHRP pour ce domaine DMVPN. Tous les routeurs (Hubs et Spokes) qui font partie du même nuage DMVPN doivent avoir le même network-id (ici, 1) pour pouvoir établir et maintenir leurs relations NHRP et communiquer entre eux.

ip nhrp nhs 172.16.100.1: Cette commande désigne le routeur Hub comme le "Next Hop Server" (NHS) pour le Spoke R3. Le Hub, dont l'adresse IP de tunnel est 172.16.100.1, est le point central que le Spoke R3 interrogera pour résoudre les adresses IP de tunnel des autres Spokes en leurs adresses IP publiques correspondantes, permettant ainsi la formation de tunnels directs Spoke-à-Spoke.

tunnel source FastEthernet0/1: Cette commande indique l'interface physique du routeur R3 (FastEthernet0/1) qui servira de point de sortie pour le trafic encapsulé du tunnel. C'est l'interface "publique" du routeur, dont l'adresse IP est utilisée comme adresse source pour les paquets GRE.

tunnel mode gre multipoint: Cette commande configure le mode de l'interface de tunnel en "Generic Routing Encapsulation (GRE) multipoint". Ce mode est la pierre angulaire du DMVPN car il permet à un seul tunnel logique sur le Hub de supporter plusieurs destinations (Spokes) sans avoir besoin de créer un tunnel point-à-point distinct pour chaque Spoke, facilitant ainsi la scalabilité du réseau.

5.2.4. Configuration des spokes DMVPN –R4 :

- Configuration de l'interface physique pour le réseau LAN :

R4

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface FastEthernet0/0
R4(config-if)# description LAN-Network
R4(config-if)# ip address 10.153.0.1 255.255.255.0
R4(config-if)# duplex auto
R4(config-if)# speed auto
R4(config-if)#!
```

Figure 5.33: Implémentation de l'interface pour le réseau LAN sur le router Spoke

Analyse de la figure 5.33 :

interface FastEthernet0/O: Cette ligne identifie l'interface FastEthernet0/0 qui est sélectionnée pour la configuration. C'est l'interface physique qui sera utilisée pour connecter le routeur R4 (désigné comme "Spoke" dans la topologie) au réseau local (LAN) de son site.

description LAN-Network: Cette commande ajoute une description à l'interface, ce qui est une bonne pratique pour documenter la configuration. Elle indique que cette interface est dédiée au "réseau LAN".

ip address 10.153.0.1 255.255.255.0 : Cette commande attribue l'adresse IP 10.153.0.1 avec un masque de sous-réseau 255.255.255.0 (ce qui correspond à un /24) à l'interface FastEthernet0/0. Cette

adresse IP servira de passerelle par défaut pour tous les périphériques connectés à ce réseau local sur le site de R4.

duplex auto et speed auto: Ces deux commandes configurent l'interface pour qu'elle négocie automatiquement le mode de communication (duplex intégral ou semi-duplex) et la vitesse de la connexion. Cela assure une compatibilité et une performance optimales avec l'équipement réseau auquel elle est connectée (par exemple, un commutateur du LAN).

!: Ce symbole indique la fin du bloc de configuration pour l'interface spécifique et le retour au mode de configuration globale du routeur.

- Configuration de l'interface physique pour le réseau WAN (public) :

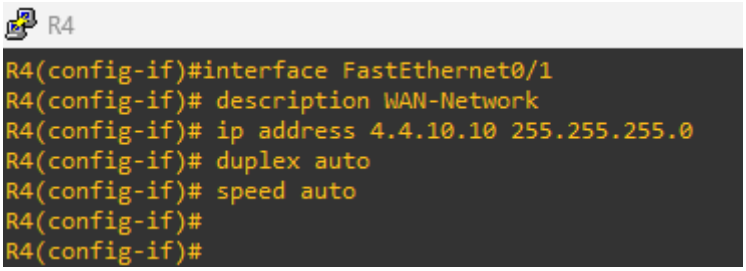

Figure 5.34: Implémentation de l'interface pour le réseau WAN sur le router spoke

Analyse de la figure 5.34:[ ]

interface FastEthernet0/1: Cette commande identifie l'interface physique FastEthernet0/1 qui se connectera au réseau étendu (WAN) pour le routeur R4.

description WAN-Network: Un texte descriptif indiquant que cette interface est dédiée au réseau WAN. C'est très utile pour la documentation et pour faciliter le dépannage.

ip address 4.4.10.10 255.255.255.0: Attribue l'adresse IP 4.4.10.10 et le masque de sous-réseau /24 à cette interface. C'est l'adresse IP du routeur R4 sur le réseau WAN.

duplex auto: Permet la négociation automatique du mode duplex (Half-Duplex ou Full-Duplex) avec l'équipement distant sur le lien WAN.

speed auto: Permet la négociation automatique de la vitesse de l'interface (par exemple, 10 Mbps ou 100 Mbps) avec l'équipement distant sur le lien WAN.

- Configuration de l'interface physique pour le réseau LAN :

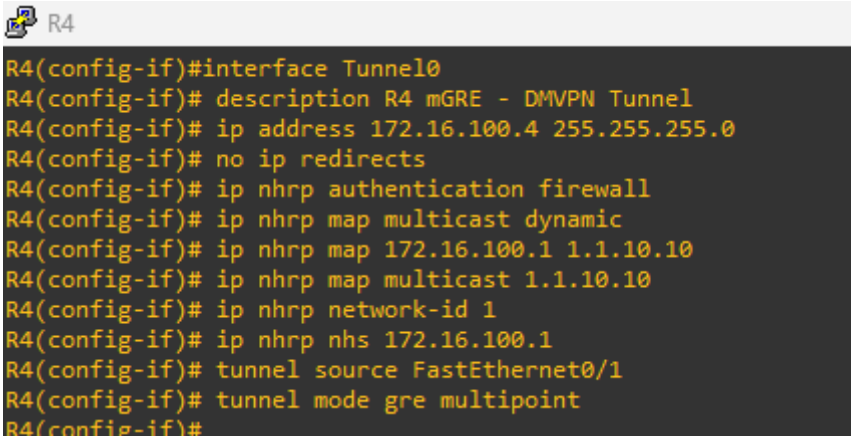

Figure 5.35: Implémentation de tunnels mGRE sur le routeur Spoke

Analyse de la figure 5.35 :[ ]

interface Tunnel0 : Cette commande identifie l'interface de tunnel virtuelle, nommée "Tunnel0", qui sera utilisée pour configurer le tunnel DMVPN. C'est une interface logique créée spécifiquement pour encapsuler et transporter le trafic à travers le réseau physique sous-jacent.

description R4 mGRE - DMVPN Tunnel : Un texte descriptif est ajouté à l'interface pour indiquer clairement que ce tunnel est un tunnel DMVPN et qu'il est configuré sur le routeur R4. C'est une bonne pratique pour faciliter la gestion et le dépannage.

ip address 172.16.100.4 255.255.255.0 : Cette commande attribue l'adresse IP 172.16.100.4 avec un masque de sous-réseau 255.255.255.0 (soit /24) à l'interface Tunnel0. Cette adresse IP est l'adresse "interne" du tunnel pour le Spoke R4 et fait partie du sous-réseau logique que tous les routeurs (Hub et Spokes) du DMVPN partagent (par exemple, le réseau 172.16.100.0/24).

no ip redirects : Cette commande permet à l'interface du routeur de gérer dynamiquement le trafic multicast à travers le tunnel DMVPN via NHRP. C'est crucial car les protocoles de routage dynamique (tels qu'OSPF ou EIGRP), souvent utilisés sur les tunnels DMVPN, dépendent du multicast pour découvrir leurs voisins et échanger des informations de routage.

ip nhrp authentication firewall : Spécifie un mot de passe pour l'authentification entre les membres du réseau NHRP (Hubs et Spokes). Ce mot doit correspondre sur tous les périphériques DMVPN pour maintenir la sécurité. Ici, le mot est "firewall".

ip nhrp map multicast dynamic : Cette commande permet au routeur de gérer dynamiquement le trafic multicast à travers le tunnel. Ceci est crucial pour les protocoles de routage comme EIGRP ou OSPF qui utilisent le multicast pour la découverte des voisins et l'échange d'informations de routage. ip nhrp map multicast 1.1.10.10 : Cette commande crée un mappage NHRP statique spécifique pour le trafic multicast. Elle associe le trafic multicast à l'adresse IP externe/publique du Hub (1.1.10.10). Cela garantit que le trafic multicast initié par le Spoke (R4) est dirigé vers le Hub, qui est ensuite responsable de le distribuer aux autres Spokes.

ip nhrp network-id 1 : Cette commande spécifie l'identifiant unique du réseau NHRP pour ce domaine DMVPN. Tous les routeurs (Hubs et Spokes) qui font partie du même nuage DMVPN doivent avoir le même network-id (ici, 1) pour pouvoir établir et maintenir leurs relations NHRP et communiquer entre eux.

ip nhrp nhs 172.16.100.1 : Cette commande désigne le routeur Hub comme le Next Hop Server (NHS) pour le Spoke R4. Le Hub, dont l'adresse IP de tunnel est 172.16.100.1, est le point central que le Spoke R4 interrogera pour résoudre les adresses IP de tunnel des autres Spokes en leurs adresses IP publiques correspondantes, permettant ainsi la formation de tunnels directs Spoke-à-Spoke.

tunnel source FastEthernet0/1 : Cette commande indique l'interface physique du routeur R4 (FastEthernet0/1) qui servira de point de sortie pour le trafic encapsulé du tunnel. C'est l'interface "publique" du routeur.

tunnel mode gre multipoint : Configure le mode du tunnel en Generic Routing Encapsulation (GRE) multipoint. Ce mode permet à un seul tunnel logique de supporter plusieurs connexions point-à-point dynamiques, ce qui est la base du fonctionnement de DMVPN.

5.2.5. Configuration de mGRE Tunnel DMVPN –R5 :

- Configuration des interfaces physiques (FastEthernet) sur le routeur R5 :

```
R5
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#int f0/1
R5(config-if)#IP ADD 1.1.10.11 255.255.255.0
R5(config-if)#NO SH
R5(config-if)#EXIT
R5(config)#
*Mar  1 00:01:48.451: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:01:49.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R5(config)#INT F1/1
R5(config-if)#NO SWITCH
R5(config-if)#NO SWITCHport
R5(config-if)#IP
*Mar  1 00:02:30.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/1, changed state to up
R5(config-if)#IP ADD 2.2.10.11 255.255.255.0
R5(config-if)#EXIT
R5(config)#INT F1/2
R5(config-if)#NO SWITCHPORT
R5(config-if)#IP ADD
*Mar  1 00:03:04.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/2, changed state to up
R5(config-if)#IP ADD 3.3.10.11 255.255.255.0
R5(config-if)#EXIT
R5(config)#INT F1/3
R5(config-if)#NO SWITCHPORT
R5(config-if)#IP ADD
*Mar  1 00:03:42.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/3, changed state to up
R5(config-if)#IP ADD 4.4.10.11 255.255.255.0
R5(config-if)#EXIT
R5(config)#
```

Figure 5.36: Implémentation de la configuration des interfaces physiques sur le routeur R5

Analyse de la figure 5.36 : []

R5#conf t : Cette commande est utilisée pour passer du mode EXEC privilégié (#) au mode de configuration globale ((config)#) sur le routeur R5. C'est la première étape nécessaire pour apporter des modifications à la configuration du routeur.

R5 (config)#int f0/1 : Cette commande permet d'entrer dans le mode de configuration de l'interface FastEthernet0/1 ((config-if)#). C'est le mode spécifique pour configurer les paramètres de cette interface.

R5 (config-if)#ip address 1.1.10.11 255.255.255.0 : Cette commande attribue l'adresse IPv4 1.1.10.11 avec le masque de sous-réseau 255.255.255.0 (équivalent à /24 en notation CIDR) à l'interface FastEthernet0/1. C'est l'identifiant unique de cette interface sur le réseau 1.1.10.0.

R5 (config-if)#NO SH (ou no shutdown) : Bien que l'intégralité de la commande no shutdown ne soit pas visible, les messages de log qui suivent confirment son exécution. Cette commande active l'interface. Par défaut, les interfaces physiques des routeurs Cisco sont administrativement désactivées (shutdown).

Messages de log pour f0/1 :

- *Mar 1 00:01:48.451: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up : Ce message indique que la couche physique (Couche 1 du modèle OSI) de l'interface est passée à l'état "up". Cela signifie que la connexion physique est détectée (câble branché).
- *Mar 1 00:01:49.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up : Ce message indique que le protocole de ligne (Couche 2 du modèle OSI) de l'interface est également passé à l'état "up". Cela signifie que l'interface est prête à échanger des trames de données. Une interface est pleinement opérationnelle ("up/up") lorsque les deux couches sont "up".

R5 (config-if)#EXIT : Permet de quitter le mode de configuration d'interface et de retourner au mode de configuration globale.

Configuration des interfaces FastEthernet1/1 (f1/1), FastEthernet1/2 (f1/2) et FastEthernet1/3 (f1/3) : Les mêmes étapes sont répétées pour ces trois interfaces, mais avec des adresses IP différentes :

- f1/1 : ip address 2.2.10.11 255.255.255.0
- f1/2 : ip address 3.3.10.11 255.255.255.0
- f1/3 : ip address 4.4.10.11 255.255.255.0

Pour chacune de ces interfaces, la commande R5 (config-if)#NO SWITCHPORT est explicitement utilisée.

no switchport : Cette commande est cruciale sur les interfaces FastEthernet d'un routeur qui pourraient, par défaut ou par leur nature, se comporter comme des ports de commutation (Couche 2). En la désactivant, on force l'interface à fonctionner en mode de couche 3 (routage), permettant l'attribution d'adresses IP et la participation au processus de routage. C'est essentiel pour qu'un routeur puisse acheminer le trafic entre différents sous-réseaux.

Des messages de log similaires (%LINEPROTO-5-UPDOWN) confirment que les protocoles de ligne de ces interfaces sont également passés à l'état "up" après l'attribution des adresses IP et l'activation.

- Configuration du routage OSPF sur R5 :

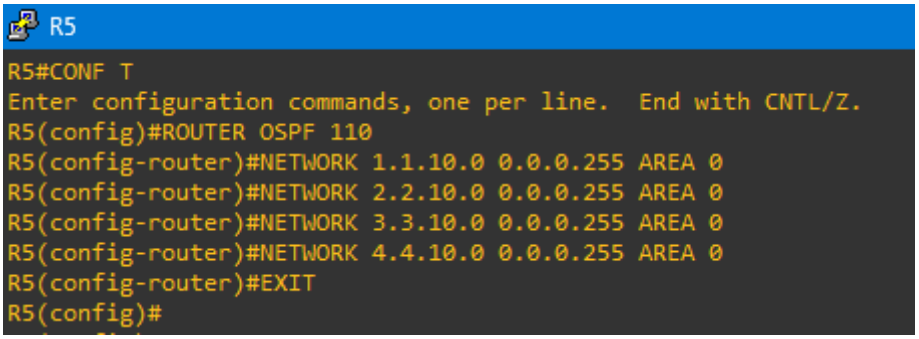

Figure 5.37: Implémentation du routage OSPF sur le routeur R5

Analyse de la figure 5.37 :[ ]

R5#CONF T : Cette commande est exécutée depuis le mode privilégié (#) et permet de passer en mode de configuration globale ((config)#). C'est la première étape pour apporter des modifications à la configuration du routeur.

R5 (config)#ROUTER OSPF 110 :

- Cette commande active le processus de routage OSPF sur le routeur R5.
- ROUTER OSPF est la commande pour spécifier que l'on configure OSPF.
- 110 est l'ID du processus OSPF. Cet ID est local au routeur et n'a pas besoin d'être le même sur tous les routeurs d'un même domaine OSPF, bien qu'il soit souvent conservé identique pour des raisons de cohérence et de facilité de gestion.

R5 (config-router)#NETWORK 1.1.10.0 0.0.0.255 AREA 0 :

- Cette commande est utilisée pour annoncer un réseau spécifique dans le domaine OSPF.
- NETWORK est la commande pour inclure des interfaces dans le processus OSPF.
- 1.1.10.0 est l'adresse réseau.
- 0.0.0.255 est le masque générique (wildcard mask). Ce masque est l'inverse du masque de sous-réseau. Pour un masque de sous-réseau de 255.255.255.0 (qui correspond à un /24), le masque générique est 0.0.0.255. Il indique que seuls les bits correspondants aux zéros du masque générique doivent correspondre exactement, tandis que les bits correspondants aux uns peuvent varier. Dans ce cas, cela signifie que toutes les interfaces dont l'adresse IP appartient au réseau 1.1.10.0/24 seront incluses dans OSPF.
- AREA 0 spécifie que ce réseau appartient à la zone OSPF 0 (l'Area Backbone). Dans OSPF, la zone 0 est la zone principale et toutes les autres zones doivent lui être connectées directement ou logiquement.

R5 (config-router)#NETWORK 2.2.10.0 0.0.0.255 AREA 0

R5 (config-router)#NETWORK 3.3.10.0 0.0.0.255 AREA 0

R5 (config-router)#NETWORK 4.4.10.0 0.0.0.255 AREA 0

- Ces commandes sont identiques à la précédente, annonçant respectivement les réseaux 2.2.10.0/24, 3.3.10.0/24 et 4.4.10.0/24 dans la zone OSPF 0. Cela signifie que les interfaces de R5 connectées à ces réseaux participeront au routage OSPF et échangeront des informations de routage avec d'autres routeurs OSPF dans la même zone.

R5 (config-router)#EXIT : Cette commande permet de quitter le mode de configuration du routeur OSPF et de revenir au mode de configuration globale ((config)#).

En résumé :

Cette configuration OSPF sur R5 a pour objectif de :

- Activer le protocole OSPF avec un ID de processus 110.
- Inclure quatre réseaux distincts (1.1.10.0/24, 2.2.10.0/24, 3.3.10.0/24, 4.4.10.0/24) dans la zone 0 d'OSPF. Cela permettra à R5 de former des adjacences OSPF avec d'autres routeurs connectés à ces réseaux et d'échanger des informations de routage pour assurer la connectivité au sein du domaine OSPF.

5.2.6. Protection - Chiffrement des tunnels DMVPN MGRE avec IPSec :

- Configuration du routeur hub R1 de notre siège :

```
R1
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#!
R1(config-isakmp)#crypto isakmp key firewall.cx address 0.0.0.0
A pre-shared key for address mask 0.0.0.0 0.0.0.0 already exists!

R1(config)#!
R1(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#!
R1(cfg-crypto-trans)#crypto ipsec profile protect-gre
R1(ipsec-profile)#set security-association lifetime seconds 86400
R1(ipsec-profile)#set transform-set TS
R1(ipsec-profile)#!
R1(ipsec-profile)#interface Tunnel 0
R1(config-if)#tunnel protection ipsec profile protect-gre
R1(config-if)#
R1(config-if)#
R1(config-if)#exit
R1(config)#exit
R1#wr
*Mar  1 00:00:51.503: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
```

Figure 5.38: Implémentation du chiffrement IPSec sur le routeur hub R1

A**nalyse de la figure 5.38: [ ]**

R1#conf t : Passe le routeur en mode de configuration globale (abrégé "conf t").

R1 (config)#crypto isakmp policy 1 : Cette commande initie la configuration d'une politique ISAKMP (Internet Security Association and Key Management Protocol), qui est la phase 1 du protocole IKE (Internet Key Exchange). L'ID de la politique est 1. ISAKMP est responsable de l'établissement d'une SA (Security Association) sécurisée entre les pairs, utilisée ensuite pour négocier la phase 2 (IPSec).

R1 (config-isakmp)#encr 3des : Définit l'algorithme de chiffrement pour la phase 1. Ici, 3des (Triple DES) est utilisé.

R1 (config-isakmp)#hash md5 : Spécifie l'algorithme de hachage (intégrité) pour la phase 1. Ici, md5 est utilisé.

R1 (config-isakmp)#authentication pre-share : Définit la méthode d'authentification entre les pairs. pre-share signifie qu'une clé pré-partagée sera utilisée.

R1 (config-isakmp)#group 2 : Spécifie le groupe Diffie-Hellman (DH) à utiliser pour l'échange de clés sécurisé. Le groupe 2 est un groupe de 1024 bits.

R1 (config-isakmp)#lifetime 86400 : Définit la durée de vie (en secondes) de la SA ISAKMP. Ici, 86400 secondes (soit 24 heures).

R1 (config)#crypto isakmp key firewall.cx address 0.0.0.0 : Configure la clé pré-partagée (firewall.cx) qui sera utilisée pour l'authentification avec n'importe quel pair (address 0.0.0.0). L'adresse 0.0.0.0 avec un masque de 0.0.0.0 (implicite ici) signifie que cette clé est globale et sera utilisée pour tous les pairs IPSec qui n'ont pas de clé plus spécifique configurée.

R1 (config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac :

- Crée un ensemble de transformations IPSec (transform-set) nommé TS. Cet ensemble définit les paramètres de la phase 2 d'IPSec.
- esp-3des : Utilise ESP (Encapsulating Security Payload) avec l'algorithme de chiffrement 3DES pour protéger les données.
- esp-md5-hmac : Utilise ESP avec l'algorithme de hachage MD5 (HMAC pour la vérification de l'intégrité) pour l'authentification des données.

R1 (config)#crypto ipsec profile protect-gre : Crée un profil IPSec nommé protect-gre. Ce profil regroupe les politiques IPSec et est ensuite appliqué à l'interface de tunnel.

R1 (ipsec-profile)#set security-association lifetime seconds 86400 : Définit la durée de vie (en secondes) de la SA IPSec (Phase 2) à 86400 secondes.

R1 (ipsec-profile)#set transform-set TS : Associe le transform-set TS créé précédemment à ce profil IPSec.

R1 (config)#interface Tunnel 0 : Passe en mode de configuration de l'interface de tunnel 0. C'est une interface logique utilisée pour encapsuler le trafic.

R1 (config-if)#tunnel protection ipsec profile protect-gre : Applique le profil IPSec protect-gre à l'interface Tunnel 0. Cela indique que tout le trafic passant par cette interface de tunnel sera protégé par IPSec selon les paramètres définis dans le profil.

R1 (config-if)#exit : Quitte le mode de configuration de l'interface.

R1 (config)#exit : Quitte le mode de configuration globale.

R1#wr :

- Commande abrégée de write memory ou copy running-config startup-config. Elle permet de sauvegarder la configuration en cours d'exécution dans la mémoire non volatile (NVRAM) du routeur, assurant ainsi que la configuration est conservée après un redémarrage.
- Le message "Building configuration..." suivi de "[OK]" confirme que la sauvegarde a réussi.

En résumé :

Cette figure montre l'implémentation complète d'un ensemble de règles IPSec (ISAKMP Phase 1 et IPSec Phase 2) sur le routeur R1, pour sécuriser une interface de tunnel (probablement une interface GRE utilisée dans un contexte DMVPN). Le routeur R1 est configuré pour négocier des SA ISAKMP et IPSec en utilisant des algorithmes et des durées de vie spécifiques, et à appliquer cette protection à tout le trafic passant par l'interface Tunnel 0. C'est une étape cruciale pour garantir la confidentialité et l'intégrité des données transitant via le tunnel.

- Configuration des routeurs spoke R2, R3 et R4 :

La configuration suivante s'applique aux routeurs spoke R2,R3 et R4

R2

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr 3des
R2(config-isakmp)#encr 3des
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#!
R2(config-isakmp)#crypto isakmp key firewall.cx address 0.0.0.0 0.0.0.0
A pre-shared key for address mask 0.0.0.0 0.0.0.0 already exists!

R2(config)#!
R2(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R2(cfg-crypto-trans)#!
R2(cfg-crypto-trans)#crypto ipsec profile protect-gre
R2(ipsec-profile)#set security-association lifetime seconds 86400
R2(ipsec-profile)#set transform-set TS
R2(ipsec-profile)#!
R2(ipsec-profile)#interface Tunnel 0
R2(config-if)#tunnel protection ipsec profile protect-gre
R2(config-if)#
R2(config-if)#exit
R2(config)#exit
R2#
*Mar  1 00:37:10.531: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Building configuration...
[OK]
R2#
```

Figure 5.39: Implémentation du chiffrement IPSec sur le routeur spoke R2

Analyse de la figure 5.39: [ ]

L'analyse de cette figure est identique à celle de la figure 39, car la configuration présentée est la même.

5.2.7. Routage entre les tunnels DMVPN MGRE :

- Sur le router Hub R1:

```
R1
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 10.151.0.0 255.255.255.0 172.16.100.2
R1(config)#ip     route    10.152.0.0     255.255.255.0    172.16.100.3
R1(config)#ip     route    10.153.0.0     255.255.255.0    172.16.100.4
R1(config)#exit
R1#
*Mar  1 00:46:22.331: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
```

Figure 5.40: Implémentation des routes statiques sur le routeur Hub R1

Analyse de la figure 5.40: [ ]

R1#conf t : Cette commande est utilisée pour passer en mode de configuration globale sur le routeur R1.

R1 (config)#ip route 10.151.0.0 255.255.255.0 172.16.100.2 :

- Cette commande configure une route statique sur R1.
- ip route: La commande pour définir une route statique.
- 10.151.0.0: L'adresse du réseau de destination. Il s'agit probablement du réseau LAN derrière le routeur spoke R2.
- 255.255.255.0: Le masque de sous-réseau pour le réseau de destination (/24).
- 172.16.100.2: L'adresse IP du prochain saut (next-hop). Dans une configuration DMVPN, cette adresse correspond à l'adresse IP de l'interface de tunnel du routeur spoke R2. Cela signifie que tout trafic destiné au réseau 10.151.0.0/24 sera envoyé à travers le tunnel vers le routeur spoke R2.

R1 (config)#ip route 10.152.0.0 255.255.255.0 172.16.100.3 : Similaire à la commande précédente, cette route statique est configurée pour le réseau 10.152.0.0/24 (probablement derrière R3), avec le next-hop 172.16.100.3, qui est l'adresse IP de l'interface de tunnel du routeur spoke R3.

R1 (config)#ip route 10.153.0.0 255.255.255.0 172.16.100.4 : De même, cette route statique est configurée pour le réseau 10.153.0.0/24 (probablement derrière R4), avec le next-hop 172.16.100.4, qui est l'adresse IP de l'interface de tunnel du routeur spoke R4.

R1 (config)#exit : Permet de quitter le mode de configuration globale.

R1#wr :

- Commande abrégée de write memory ou copy running-config startup-config. Elle sauvegarde la configuration en cours d'exécution dans la mémoire non volatile (NVRAM) du routeur, assurant sa persistance après un redémarrage.
- Les messages "Building configuration..." et "[OK]" confirment la réussite de la sauvegarde.

➢ Sur le router spoke R2 :

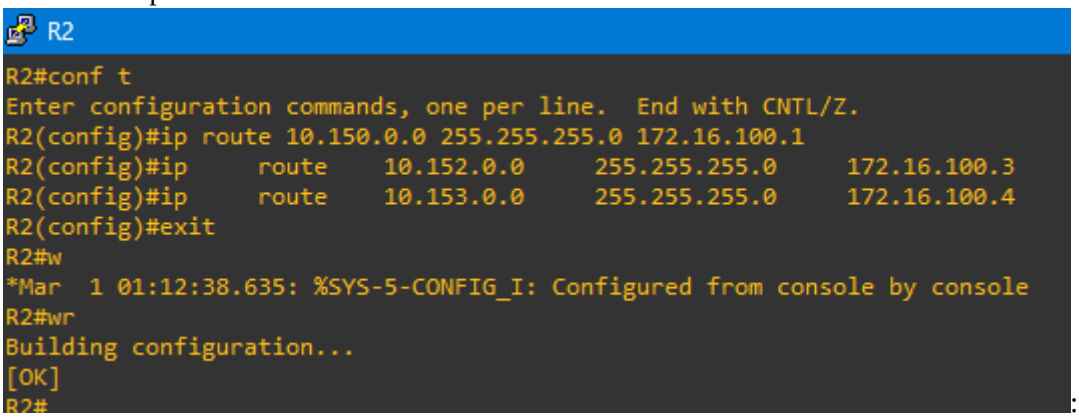

Figure 5.41: Implémentation des routes statiques sur le routeur spoke R2

Analyse de la figure 5.41: [ ]

R2#conf t : Cette commande est utilisée pour passer du mode EXEC privilégié au mode de configuration globale sur le routeur R2. C'est la première étape nécessaire pour apporter des modifications à la configuration du routeur.

R2 (config)#ip route 10.150.0.0 255.255.255.0 172.16.100.1 :

- Cette commande configure une route statique sur R2.
- ip route : La commande de base pour définir une route statique.
- 10.150.0.0 : L'adresse du réseau de destination. Il s'agit du réseau 10.150.0.0.
- 255.255.255.0 : Le masque de sous-réseau pour le réseau de destination (/24). Il indique que le routeur doit acheminer les paquets dont les 24 premiers bits de l'adresse IP de destination correspondent à 10.150.0.0 vers le prochain saut spécifié.
- 172.16.100.1 : L'adresse IP du prochain saut (next-hop). Pour que R2 atteigne le réseau 10.150.0.0, il doit envoyer les paquets à cette adresse IP. Dans une topologie Hub-and-Spoke (comme suggéré par "spoke R2"), cette adresse correspondrait probablement à l'adresse IP d'une interface sur le routeur central (Hub) ou un autre routeur via lequel le trafic pour 10.150.0.0 doit passer. Cela signifie que tout trafic destiné au réseau 10.150.0.0/24 sera envoyé à travers l'interface de R2 qui est joignable par 172.16.100.1.

R2 (config)#ip route 10.152.0.0 255.255.255.0 172.16.100.3 :

- Similaire à la commande précédente, cette route statique est configurée pour le réseau 10.152.0.0/24.
- Le next-hop pour ce réseau est 172.16.100.3. Cela implique que R2 utilise un chemin différent ou une interface spécifique pour atteindre ce réseau via cette adresse IP de prochain saut.

R2 (config)#ip route 10.153.0.0 255.255.255.0 172.16.100.4 :

- De même, cette route statique est configurée pour le réseau 10.153.0.0/24.
- Le next-hop pour ce réseau est 172.16.100.4. Cela montre que R2 a besoin de routes explicites pour atteindre ces différents réseaux, probablement situés derrière le routeur central ou d'autres spokes dans la topologie.

R2 (config)#exit : Permet de quitter le mode de configuration globale et de retourner au mode EXEC privilégié.

R2#wr :

- Cette commande est l'abréviation de write memory ou copy running-config startup-config.
- Elle sauvegarde la configuration active (running-config) qui est en RAM vers la mémoire non volatile (NVRAM) du routeur. Cela garantit que la configuration sera conservée et rechargée automatiquement au prochain redémarrage du routeur. Sans cette commande, toutes les modifications apportées seraient perdues en cas de redémarrage ou de coupure de courant.
- Le message Building configuration... [OK] confirme que la sauvegarde a été effectuée avec succès.

➢ Sur le router spoke R3 :

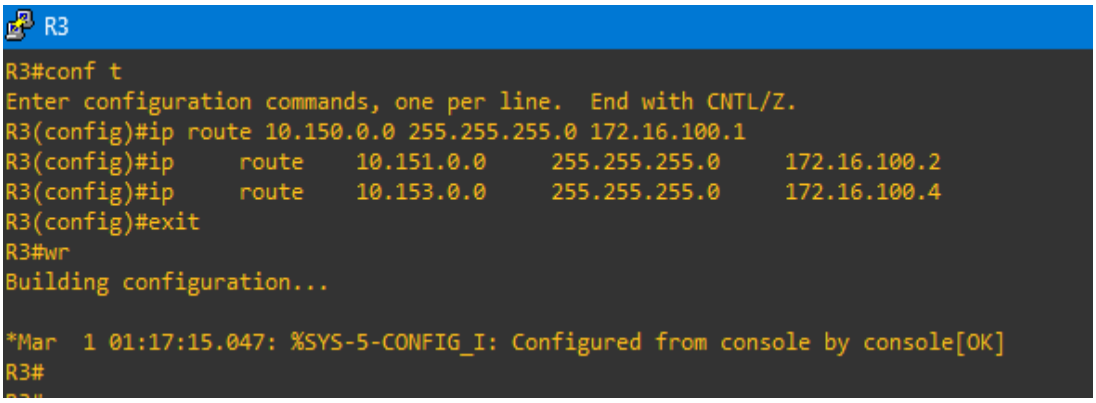

Figure 5.42: Implémentation des routes statiques sur le routeur spoke R3

Analyse de la figure 5.42: [ ]

R3#conf t : Cette commande est utilisée pour passer du mode EXEC privilégié (#) au mode de configuration globale ((config)#) sur le routeur R3. C'est l'étape initiale et nécessaire pour toute modification de la configuration du routeur.

R3(config)#ip route 10.150.0.0 255.255.255.0 172.16.100.1 :

- Cette commande configure une route statique sur R3.
- ip route : C'est la commande principale utilisée pour définir une route statique.
- 10.150.0.0 : Représente l'adresse du réseau de destination. Il s'agit du réseau 10.150.0.0. Le routeur R3 apprend que pour envoyer du trafic à ce réseau, il doit suivre cette route.
- 255.255.255.0 : C'est le masque de sous-réseau (/24) du réseau de destination. Il indique que R3 doit faire correspondre les 24 premiers bits de l'adresse IP de destination d'un paquet pour qu'il soit routé via cette entrée.
- 172.16.100.1 : C'est l'adresse IP du prochain saut (next-hop). Pour que R3 puisse atteindre le réseau 10.150.0.0, tous les paquets destinés à ce réseau seront envoyés à l'adresse IP 172.16.100.1. Dans une topologie Hub-and-Spoke, cette adresse correspondrait typiquement à une interface sur le routeur central (Hub) ou un autre point d'accès via lequel les réseaux distants sont joignables.

R3(config)#ip route 10.151.0.0 255.255.255.0 172.16.100.2 :

- Cette commande configure une deuxième route statique pour le réseau de destination 10.151.0.0/24.
- Le prochain saut pour ce réseau est 172.16.100.2. Cela signifie que R3 utilise un chemin différent, ou un autre point d'accès sur le routeur central, pour atteindre ce réseau.

R3(config)#ip route 10.153.0.0 255.255.255.0 172.16.100.4 :

- Une troisième route statique est configurée pour le réseau 10.153.0.0/24.
- Le prochain saut pour ce réseau est 172.16.100.4. Cette configuration met en évidence que R3 a besoin de routes explicites pour atteindre ces réseaux spécifiques, qui sont probablement des segments de réseau situés derrière le routeur central ou d'autres spokes dans la même topologie.

R3(config)#exit : Permet de quitter le mode de configuration globale et de revenir au mode EXEC privilégié.

R3#wr :

- Cette commande est une abréviation de write memory ou copy running-config startup-config.
- Elle sauvegarde la configuration active (qui est volatile et se trouve en RAM) vers la mémoire non volatile (NVRAM) du routeur. Cette étape est cruciale car elle garantit que la configuration sera rechargée automatiquement après un redémarrage du routeur ou une coupure de courant, évitant ainsi la perte des configurations appliquées.

- Le message Building configuration... [OK] confirme que la sauvegarde a été effectuée avec succès.

➢ Sur le router spoke R4 :

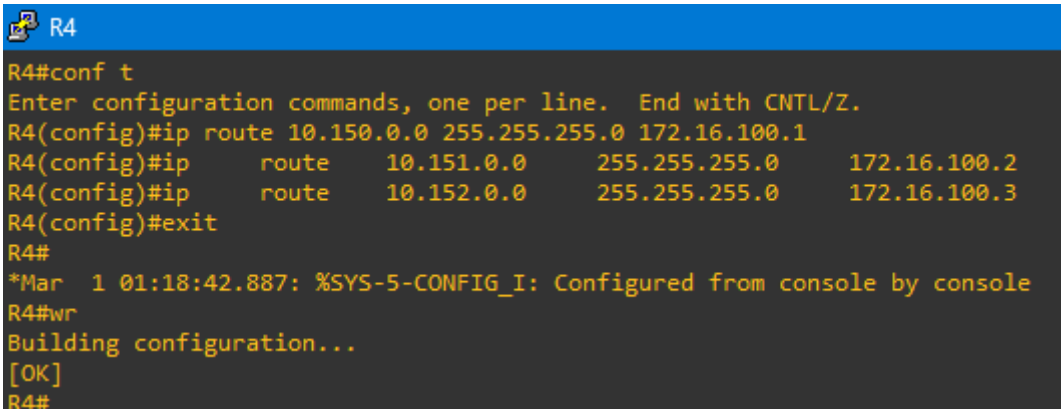

Figure 5.43: Implémentation des routes statiques sur le routeur spoke R4

Analyse de la figure 5.43: [ ]

R4#conf t : Cette commande est utilisée pour passer du mode EXEC privilégié (#) au mode de configuration globale ((config)#) sur le routeur R4. C'est l'étape préliminaire nécessaire pour apporter des modifications à la configuration du routeur.

R4 (config)#ip route 10.150.0.0 255.255.255.0 172.16.100.1 :

- Cette commande configure une route statique sur R4.
- ip route : C'est la commande fondamentale pour définir une route statique.
- 10.150.0.0 : Représente l'adresse du réseau de destination. Il s'agit du réseau 10.150.0.0. Le routeur R4 est instruit que pour envoyer du trafic à ce réseau, il doit utiliser cette route.
- 255.255.255.0 : C'est le masque de sous-réseau (/24) du réseau de destination. Il indique que R4 doit faire correspondre les 24 premiers bits de l'adresse IP de destination d'un paquet pour qu'il soit routé via cette entrée.
- 172.16.100.1 : C'est l'adresse IP du prochain saut (next-hop). Pour que R4 puisse atteindre le réseau 10.150.0.0, tous les paquets destinés à ce réseau seront transférés à l'adresse IP 172.16.100.1. Dans une topologie Hub-and-Spoke, cette adresse correspondrait typiquement à l'adresse IP d'une interface sur le routeur central (Hub) ou un autre point d'interconnexion par lequel les réseaux distants sont joignables. Cela signifie que tout trafic destiné au réseau 10.150.0.0/24 sera envoyé via l'interface de R4 qui est joignable par 172.16.100.1.

R4 (config)#ip route 10.151.0.0 255.255.255.0 172.16.100.2 :

- Similaire à la commande précédente, cette route statique est configurée pour le réseau 10.151.0.0/24.
- Le next-hop pour ce réseau est 172.16.100.2. Ceci suggère un autre chemin ou un autre point d'accès sur le routeur central ou un autre spoke pour atteindre ce réseau.

R4 (config)#ip route 10.152.0.0 255.255.255.0 172.16.100.3 :

- De même, cette route statique est configurée pour le réseau 10.152.0.0/24.
- Le next-hop pour ce réseau est 172.16.100.3. Cette configuration montre que R4 a besoin de routes explicites pour atteindre ces différents réseaux, qui sont probablement des segments de réseau situés derrière le routeur central ou d'autres spokes dans la même topologie.

R4 (config)#exit : Permet de quitter le mode de configuration globale et de retourner au mode EXEC privilégié.

R4#wr :

- Cette commande est l'abréviation de write memory ou copy running-config startup-config.
- Elle sauvegarde la configuration active (qui réside en RAM et est donc volatile) vers la mémoire non volatile (NVRAM) du routeur. Cette étape est cruciale pour assurer que la configuration appliquée persiste après un redémarrage du routeur ou une coupure de courant.
- Le message Building configuration... [OK] confirme que la sauvegarde a été effectuée avec succès.

5.2.8. Déploiement du protocole OSPF pour le réseau DMVPN (R1, R2, R3, R4) :

- Sur le router Hub R1 :

```
R1
R1#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ROUTER OSPF 110
R1(config-router)#NETWORK 1.1.10.0 0.0.0.255 AREA 0
R1(config-router)#NETWORK 10.150.0.0 0.0.0.255 AREA 0
R1(config-router)#EXIT
R1(config)#EXIT
R1#W
*Mar  1 00:04:05.959: %SYS-5-CONFIG_I: Configured from console by console
R1#WR
Building configuration...
[OK]
R1#
```

Figure 5.44: Implémentation de OSPF sur le router Hub-R1

- Sur le router spoke R2 :

```
R2
R2#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ROUTER OSPF 110
R2(config-router)#NETWORK 2.2.10.0 0.0.0.255 AREA 0
R2(config-router)#NETWORK 10.151.0.0 0.0.0.255 AREA 0
R2(config-router)#EXIT
R2(config)#EXIT
R2#WR
*Mar  1 00:08:47.243: %SYS-5-CONFIG_I: Configured from console by console
R2#WR
Building configuration...
[OK]
R2#
```

Figure 5.45: Implémentation de OSPF sur le router spoke-R2

- Sur le router spoke R3 :

```
R3
R3#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ROUTER OSPF 110
R3(config-router)#NETWORK 3.3.10.0 0.0.0.255 AREA 0
R3(config-router)#NETWORK 10.152.0.0 0.0.0.255 AREA 0
R3(config-router)#EXIT
R3(config)#EXIT
R3#W
*Mar  1 00:10:49.215: %SYS-5-CONFIG_I: Configured from console by console
R3#WR
Building configuration...
[OK]
R3#
```

Figure 5.46: Implémentation de OSPF sur le router spoke-R3

- Sur le router spoke R4 :

```
R4
R4#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ROUTER OSPF 110
R4(config-router)#NETWORK 4.4.10.0 0.0.0.255 AREA 0
R4(config-router)#NETWORK 10.153.0.0 0.0.0.255 AREA 0
R4(config-router)#EXIT
R4(config)#EXIT
R4#
*Mar  1 00:12:41.547: %SYS-5-CONFIG_I: Configured from console by console
R4#WR
Building configuration...
[OK]
R4#
```

Figure 5.47: Implémentation de OSPF sur le router spoke-R4

Analyse de la figures 5.44, 5.45, 5.46, 5.47 : [ ]

Activation et Process ID OSPF Cohérents : Sur tous les routeurs (R1, R2, R3, R4), l'activation d'OSPF se fait par la commande ROUTER OSPF 110. L'identifiant de processus 110, bien que localement significatif pour chaque routeur, est maintenu identique sur l'ensemble du réseau. Cette cohérence est une bonne pratique et indique que tous les routeurs appartiennent à la même instance logique OSPF, facilitant ainsi leur interconnexion.

Utilisation Exclusive de l'Area 0 (Backbone Area) : Toutes les commandes NETWORK sur l'ensemble des routeurs spécifient AREA 0. L'Area 0 est la zone dorsale (backbone area) d'OSPF et est un composant fondamental de toute topologie OSPF. Dans le contexte d'un DMVPN, il est courant de placer tous les routeurs (Hub et Spokes) dans l'Area 0 pour simplifier la conception du routage, surtout si la topologie ne justifie pas une segmentation en zones multiples.

Annonce du Réseau de Tunnel DMVPN Commun (10.150.0.0/24) : La commande NETWORK 10.150.0.0 0.0.0.255 AREA 0 est présente sur le Hub R1 (Figure 45) et sur tous les Spokes R2, R3, R4 (Figures 46,47 et 48). Le masque générique 0.0.0.255 indique un sous-réseau /24. Ce réseau est crucial car il représente généralement le segment IP des interfaces de tunnel GRE/mGRE des routeurs DMVPN. En incluant ce réseau dans OSPF :

- Le Hub R1 peut former des adjacences OSPF avec les Spokes via leurs tunnels.
- Les Spokes (R2, R3, R4) peuvent établir des relations de voisinage OSPF avec le Hub, apprenant ainsi les routes nécessaires pour communiquer.
- Cela jette les bases de l'établissement de tunnels spoke-to-spoke et du routage direct entre les branches.

Annonce des Réseaux Locaux/Loopbacks Uniques :

- R1 (Figure 45) : Annonce NETWORK 1.1.10.0 0.0.0.255 AREA 0. Il s'agit probablement d'une interface Loopback sur le Hub, souvent utilisée comme identifiant stable pour le routeur ou comme source pour les tunnels et le protocole NHRP.
- R2 (Figure 46) : Annonce NETWORK 2.2.10.0 0.0.0.255 AREA 0.
- R3 (Figure 47) : Annonce NETWORK 3.3.10.0 0.0.0.255 AREA 0.
- R4 (Figure 48) : Annonce NETWORK 4.4.10.0 0.0.0.255 AREA 0.

Ces réseaux (probablement des interfaces Loopback uniques à chaque Spoke ou des réseaux LAN derrière chaque site distant) sont annoncés dans OSPF. Cela permet à tous les participants du réseau DMVPN (Hub et autres Spokes) d'apprendre les routes vers les réseaux de chaque site distant, assurant ainsi une connectivité inter-sites complète.

Processus de Sauvegarde de la Configuration : Après chaque bloc de configuration, les commandes EXIT successives ramènent au mode d'exécution privilégié, où la commande WR (ou copy running-config startup-config) est utilisée pour sauvegarder la configuration active dans la mémoire non volatile (NVRAM). Ceci garantit que les modifications persisteront après un redémarrage du routeur.

5.2.9. Attribution des adresses IP à chaque poste de travail:

- Sur PC1 (LAN-ALGER) :

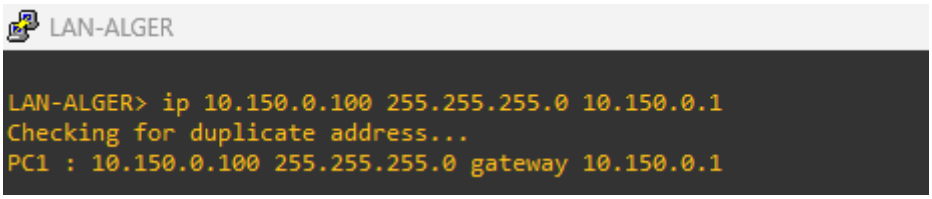

Figure 5.48: Commande de configuration IP sur PC1 (LAN-ALGER)

- Sur PC2 (LAN-HMD) :

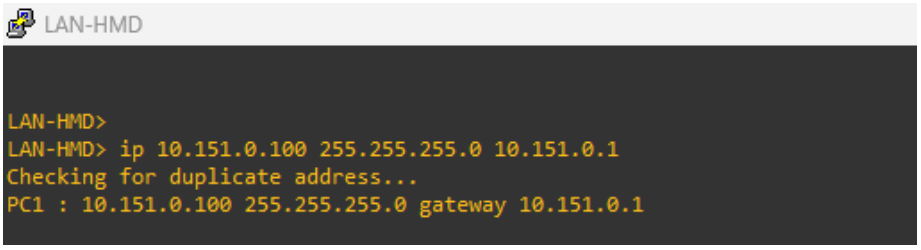

Figure 5.49: Commande de configuration IP sur PC2 (LAN-HMD)

- Sur PC3 (LAN-HRM) :

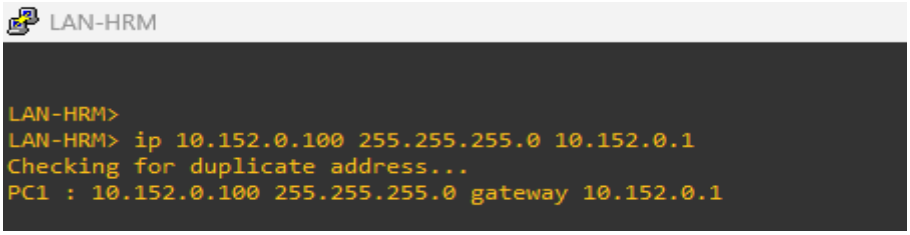

Figure 5.50: Commande de configuration IP sur PC3 (LAN-HRM)

- Sur PC4 (LAN-SKIKDA) :

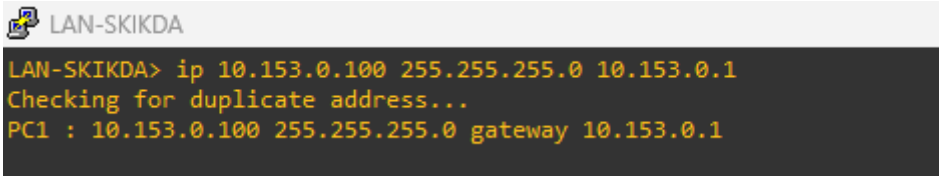

Figure 5.51: Commande de configuration IP sur PC3 (LAN-SKIKDA)

Analyse de la figures 5.47, 5.48, 5.49, 5.51 : [ ]

Les figures 63 à 66 présentent les configurations d'adresses IP statiques pour quatre ordinateurs (PC1 à PC4), chacun appartenant à un réseau local (LAN) distinct. Ces configurations suivent un schéma cohérent :

- Adresses IP des PC : Les PC sont configurés avec des adresses IP se terminant par .100 (ex: 10.150.0.100 pour PC1, 10.151.0.100 pour PC2, etc.).
- Masque de sous-réseau : Tous les LANs utilisent un masque de sous-réseau 255.255.255.0 (sous-réseau de classe C), indiquant 254 hôtes utilisables par segment.
- Passerelle par défaut : La passerelle par défaut pour chaque LAN est toujours l'adresse .1 du même sous-réseau (ex: 10.150.0.1 pour PC1, 10.151.0.1 pour PC2, etc.).
- Segmentation réseau : Chaque LAN (ALGER, HMD, HRMD, SKIKDA) est différencié par le troisième octet de l'adresse IP (150, 151, 152, 153), suggérant une segmentation logique du réseau pour des sites ou départements distincts.
- Vérification des doublons : La mention "checking for duplicate address" indique une pratique standard pour éviter les conflits d'adresses IP.

5.2.10. Test ping de la connectivité avant la configuration des listes d'accés :

- Sur PC1 (LAN-ALGER) :

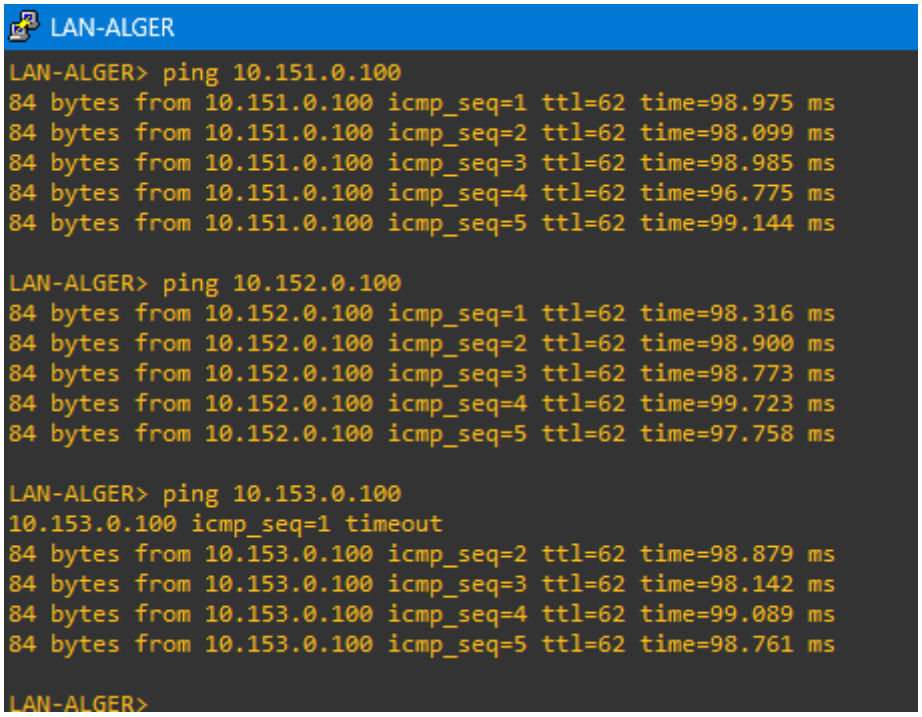

Figure 5.52: Résultats des tests de connectivité ping depuis LAN-ALGER

Analyse de la figure 5.52 :

Test de connectivité vers 10.151.0.100 :

- Cinq paquets (icmp_seq de 1 à 5) ont été envoyés.
- Tous les paquets ont reçu des réponses réussies (84 octets), avec une valeur TTL (Time To Live) de 62.
- Les temps de réponse étaient stables, variant entre 98.975 ms et 99.144 ms.

Résultat : Connectivité réussie et stable vers la destination 10.151.0.100.

Test de connectivité vers 10.152.0.100 :

- Cinq paquets (icmp_seq de 1 à 5) ont été envoyés.
- Tous les paquets ont reçu des réponses réussies (84 octets), avec une valeur TTL de 62.
- Les temps de réponse étaient stables, variant entre 97.758 ms et 98.900 ms.

Résultat : Connectivité réussie et stable vers la destination 10.152.0.100.

Test de connectivité vers 10.153.0.100 :

- Cinq paquets (icmp_seq de 1 à 5) ont été envoyés.
- Le premier paquet (icmp_seq=1) a subi un "timeout" (délai d'attente dépassé), signifiant qu'aucune réponse n'a été reçue dans le temps imparti.
- Les quatre paquets suivants (icmp_seq=2 à icmp_seq=5) ont reçu des réponses réussies (84 octets), avec une valeur TTL de 62.
- Les temps de réponse pour les paquets réussis variaient entre 98.089 ms et 98.879 ms.

Résultat : Il y a une connectivité vers la destination 10.153.0.100, mais le premier paquet a subi un timeout. Cela pourrait être dû à une résolution ARP (Address Resolution Protocol) initiale, à un réveil de l'appareil après une période d'inactivité, ou à un problème réseau transitoire, mais la connectivité s'est stabilisée par la suite.

5.2.11. Configuration de l’access-list sur R1 :

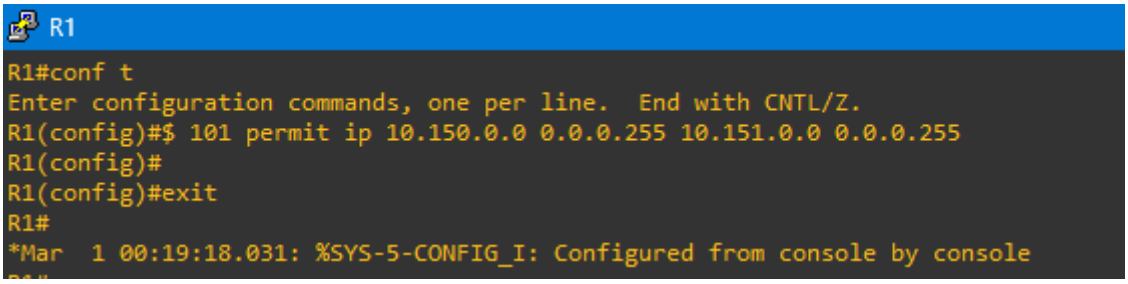

Figure 5.53: Configuration de la règle « permit » pour l’access-list 101 sur R1

Analyse de la figure 5.53 :

R1 (config)#$ 101 permit ip 10.150.0.0 0.0.0.255 10.151.0.0 0.0.0.255 :

Description: C'est la commande principale de configuration de l'ACL Décortiquons-la :

- access-list (implicite avant le 101): Indique que la commande concerne une liste de contrôle d'accès. Le fait que le nombre 101 soit utilisé immédiatement après le prompt R1 (config)#$ suggère une erreur de frappe ou une abréviation, et la commande correcte devrait commencer par access-list. Cependant, le routeur Cisco est souvent tolérant aux abréviations si elles sont non ambiguës.
- 101: Ce nombre indique qu'il s'agit d'une ACL étendue (les ACLs étendues utilisent les nombres de 100 à 199 et de 2000 à 2699). Les ACLs étendues sont plus granulaires que les ACLs standard, car elles peuvent filtrer sur la source, la destination, le protocole et les ports.
- Permit : Cette action signifie que le trafic correspondant à cette règle sera autorisé à passer.
- ip: Indique que cette règle s'applique à tous les types de trafic IP (TCP, UDP, ICMP, etc.).
- 10.150.0.0: C'est l'adresse réseau source que cette règle est censée faire correspondr
- 0.0.0.255: C'est le masque générique (wildcard mask) associé à l'adresse source. Un wildcard mask fonctionne à l'opposé d'un masque de sous-réseau. Un 0 dans le wildcard mask signifie que le bit correspondant dans l'adresse IP doit correspondre exactement. Un 255 signifie que le bit correspondant peut être n'importe quelle valeur.
    - Ici, 0.0.0.255 appliqué à 10.150.0.0 signifie que cette règle correspondra à toutes les adresses IP allant de 10.150.0.0 à 10.150.0.255. En d'autres termes, elle correspond au sous-réseau 10.150.0.0/24.
- 10.151.0.0: C'est l'adresse réseau de destination que cette règle est censée faire correspondre
- 0.0.0.255: C'est le masque générique (wildcard mask) associé à l'adresse de destination. Similairement au masque source, cela signifie que la règle correspondra à toutes les adresses IP allant de 10.151.0.0 à 10.151.0.255, c'est-à-dire le sous-réseau 10.151.0.0/24.

En résumé :

Cette règle permit autorise le trafic IP dont la source est dans le sous-réseau 10.150.0.0/24 ET dont la destination est dans le sous-réseau 10.151.0.0/24.

5.2.12. Test ping de la connectivité après la configuration des listes d'accés :

- Sur PC1 (LAN-ALGER) :

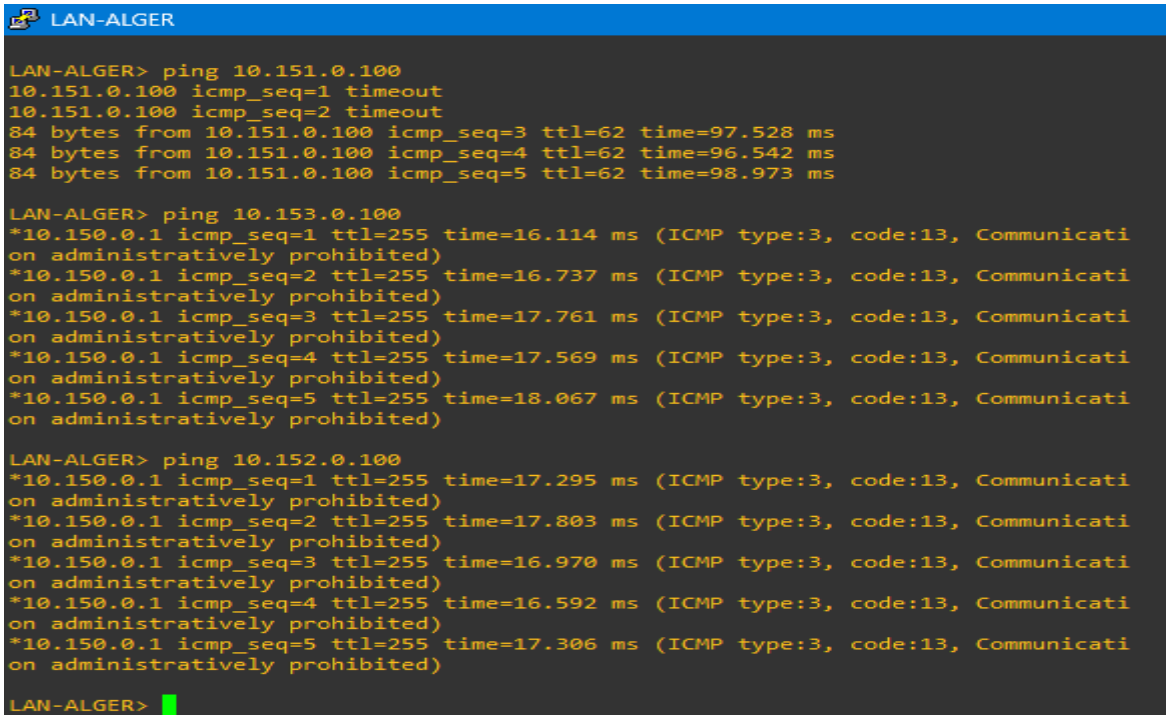

Figure 5.54: Test de connectivité ping vers différentes adresses IP du LAN-ALGER

Analyse de la figure 5.54 :

Premier ping vers 10.151.0.100 :

- Les deux premières requêtes icmp_seq=0 et icmp_seq=1 affichent un "timeout". Cela signifie que l'hôte distant (10.151.0.100) n'a pas répondu dans le délai imparti. Cela pourrait indiquer que l'hôte était initialement indisponible, en cours de démarrage, ou qu'il y avait une latence temporaire du réseau ou un problème de résolution ARP initial.
- Les requêtes suivantes (icmp_seq=2, icmp_seq=3, icmp_seq=4, icmp_seq=5) réussissent. Elles montrent des temps de réponse autour de 96-98 ms et un TTL (Time To Live) de 62. Le TTL de 62 suggère que les paquets ont traversé un certain nombre de sauts (routeurs) pour atteindre la destination, mais qu'ils sont arrivés à bon port. La connectivité avec 10.151.0.100 est donc établie après un démarrage difficile ou une interruption temporaire.

Deuxième ping vers 10.153.0.100 :

- Toutes les requêtes de ping (icmp_seq=0 à icmp_seq=5) vers cette adresse IP échouent avec le message d'erreur "ICMP type:3, code:13, Communication administratively prohibited".
- Explication de l'erreur :

    - ICMP type 3 (Destination Unreachable) : Indique que la destination ne peut pas être atteinte.
    - Code 13 (Communication administratively prohibited) : Ce code est très spécifique et signifie que la communication a été délibérément bloquée par un mécanisme de sécurité sur le réseau, tel qu'un pare-feu, une liste de contrôle d'accès (ACL) configurée sur un routeur, ou une politique de sécurité empêchant ce type de trafic (ICMP dans ce cas) entre l'émetteur (LAN-ALGER) et la destination (10.153.0.100).
- Cela suggère fortement que l'hôte 10.153.0.100 est probablement en ligne et joignable au niveau IP, mais qu'une règle de sécurité activement configurée sur le chemin réseau ou sur l'hôte lui-même bloque les requêtes ping.

Troisième ping vers 10.152.0.100 :

- Similairement au deuxième ping, toutes les requêtes (icmp_seq=0 à icmp_seq=5) vers cette adresse échouent également avec le même message d'erreur : "ICMP type:3, code:13, Communication administratively prohibited".
- La même explication s'applique ici : la communication ICMP vers 10.152.0.100 est activement bloquée par une politique de sécurité (pare-feu, ACL, etc.) sur le réseau ou sur l'hôte cible.

5. 3. Résultat et vérification :

5.3.1. Vérification l'état des interfaces :

- Vérification l'état des interfaces de router Hub (R1) :

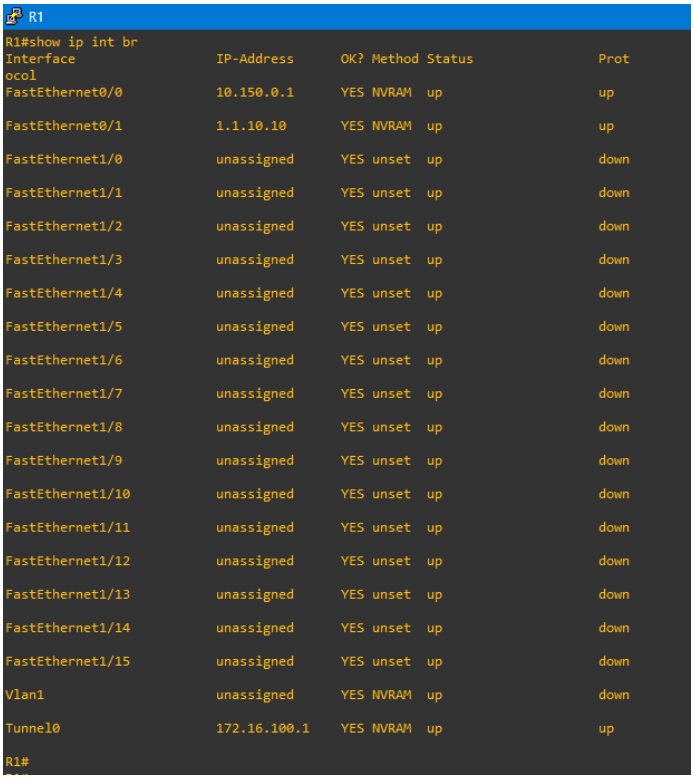

Figure 5.55: Exécution de la command show IP interface brief au niveau de HUB-R1

Analyse de la figure 5.55 :

Dans la partie de configuration du réseau, trois interfaces ont été mises en place :

- FastEthernet0/0 avec l'adresse IP 10.150.0.1 et un statut "up".
- FastEthernet0/1 avec l'adresse IP 1.1.10.10 et un statut "up".
- Tunnel0 avec l'adresse IP 172.16.100.1 et un statut "up".

Les autres interfaces FastEthernet (de 0/2 à 0/15) et VLAN1 sont "unassigned" et leur statut est "down".

- Vérification l'état des interfaces de router Spoke (R2) :

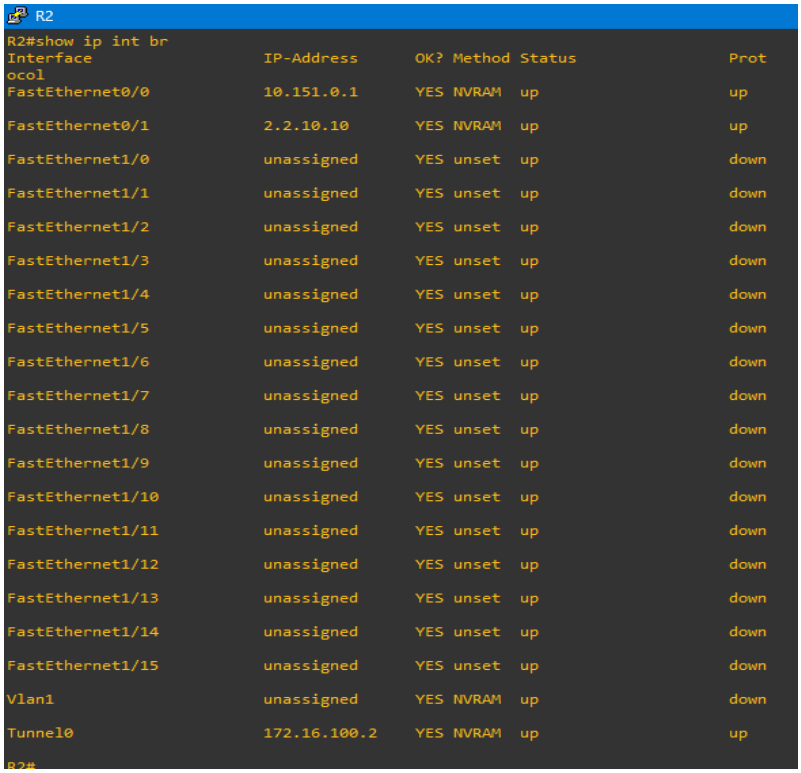

Figure 5.56: Exécution de la command show IP interface brief au niveau de SPOKE-R2

Analyse de la figure 5.56 :

Dans la partie de configuration du réseau, trois interfaces ont été mises en place :

- FastEthernet0/0 avec l'adresse IP 10.151.0.1 et un statut "up".
- FastEthernet0/1 avec l'adresse IP 2.2.10.10 et un statut "up".
- Tunnel0 avec l'adresse IP 172.16.100.1 et un statut "up".

Les interfaces FastEthernet1/0 à FastEthernet1/15 et Vlan1 sont "unassigned" et leur statut est "down".

5.3.2. Vérification de la configuration active du périphérique (commande « show run ») :

- Sur le router R1 (HUB) :

```
R1
R1#show run
Building configuration...
```

Figure 5.57: Exécution de la command show run sur R1 (HUB)

a) Tunnel :

```
R1
interface Tunnel0
 description mGRE - DMVPN Tunnel
 ip address 172.16.100.1 255.255.255.0
 no ip redirects
 ip nhrp authentication firewall
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source 1.1.10.10
 tunnel mode gre multipoint
 tunnel protection ipsec profile protect-gre
!
```

Figure 5.58: Extrait de la configuration de l'interface tunnel (DMVPN mGRE) sur R1 (Hub)

b) Les interfaces :

```
R1
interface FastEthernet0/1
 description WAN-Network
 ip address 1.1.10.10 255.255.255.0
 duplex auto
 speed auto
!
```

```
R1
interface FastEthernet0/0
 description LAN-Network
 ip address 10.150.0.1 255.255.255.0
 duplex auto
 speed auto
!
```

Figure 5.59: Exécution de la configuration des interfaces FastEthernet sur R1 (Hub)

c) OSPF :

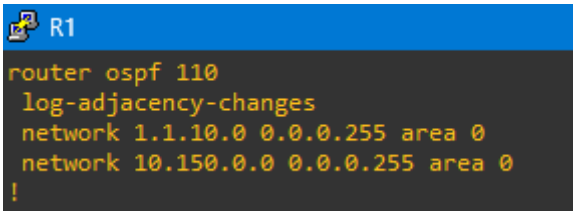

Figure 5.60: Exécution de la configuration du protocole OSPF sur R1 (Hub)

d) Access-list :

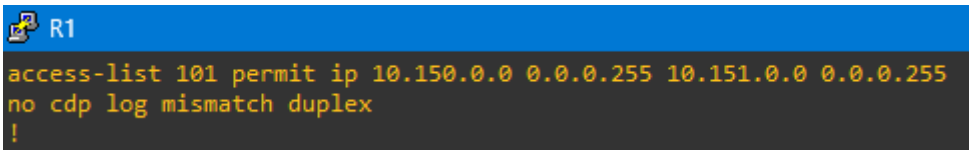

Figure 5.61: Exécution de la configuration de Access-list 101 sur le routeur R1 (Hub)

- Sur le router R2 (SPOKE) :

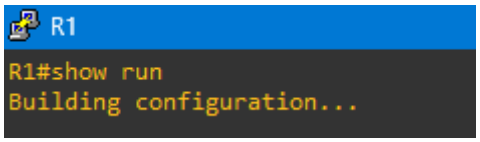

Figure 5.62: Exécution de la command show run sur R2 (Spoke)

a) Tunnel :

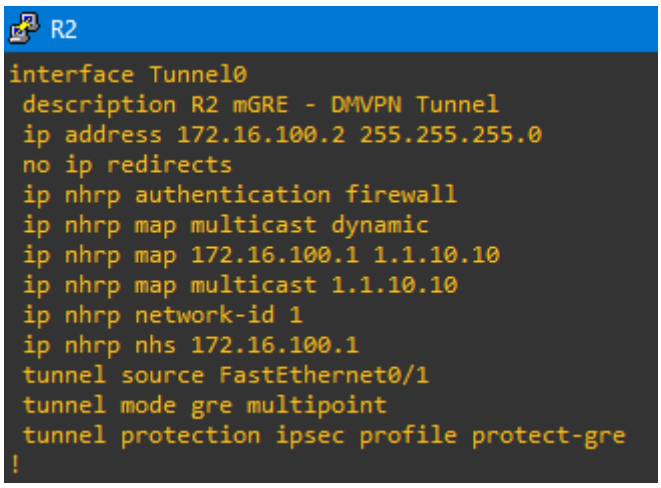

Figure 5.63: Extrait de la configuration de l'interface tunnel (DMVPN mGRE) sur R2 (Spoke)

b) Les interfaces :

R2

```
interface FastEthernet0/0
 description LAN-Network
 ip address 10.151.0.1 255.255.255.0
 duplex auto
 speed auto
!
```

R2

```
interface FastEthernet0/1
 description WAN-Network
 ip address 2.2.10.10 255.255.255.0
 duplex auto
 speed auto
!
```

Figure 5.64: Exécution de la configuration des interfaces FastEthernet sur R2 (Spoke)

c) OSPF :

R2

```
router ospf 110
 log-adjacency-changes
 network 2.2.10.0 0.0.0.255 area 0
 network 10.151.0.0 0.0.0.255 area 0
!
```

Figure 5.65: Exécution de la configuration du protocole OSPF sur R2 (Spoke)

5.3.3. Affichage des entrées NHRP pour les réseaux distants accessibles via les tunnels DMVPN (commande "show ip nhrp") :

- Exécution de commande au niveau de HUB :

R1

```
R1#SHOW IP NHRP
172.16.100.2/32 via 172.16.100.2, Tunnel0 created 00:25:02, expire 01:34:57
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 2.2.10.10
172.16.100.3/32 via 172.16.100.3, Tunnel0 created 00:25:14, expire 01:34:45
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 3.3.10.10
172.16.100.4/32 via 172.16.100.4, Tunnel0 created 00:00:59, expire 01:59:00
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 4.4.10.10
R1#
```

Figure 5.66: Affichage de la table NHRP sur le routeur Hub (R1)

Analyse de la figure 5.66 :

Dans ce résultat, les adresses IP distantes suivantes ont été résolues avec succès par le Hub (R1) via le Tunnel0 :

- L'adresse 172.16.100.2/32 est résolue via l'adresse Next Hop 172.16.100.2 et correspond à l'adresse NBMA 2.2.10.10. L'entrée est de type dynamique et enregistrée.
- L'adresse 172.16.100.3/32 est résolue via l'adresse Next Hop 172.16.100.3 et correspond à l'adresse NBMA 3.3.10.10. L'entrée est de type dynamique et enregistrée.
- L'adresse 172.16.100.4/32 est résolue via l'adresse Next Hop 172.16.100.4 et correspond à l'adresse NBMA 4.4.10.10. L'entrée est de type dynamique et enregistrée.

- Exécution de commande au niveau de SPOKE :

R2

```
R2#show IP NHRP
172.16.100.1/32 via 172.16.100.1, Tunnel0 created 00:30:17, never expire
  Type: static, Flags: authoritative used
  NBMA address: 1.1.10.10
R2#
```

Figure 5.67: Affichage de la table NHRP sur le routeur Spoke (R2)

Analyse de la figure 5.67 :

Dans ce résultat, l'adresse IP distante 172.16.100.1/32 a été résolue avec succès par le Spoke (R2) via le Tunnel0. Cette adresse correspond à l'adresse IP du Hub. L'entrée est de type statique, car le Spoke est configuré pour connaître l'adresse de son Hub de manière explicite. L'adresse NBMA associée au Hub est 1.1.10.10. L'entrée est marquée comme "authoritative used", ce qui signifie qu'elle est utilisée comme source d'information fiable pour le routage.

5.3.4. Affichage des entrées NHRP pour les réseaux distants accessibles via les tunnels DMVPN (commande "show crypto isakmp sa detail ") :

- Exécution de commande au niveau de HUB :

```
R1
R1#SHOW CRYPTO ISAKMP SA DETAIL
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.
5     1.1.10.10       4.4.10.10                ACTIVE 3des md5  psk  2  23:21:40
       Connection-id:Engine-id =  5:1(software)
6     1.1.10.10       2.2.10.10                ACTIVE 3des md5  psk  2  23:21:50
       Connection-id:Engine-id =  6:1(software)
4     1.1.10.10       3.3.10.10                ACTIVE 3des md5  psk  2  23:21:39
       Connection-id:Engine-id =  4:1(software)
R1#
```

Figure 5.68: Affichage de la table ISAKMP SA sur le routeur HUB (R1)

Analyse de la figure 5.68:

- Trois connexions actives : Le routeur R1 a réussi à établir trois connexions sécurisées avec d'autres routeurs distants.
- Connexions réussies : Le mot "ACTIVE" pour chaque connexion signifie que la Phase 1 de la sécurité est bien établie avec chaque partenaire. C'est essentiel pour la suite.
- Partenaires distants : Les adresses 4.4.10.10, 2.2.10.10 et 3.3.10.10 sont les "autres bouts" des tunnels, probablement des routeurs "spokes" dans un réseau DMVPN.

En résumé :

Cette figure prouve que le routeur HUB (R1) communique correctement et de manière sécurisée avec au moins trois autres routeurs. C'est une étape indispensable pour que les tunnels VPN fonctionnent et que les données puissent voyager en toute sécurité. Si ces connexions n'étaient pas "actives", le VPN ne fonctionnerait pas.

- Exécution de commande au niveau de SPOKE :

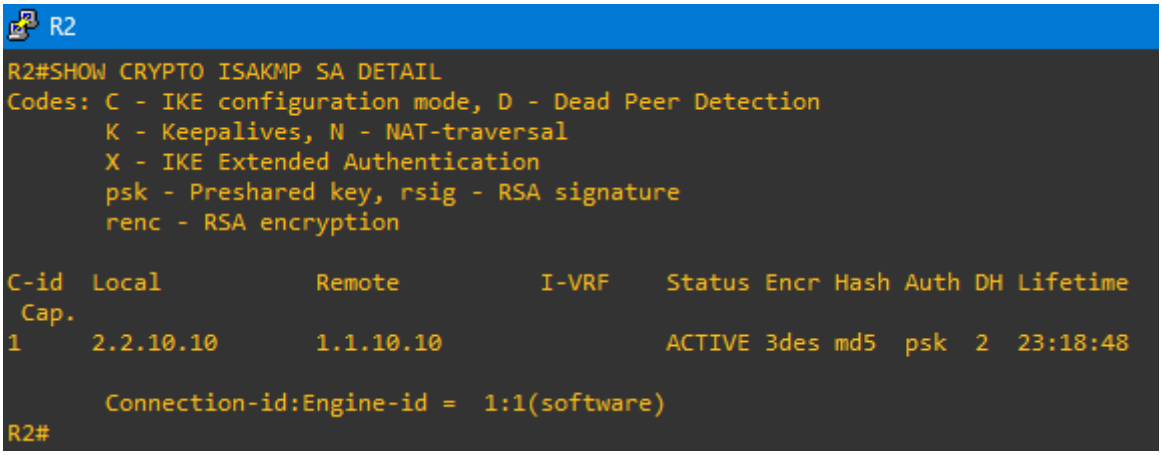

Figure 5.69: Affichage de la table ISAKMP SA sur le routeur SPOKE (R2)

Analyse de la figure 5.69:

Une connexion active : Le routeur R2 a réussi à établir une connexion sécurisée avec un autre routeur distant.

Connexion réussie : Le mot "ACTIVE" signifie que la Phase 1 de la sécurité est bien établie avec le partenaire. C'est essentiel pour la suite.

Partenaires :

- L'adresse locale du routeur R2 est 2.2.10.10.
- L'adresse distante à laquelle il se connecte est 1.1.10.10. Cette adresse est très probablement celle du routeur central (HUB) que nous avons vu dans l'analyse précédente (R1).

En résumé :

Cette figure confirme que le routeur SPOKE (R2) communique correctement et de manière sécurisée avec le routeur central (HUB). C'est une étape fondamentale et indispensable pour que les tunnels VPN fonctionnent et que les données puissent voyager en toute sécurité. Sans cette connexion "active", le VPN ne fonctionnerait pas.

5.3.5. Test de Traçage de Route (Trace-route) pour la vérification de la connectivité :

Dans cette phase de l'implémentation, nous avons effectué des tests de traçage de route (trace-route) depuis la station de travail (LAN-HMD) vers une adresse IP spécifique 10.153.0.100, après avoir supprimé l'access-list afin de vérifier la connectivité et d'identifier le chemin emprunté par les paquets de données à travers le réseau.

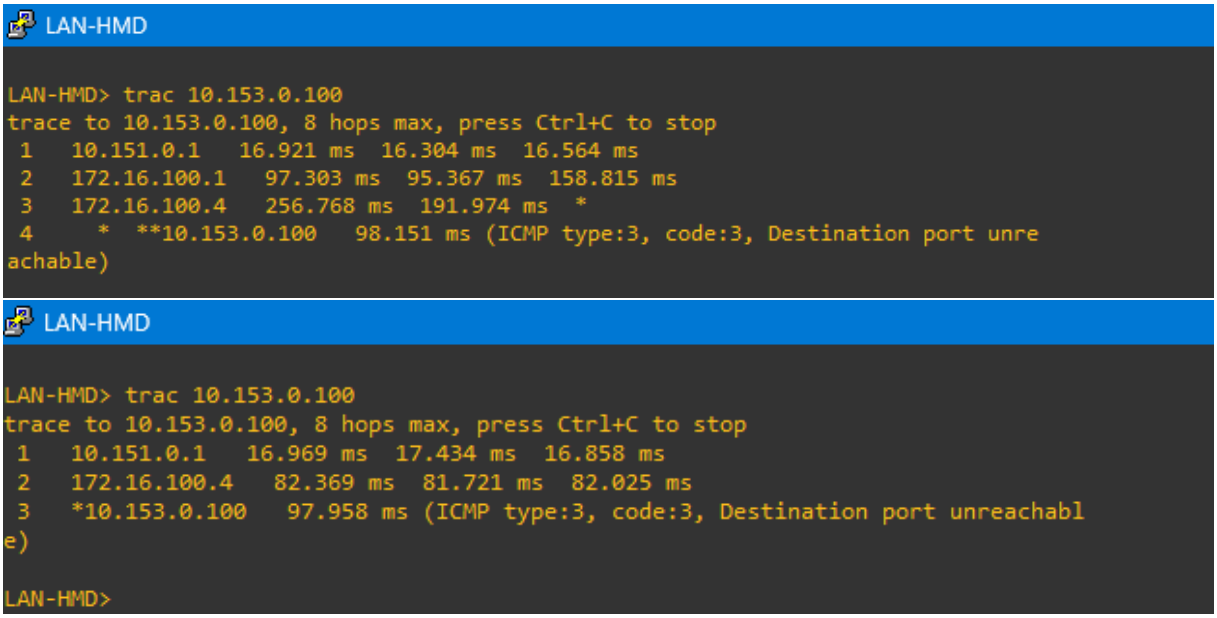

Figure 5.70: Résultats de traçage de route depuis le LAN-HMD vers 10.153.0.100

Analyse de la figure 5.70 :

- Saut 1 (10.151.0.1): Il s'agit du premier routeur ou de la passerelle par défaut du réseau local du site Spoke. Les temps de réponse sont faibles (environ 16-17 ms), ce qui est typique pour un saut au sein d'un même segment de réseau local.
- Saut 2 (172.16.100.1): Ce saut indique le passage par un équipement intermédiaire, probablement un routeur central ou un point d'entrée/sortie du VPN. On observe une augmentation significative des temps de réponse (entre 82 ms et 160 ms), suggérant l'établissement d'une connexion sur un réseau plus étendu ou le traitement supplémentaire lié au tunnel VPN.
- Saut 3 (172.16.100.4): Un autre saut intermédiaire dans le même réseau privé. Les temps de réponse sont similaires ou légèrement inférieurs à ceux du saut précédent dans la deuxième tentative (environ 97 ms), mais la première tentative montre une variabilité plus importante, incluant un * (timeout) pour l'une des requêtes, ce qui pourrait indiquer une légère fluctuation passagère du réseau ou une surcharge ponctuelle de ce routeur.
- Saut 4 (10.153.0.100): La destination finale est atteinte. Le temps de réponse est d'environ 98 ms. La mention (ICMP type:3, code:3, Destination port unreachable) indique que, bien que la machine cible 10.153.0.100 soit joignable au niveau IP (les

paquets y sont parvenus), un service spécifique ou un port n'est pas disponible ou est bloqué. Cette erreur est courante et signifie généralement qu'un pare-feu sur la machine cible empêche l'accès au port ICMP utilisé par tracert, ou qu'aucune application n'écoute sur ce port. L'essentiel est que le paquet a bien atteint la machine cible, confirmant la connectivité réseau sous-jacente entre le Spoke et cette destination.

But de la commande trace-route :

La commande tracert (ou traceroute sur les systèmes d'exploitation de type Unix) est un outil de diagnostic réseau utilisé pour tracer le chemin qu'empruntent les paquets IP depuis un point source jusqu'à une destination. La commande fonctionne en envoyant des paquets avec des valeurs de temps de vie (Time-To-Live - TTL) incrémentales et en recevant des messages ICMP "Time Exceeded" de chaque routeur le long du chemin. Cela permet d'identifier chaque "saut" (hop) ou routeur traversé par le trafic, ainsi que de mesurer le temps aller-retour (Round Trip Time - RTT) pour chaque saut.

A travers cet outil, nous avons pu observer concrètement le fonctionnement de DMVP

Conclusion générale

Ce mémoire a exploré en profondeur les VPN IPsec multipoint dynamiques, en mettant l'accent sur l'intégration des protocoles GRE multipoint et NHRP pour étendre et optimiser les connexions VPN IPsec. Nous avons démontré comment cette architecture permet d'établir des communications sécurisées et flexibles entre de multiples sites, surpassant les limites des configurations VPN point-à-point traditionnelles.

Le projet sur lequel j'ai travaillé au sein de l'entreprise SONATRACH a clairement mis en évidence la pertinence et l'efficacité de cette solution dans un environnement institutionnel complexe. L'implémentation de cette technologie a permis à SONATRACH d'améliorer significativement la connectivité de ses sites distants, de renforcer la sécurité de ses échanges de données et d'optimiser l'utilisation de ses ressources réseau. Les résultats obtenus ont confirmé les avantages inhérents à l'utilisation de GRE multipoint et NHRP pour automatiser l'établissement des tunnels VPN IPsec et simplifier la gestion d'un réseau étendu.

Cependant, il est essentiel de reconnaître que, malgré la robustesse de cette approche, elle fait face à des défis, notamment en ce qui concerne l'équilibrage de charge dynamique et le basculement instantané en cas de défaillance. Ce sont des aspects où les technologies plus récentes comme le SD-WAN apportent des améliorations significatives.

En conclusion, ce projet n'a pas seulement approfondi notre compréhension des VPN IPsec multipoint dynamiques, mais il a également souligné leur valeur opérationnelle pour des entreprises de la taille de SONATRACH. Il ouvre la voie à de futures recherches sur l'intégration de ces architectures avec des solutions plus agiles et intelligentes afin de répondre aux besoins évolutifs des réseaux d'entreprise modernes.

Références :

[1] Delamontagne, M. (2024, 17 janvier). Quiz - Nombre de machine dans un réseau informatique. Dans LE GRAND ORAL: Exemples rédigés NSI Numérique et sciences Informatiques. http://www.science-du-numerique.fr/quiz-nombre-de-machine-dans-un-reseau-informatique-2

[2] 2Y.Technologie. (2022, 1 octobre). le modèle osi présentation simple animé [Vidéo]. YouTube. http://www.youtube.com/watch?v=j7D1sMEGANO

[3] IT Dose. (2023, 4 mai). IP Address و Subnet Mask والفرق بين Public IP Private IP شرح مفصل Video YouTube. https://www.youtube.com

[4] Farrier, E. (2021, 22 avril). Public vs. Private IP Addresses: What's the Difference? Avast Academy. https://www.youtube.com/watch?v=Nnv36wG_iCI&t=361s&ab_channel=ITDose

[5] informatique-tuto. (2022, 5 février). Types de réseaux et topologies (Bus, étoile, anneau) [Vidéo]. YouTube. https://www.youtube.com/watch?v=_88pXPp2CaU&t=42s&ab_channel=informatique-tuto

[6] MVogal. (s.d.). Une image de tableau de topologie de bus de réseau [Image]. Dreamstime. Consulté le 16 mai 2025. https://fr.dreamstime.com/photos-libres-droits-tableau-topologie-bus-image29007878

[7] Ecole La Marche. (s.d.). II. Réseaux informatiques: 7. Topologie des réseaux. Bac STI 2D. 16 mai 2025. https://sti2d.ecolelamache.org/ii_rseaux_informatiques___7_topologie_des_rseaux.html

[8] Black Box. (s.d.). Réseau d'entreprise - Topologie en anneau. Black Box. 16 mai 2025.https://www.blackbox.fr/fr-fr/page/41455/Information/Technique/black-box-explique/Networking/Topologie-circulaire-pour-le-reseau

[9] Mr Mehdi, Faculté de Technologie, Université Saad Dahleb Blida 1. (2017/2018). Routage IP.

[10] Tran, M. (s.d.). TCP/IP - Le routage dynamique [Présentation]. SlidePlayer.17 mai 2025. https://slideplayer.fr/slide/470095/

[11] aeres-evaluation. (2020, 26 février). VPN: définition + tout ce qu'il faut savoir au sujet de ce service. Consulté le 11 juin 2025. https://www.aeres-evaluation.fr/vpn-definition/

[12] AMIAR, D. 2013/2014. Mise en place d'un VPN dans un réseau d'entreprise, Mémoire de Master académique, Université Mouloud Tizi Ouzou, Faculté de Génie Électrique, Département Informatique.

[13] Boisson, T. (2021, 3 mars). Les VPN: une technologie aux multiples avantages. Trust My Science. https://trustmyscience.com/vpn-technologie-multiples-avantages/

[14] Mawusse, M. A. (2018/2019). Configuration DMVPN, IPsec et NAT sur les routeurs Internet BGP [Document]. ESGIG L'école des leaders. https://fr.scribd.com/document/437907726/Dmvpn

[15] Cisco Community. (s.d.). Conociendo Dynamic Multipoint VPN (DMVPN). Cisco Community Blogs Routing y Switching. 18 mai 2025. https://community.cisco.com/t5/blogs-routing-y-switching/conociendo-dynamic-multipoint-vpn-dmvpn/ba-p/3101118

[16] oumar.ndiath. (s.d.). VPN IPSec multipoint dynamiques (utilisation de GRE multipoint/NHRP pour étendre les VPN IPsec) [Document Scribd]. Scribd. 20 mai 2015. https://fr.scribd.com/document/446784884/41940-dmvpn

[17] Goffinet, F. (s.d.). Installer et configurer GNS3. ciscogoffinet.org. 4 juin 2015. https://cisco.goffinet.org/ccna/cisco-ios-cli/installer-et-configurer-gns3/