REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Blida 1	*Sonatrach*
Faculté des Sciences	*Direction générale*
Département d'Informatique	*Département ISI*

Mémoire pour l'obtention du diplome de Master

Spécialité : Systèmes Informatiques et Réseaux

Thème

Mise en place du réseau Wan de la Sonatrach sur une plateforme virtuelle

---

Réalisé par:

Mouhous Khadidja et Nemri Lynda

Soutenu le 28/09/2022 devant le jury composé de:

Président	*Ould Khaoua Med*	*Université de Blida 1*
Examinatrice	*Bey Fella*	*Université de Blida 1*
Encadreur	*Benyahia Med*	*Université de Blida 1*
Encadreur externe	*Bacha Ibtissem*	*Entreprise Sonatrach DG*

Promotion 2021 / 2022

Remerciements

Nous adressons nos sincères remerciements à Dieu tout puissant, nos parents qui nous ont toujours soutenus dans nos objectifs par leurs encouragements, ainsi que toutes les personnes ayant contribué au succès de notre parcours universitaire en Master, de notre stage, et qui nous ont aidées à mener à bien ce projet.

Nous voudrions dans un premier temps remercier notre promotrice Mme. Bacha Ibtissam, ainsi que Mr Kacem Islam, pour leur patience, leur disponibilité et surtout leurs précieux conseils, de nous avoir encadrées, orientées, et aidées dans cette expérience unique. Et en particulier les cadres de l'organisme de la Sonatrach, Messieurs Kadri Tarik et Irathen Othmane et toute l'équipe de la direction ISI pour nous avoir donné cette occasion extraordinaire de réaliser notre travail sur le terrain.

On remercie également toute l'équipe pédagogique de l'université de Saad Dahlab Blida 1 du département Informatique, les intervenants professionnels et responsables de notre formation, pour avoir assuré la partie théorique de ce travail en particulier Monsieur Benyahia Mohamed d'avoir accepté de diriger cette étude.

Nous désirons aussi adresser notre reconnaissance, à nos amis, famille, collègues d'études, et toute autre tierce personne ayant participé physiquement ou mentalement par leur soutien pour notre réussite.

Dédicaces

Á mes très chers parents,
ma fierté et la source de ma réussite car ils se sont sacrifiés pour me fournir une atmosphère de travail disposant de toutes les meilleures conditions,
sans eux rien n'aurait pu être facile, que dieu me les garde et les protège.
Á mes très chères grand-mères que dieu me les garde en bonne santé.
À mon grand frère Atmane et ma chère sœur Abir.

khadidja

ملخص

أصبح التطور في المجال الحالي على الشبكات ، والتقدم التكنولوجي وتطبيقه، بالإضافة إلى التقييم والتحسين أمرًا صعبًا للغاية. غالبا لظهور مشاكل التعقيد واستهلاك الوقت والمال والجهد. كحل لذلك ، أجريت عمليات محاكاة للشبكة في الميدان ، ومن ثم تم تطوير العديد من أجهزة المحاكاة لأنظمة المراقبة ومنع الأخطاء. الهدف من مشروعنا هو إعادة إنتاج شبكة Sonatrach على منصة افتراضية ، باستخدام محاكيات الشبكة ، بما في ذلك ENSP للمعدات التي تحمل علامة Huwaei و GNS3 للمعدات التي تحمل علامة Cisco مع ترابطها بين الشمال والجنوب \ الشرق والغرب. بالإضافة إلى توحيد التكوينات الحالية لضمان التحسين من حيث موازنة التحميل والتكرار الكامل وتطبيق جودة الخدمة مع توافق أفضل مع بروتوكولات التوجيه MPLS/BGP.

Abstract

The evolution in the current field on networks, the advancement and application of technologies, as well as the evaluation and improvement have become quite difficult. Problems of complexity, consumption of time, money and effort, but also physical limitations. As a solution to this, network simulations took place in the field, hence the development of various simulators of monitoring and bug prevention systems.
The aim of our project is to reproduce the Sonatrach network on a virtual platform, using network simulators, in particular ENSP for Huawei brand equipment, and GNS3 for Cisco brand equipment, in order to simulate the architecture. Hybrid P/PE/CE, with its North-South/East-West interconnections. As well as the standardization of existing configurations in order to ensure optimization in terms of load balancing, full redundancy, and application of QoS and better compliance of MPLS/BGP routing protocols.

Keywords: Bgp,Mpls,Vrf,GNS3,Ensp

Résumé

L'évolution dans le domaine actuel sur les réseaux, l'avancement et l'application des technologies, ainsi que l'évaluation et l'amélioration sont devenus assez difficiles. Des problèmes de complexité, de consommation de temps, d'argent et d'efforts, mais aussi des limitations physiques. En guise de solution à cela, des simulations de réseau ont eu lieu sur le terrain, d'où l'élaboration de différents simulateurs de systèmes de surveillance et de prévention de bugs.
Le but de notre projet est de reproduire le réseau de la Sonatrach sur une plateforme virtuelle, à l'aide de simulateurs réseau, notamment ENSP pour les équipements de marque Huawei, et GNS3 pour les équipements de marque Cisco, afin de simuler l'architecture Hybride P/PE/CE, avec ses interconnexions Nord-Sud/ Est-West. Ainsi que la normalisation des configurations existantes dans le but d'assurer une optimisation en termes d'équilibrage de charge, d'une redondance totale, et d'une application des QoS et une meilleure conformité des protocoles de routage MPLS/BGP.

Mots clés : Bgp,Mpls,Vrf,GNS3,Ensp

Table des matieres

Table des figures

Liste des abréviations

AS Autonomous System

ATM Asynchronous Transfer Mode

BGP Border Gateway Protocol

CE Customer Edge

CPU Central Processing Unit

DCI Data Centers Interconnection

DNS Domain Name System

EIGRP Enhanced Interior Gateway Routing Protocol

eNSP Enterprise Network Simulation Platform

FAI Fournisseur d'Accés Internet

FDDI Fiber Distributed Data Interface

FTP File Transfer Protocol

GNS3 Graphical Network Simulator

Gbps Gigabits per second

GE Gigabit Ethernet

HDMI High-Definition Multimedia Interface

HTTP Hypertext Transfer Protocol

IBGP Interior Border Gateway Protocol

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

IoT Internet of Things

IP Internet Protocol

IPV4 Internet Protocol Version4

IPV6 Internet Protocol Version6

IPsec Internet Protocol Security

IOS Image Operating System

ISO International Standard Organization

LAN Local Area Network

LDP Label Distribution Protocol

LER Label Edge Router

LFIB Label Forwarding Information Base

LSDB Link State Data Base

LSP Label switched path

LSR Label Switch Router

LTE Long Term Evolution

Mbps Megabytes per second

MP BGP Multiprotocol BGP

MPLS Multiprotocol Label Switching

MPPS Mega Packet Per Second

MTU Maximum Transmission Unit

NAT Network Address Translation

OSI Open System Interconnection

OSPF Open Shortest Path First

P Provider

PE Provider Edge

PDU Protocol Data Unit

PPS Packet Per Second

RAM Random Access Memory

RD Route Distinguisher

RFC Request For Comments

RIP Routing Information Protocol

RT Route Target

SDN Software Defined Network

SD-WAN Software-Defined Wide-Area Networking

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SSL Secure Sockets Layer

SP Service Provider

SPF Shortest Path First

SVC Switched Virtual Circuits

T Tera

TEP Tonnes Equivalent Pétrole

TCP Transmission Control Protocol

VLSM Variable Length Subnet Mask

VoIP Voice Over IP

VRF Virtual Routing and Forwarding

VR Virtual Router

VRI Virtual Router Interface

VPN Virtual Private Network

VC Virtual Circuits

W WATT

WAN Wide Area Network

WLAN Wireless Local Area Network

WSN Wireless sensor network

Introduction générale

L'informatique étant devenue un outil incontournable de gestion, d'organisation, de production et de communication. Les réseaux informatiques d'une entreprise mettent en œuvre des données sensibles, les stockent, et les partagent principalement en interne, différentes méthodes et architectures informatiques sont utilisées dans ces cas là. Il est impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leurs caractères électroniques et confidentiels. Cependant, les données sensibles du système d'information d'une entreprise sont exposées à plusieurs risques.

Le secteur économique de l'énergie en Algérie occupe une place très Importante dans l'économie du pays. Sonatrach est un groupe entièrement intégré sur toute la chaîne de valeur des hydrocarbures, elle possède plusieurs directions, qui sont toutes reliées par des réseaux informatiques formant ainsi une grande toile d'araignée.

La direction ISI, étant celle qui maintient cette toile vivante, a pour objectif principal ; Le développement et la mise en œuvre de l'infrastructure informatique en matière de réseau de service informatique, et la conception d'un réseau d'interconnexion des sites du groupe, en assurant son administration, son exploitation et sa maintenance.

En tant qu'informaticiens, nous savons que, chaque erreur dans un réseau, peut dangereusement nuire à l'intégrité du système, qu'elle soit un bug , une faille de sécurité, ou un protocole obsolète.

Notre objectif, est de faire par un premier temps, la simulation du grand réseau national de la Sonatrach, ses filiales nord sud est ouest, puis dans un deuxième temps proposer des améliorations en termes de sécurité, et qualité de service.

Dans notre cas, la méthode exacte est de faire appel à des protocoles, tel que le MPLS et BGP pour la simulation, étant donné que les réseaux de backbone, sont des réseaux assez évolutifs, qui doivent être tout le temps sous surveillance et maintenance.

Chapitre 1

Présentation De L'organisme D'accueil

1.1. Introduction

Dans ce chapitre nous allons aborder la présentation de la Sonatrach en mettant en avant son historique global, ses diverses missions, L'organigramme de la direction générale de Sonatrach (DG) et de ses départements, ainsi que la direction centrale « Informatique et Systèmes d'Information », étant donné que notre projet d'études est rattaché à celle-ci.

1.2. Présentation de la Sonatrach

Sonatrach est une compagnie nationale algérienne créée le 31 décembre 1963, elle est spécialisée dans la recherche, l'exploitation, le transport par canalisation, la transformation et la commercialisation des hydrocarbures et de leurs dérivés.
Elle a pour missions de valoriser de façon optimale les ressources nationales d'hydrocarbures et de créer des richesses au service du développement économique et social du pays.
Compagnie pétrolière intégrée, Sonatrach est un acteur majeur dans le domaine du pétrole et du gaz. Elle exerce ses activités dans quatre principaux domaines ; l'Amont, l'Aval, le transport par Canalisation et la Commercialisation. [1]

Slogan	« L'énergie du changement »
Logo (Depuis 1967)	
Direction (PDG)	Mr.Toufik Hakkar.
Dépendance hiérarchique	Entreprise publique économique à caractère industriel et commercial.
Effectif	180 000 personnes dans l'ensemble du groupe de Sonatrach.
Capital social(2020)	Les capitaux propres consolidés affichent un montant de 7 888 763 MDZD, ils sont constitués de : • Capital Social 1 000 000 MDZD. • Réserves consolidées qui s'élèvent à 1 011 275 MDZD.
Chiffre d'affaires (2021)	38 milliards de dollars.
Résultat net (2019)	338 milliards de dinars.
Production	Sonatrach, est la première entreprise du continent africain, elle est classée 11ème parmi les compagnies pétrolières mondiales, le 2ème exportateur de GPL et le 3ème exportateur de gaz naturel. [1] Dans un bilan des réalisations de l'année 2021, le groupe pétrolier précise que les premiers indicateurs de production révèlent une augmentation de près de 5% de la production d'hydrocarbures, qui passe de 175,9 millions de Tonnes Equivalent Pétrole (TEP) en 2020 à 185,2 millions de TEP en 2021.

	Pour ce qui est du volume de production au niveau des unités de raffinage, la compagnie pétrolière annonce une stabilité de l'ordre de 27,9 millions de TEP en 2021, contre 27,8 millions en 2020. S'agissant de la production de gaz naturel liquéfié (GNL), Sonatrach a réalisé l'an dernier une "avancée remarquable" de 14% dans ce domaine, ajoutant que le niveau de production a atteint 26,3 millions de m3 en 2021 par rapport à la quantité produite en 2020 (23,1 millions de m3). [2]
Produits	Pétrole, gaz naturel, GNL[1].
Forme économique	Sontrach est une entreprise industrielle, sa classification est justifiée par la nature des biens qu'elle produit en l'occurrence ; les hydrocarbures qui fondent partie de la branche économique du secteur industriel.[1]
Forme Juridique	Société Par Actions (SPA) étatique.
Filiales	Natfal, ENTP, Enip, Enafor, ENGTP, Enac, Sipex, Enageo, Ensp, Hyproc SC, Tassili Airlines.
Site web	www.sonatrach.com. [3]

- **Siége social :**
  La direction générale de Sonatrach est situé à Djenane El Malik à Hydra, 16035 Alger, Algérie. [5] [3]

FIGURE 1.1 : Siège social de Sonatrach
[6]

[1]Gaz naturel de qualité commerciale condensé à l'état liquide. [4]

1.3. L'organisation de la Sonatrach

Dans le schéma d'organisation de la microstructure de groupe Sonatrach, les fonctions et responsabilités s'exercent dans deux sphères ;

- **La Direction Générale du groupe :** Assure les fonctions de pilotage stratégique de cohérence et d'appui, elle comprend :
  - Le Président Directeur Général.
  - Le Secrétaire Général : qui comprend la sûreté interne, la gestion du siège et le comité ADHOC.
  - La Comité Exécutif qui comprend les Vice-présidents Amont, Aval, transport par canalisation et commercialisation.
  - La Comité Examen et Orientation qui comprend des membres permanents, des membres désignés par volet et un secrétariat commun. Les fonctions et responsabilités de ce comité couvrent trois volets : partenariat, acquisition de projet, contrats et ressources humaines.
- **Le staff :** Il comprend les conseils, les leaders de dossiers et d'opérations à portée stratégique ou Symbolique, les assistants et le secrétariat. Les principales structures de la Sonatrach :
  - Les structures opérationnelles.
  - Le Holding international.
  - Les structures fonctionnelles.[1]

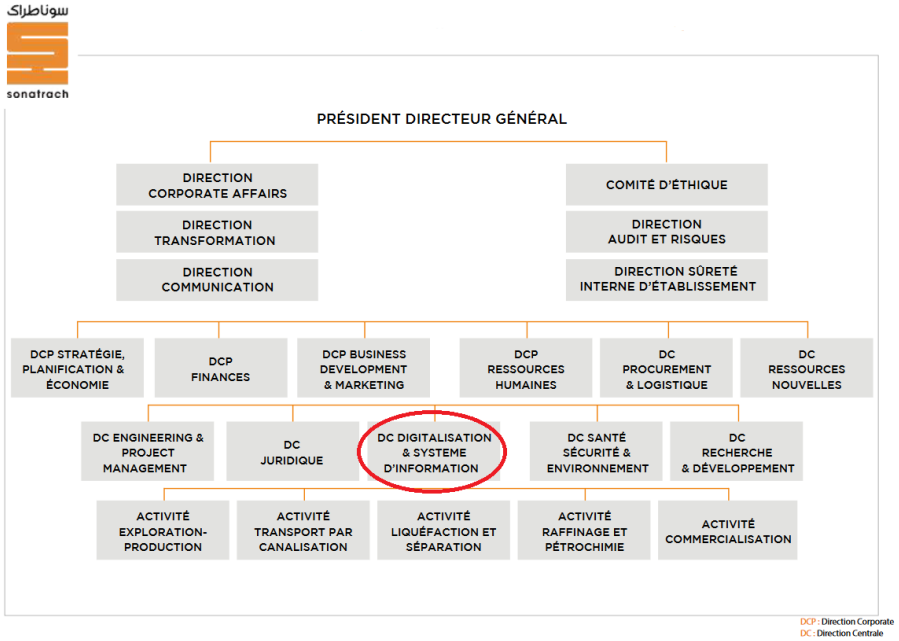


FIGURE 1.2 : Organigramme de la macrostructure de Sonatrach [5]

1.4. Présentation de la direction centrale Informatique & Système d'Information (ISI)

La direction centrale-ISI (DC-ISI) est chargée de la définition des politiques et stratégies de la Sonatrach en matière de système d'information, de technologies de l'information et de la gestion documentaire.
D'une manière générale, elle est responsable de la projection, de la planification, et du développement du SI de l'entreprise afin de l'aligner avec sa stratégie et de l'harmonisation des environnements et des pratiques relatives aux trois directions SI, IT et à QMA.
La (DC_ISI) est la direction de traitement principale de l'entreprise Sonatrach en matière informatique, elle constitue :

- L'outil privilégié de la direction générale en matière d'informatique.
- Le centre de traitement des directions centrales.
- Le prestataire de service qui indique les structures opérationnelles. [1]

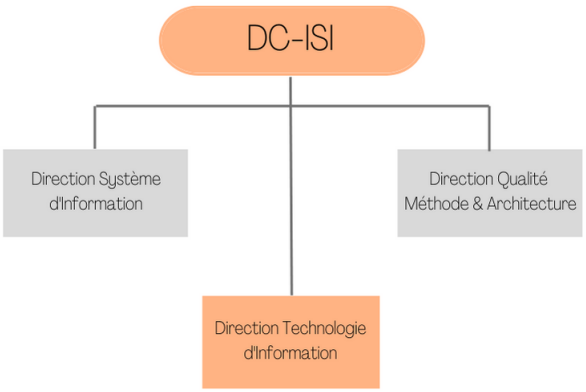


FIGURE 1.3 : Organigramme de la direction centrale ISI
[1]

1.5. Les missions de la direction centrale (ISI)

La Direction Centrale Informatique et Système d'Information (DC–ISI) a pour missions essentielles :

- Le développement de la politique de sécurité du système d'information et technologies de l'information de la société ainsi que leur diffusion et le contrôle de leur application.
- La définition de normes et standards en matière de système d'information et de technologies de l'information et de la gestion documentaire que leur diffusion et le contrôle de leur application.
- La mise en place d'un plan de modernisation du système d'information et des technologies de l'information et l'accompagnement aux changements au niveau de la société.
- Le développement et la mise en œuvre de l'infrastructure informatique en matière de réseau de service informatique d'accès à internet de messagerie et de solutions de mobilité.
- La conception et la mise en place d'un réseau d'interconnexion des sites du groupe en assurant son administration, son exploitation et sa maintenance.
- La mise en place de la gestion d'un système d'information documentaire permettant la capitalisation du savoir-faire, la conservation de la société

et la sauvegarde de son patrimoine documentaire.

- La maîtrise d'œuvre et l'assistance à maîtrise d'ouvrage auprès des activités opérationnelles.
- Le développement et la mise en œuvre d'un système de management de la qualité pour l'ensemble de la structure informatique de la société.
- L'élaboration des cahiers des charges relatifs aux systèmes d'information et technologies de l'information en collaboration avec les structures de la société.
- Le pilotage et la gestion des projets informatiques structurants et d'intégration.
- La coordination avec direction télécommunications de l'activité transport par canalisation a la définition de la politique et les standards en matière de télécommunication basées sur l'infrastructure informatique.
- Le conseil et l'assistance aux structures de la société en matière de système d'information et des technologies de l'information.
- La coordination de la politique en matière d'organisation et de mise en place de la fonction gestion des documents des archives au sein du groupe.
- La constitution des centres d'expertise dans chacun des domaines d'activité de la DC ISI.
- Le développement des relations avec les institutions spécialisées en matière de système d'information et des technologies de l'information.
- L'appui aux projets de la société. [1]

Chapitre 2

Étude Du Thème

2.1. Problématique

La mise en place des technologies de l'information, du réseau WAN de la Sonatrach d'une façon complète, et de sa maintenance et son évaluation, sont très couteuses en termes d'équipements, d'argent, de temps et d'efforts. Mais aussi,en termes de limitations géographiques.

2.2. Spécifications des besoins

Suite aux échanges effectués avec notre responsable a l'ISI, plusieurs besoins ont été relevés, à savoir :

- Besoin de crypter/sécuriser de façon efficace les données qui transitent le backbone.
- Besoin de positionner les filiales et les segmenter en sous réseau.
- Besoin de mettre en place le réseau WAN câblé avec ces interconnexions Nord-Sud-Est-Ouest.
- Besoin d'assurer le bon acheminement des paquets entre les filiales.
- Besoin de contrôler les accès des filiales.
- Besoin d'utiliser des équipements et protocoles de routage adéquats.

2.3. Objectifs

A travers notre stage, ainsi que notre formation universitaire en réseaux, en tant qu'étudiants, notre but est de répondre aux besoins énumérés plus haut. Notre objectif principal qui consiste à la configuration et la mise en place du réseau WAN actuel de la Sonatrach via une simulation virtuelle sur deux plateformes différentes, avec ses interconnexions pour l'échange des informations entre l'ensemble des équipements de ce dernier afin d'aboutir à des solutions pour certains problèmes et bugs, ainsi qu'une perspective d'amélioration.

2.4. Démarches à suivre

Dans la suite de notre étude, nous allons mettre en place le réseau actuel de la Sonatrach en mettant l'accent sur la protection et le bon acheminement des données du réseau avec l'utilisation des protocoles de routage conforme. Nous finirons par une sorte de techniques plus efficace et moderne afin d'améliorer cette architecture réseau.

Chapitre 3

Outils De Simulation Et Routage

3.1. Introduction

La simulation, en général, est l'imitation fictive d'une situation réelle. Dans le domaine des réseaux informatiques, la simulation réseau est une technique qui sert à reproduire et à gérer l'architecture d'un réseau virtuellement. Ce qui est bien avec les simulateurs c'est que l'administrateur réseau peut faire son traitement sur des équipements logiques avant d'implémenter le réseau en pratique, ce qui lui permettra de réduire les risques en faisant des tests sous différentes charges de trafic et dans diverses conditions de pannes, sans nuire aux réseaux existants mais aussi d'en apprendre à chaque fois sur le nouveau matériel et les logiciels avant de les acheter. Il existe plusieurs logiciels de simulation réseau, on trouve le gns3, ensp, marionnet, eve et bien d'autres.[7] Pour la réalisation de ce projet on a opté pour ces deux simulateurs : eNSP pour les équipements Huawei et Gns3 pour les équipements Cisco.

- **Différence entre les deux simulation continue et discrète :** La simulation d'événements discrets (DES) modélise le fonctionnement d'un système comme une séquence d'événements discrets qui se produisent à différents intervalles de temps. La simulation continue (CS) modélise les opérations d'un système pour suivre en continu les réponses du système pendant toute la durée de la simulation. [8]

3.2. Définition d'un simulateur réseau

Le logiciel utilisé pour prédire les performances d'un réseau informatique est appelé simulateur de réseau. Ceux-ci sont utilisés lors des communications

réseau, qui sont devenues trop difficiles pour que les techniques analytiques fixes offrent une compréhension précise des performances du système. Dans un simulateur, le réseau informatique peut être simulé à l'aide de liens, de dispositifs et d'applications comme ceux qui sont utilisés aujourd'hui : IoT,5G, WLAN, réseaux ad hoc de mobiles, WSN, LTE, réseaux ad hoc de véhicules, etc. [9]

3.2.1 Présentation du simulateur GNS3

Graphical Network Simulator (GNS3) est un logiciel open source qui peut être considéré comme un lieu de rencontre pour une variété d'émulateurs de système d'exploitation.
Les émulateurs pris en charge par GNS3 sont les suivants :

- **Dynamips :** C'est le plus connu et le plus important d'entre eux, permet d'émuler des routeurs Cisco et fournit une collection de périphériques et d'interfaces génériques.
- **Qemu :** il fournit l'émulation des périphériques Cisco ASA, des routeurs Juniper, des routeurs Vyatta et des hôtes Linux.
- **Pemu :** Il s'agit d'une variante de Qemu utilisée expressément pour les pare-feux Cisco PIX.
- **VirtualBox :** Cela fournit une émulation des routeurs Juniper, des routeurs Vyatta, des hôtes Linux et des hôtes Windows.

Les appareils comme les routeurs et les pare-feu nécessitent une sorte d'application de terminal pour donner accès, elle diffère selon le système d'exploitation, elle peut être Gnome Terminal, iTerm2, Konsole, PuTTY, SecureCRT, SuperPutty, TeraTerm, Windows Telnet client ou même Xterm.[10]

- **Avantages de GNS3 :**
  - Il permet de construire des topologies complexes.
  - Il est possible de capturer en temps réel le trafic qui passe par les interfaces des périphériques.
  - Les topologies créées sont importables/exportables. GNS3 est gratuit d'utilisation.
  - Il évolue rapidement en plusieurs branches. [11]
- **Configuration système requise pour GNS3 :**
  Avant de commencer à exécuter GNS3 sur l'ordinateur, il faut d'abord

assurer qu'il est à la hauteur, et cela dépendra en grande partie du nombre d'appareils qui seront inclus dans les simulations et de leurs quantité de mémoire car chaque instance d'un routeur ou de tout autre périphérique qui sera exécuté va générer une copie de son propre système d'exploitation qui concourra pour les cycles de RAM et de CPU de l'ordinateur hôte.[10]

Item	Requirement
Operating System	Windows 7 (64 bit) or later
Processor	2 or more Logical cores
Virtualization	Virtualization extensions required. You may need to enable this via your computer's BIOS.
Memory	4 GB RAM
Storage	1 GB available space (Windows Installation is < 200 MB).
Additional Notes	You may need additional storage for your operating system and device images.

FIGURE 3.1 : Configuration minimale
[12]

Item	Requirement
Operating System	Windows 7 (64 bit) or later
Processor	4 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT
Virtualization	Virtualization extensions required. You may need to enable this via your computer's BIOS.
Memory	16 GB RAM
Storage	Solid-state Drive (SDD) with 35 GB available space
Additional Notes	Virtualizing devices is processor and memory intensive. More is better but properly configured device trumps RAM and Processing power.

FIGURE 3.2 : Configuration recommandée
[12]

Item	Requirement
Operating System	Windows 7 (64 bit) or later
Processor	Core i7 or i9 Intel CPU / R7 or R9 AMD CPU / 8 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT
Virtualization	Virtualization extensions required. You will need to enable this via your computer's BIOS.
Memory	32 GB RAM
Storage	Solid-state Drive (SDD) with 80 GB available space
Additional Notes	Virtualizing devices is processor and memory intensive. More is better, but a properly configured device trumps RAM and processing power.

FIGURE 3.3 : Configuration optimale
[12]

3.2.2 Présentation du simulateur ENSP

C'est un logiciel gratuit propriétaire de "Huawei Technologies" spécialisé dans la simulation de réseaux informatiques, semblable à Packet Tracer, Junosphere ou encore l'alternative libre GNS3.
Il simule les routeurs et les commutateurs Huawei d'entreprise, offrant une présentation parfaite des appareils réels. eNSP prend en charge la simulation de réseau à grande échelle et permet aux utilisateurs de mettre en œuvre des tests expérimentaux et d'apprendre les technologies de réseau sans utiliser de dispositifs réels.[13]

- On décrit quelques avantages :
  - **Simulation précise :** eNSP simule de près les éléments réels du réseau.
  - **Déploiement distribué :** le serveur eNSP peut facilement être déployé sur plusieurs serveurs, formant un réseau complexe.
  - **Mélange de virtuel et de physique :** il permet une expérience à la fois virtuelle et mixte ce qui aide à Surmonter la limitation des ressources réseau insuffisantes. [13]
- **Configuration système requise pour eNSP :**

Item	Minimum Configuration	Recommended Configuration	Expanded Configuration
CPU	Dual-core 2.0 GHz or faster	Dual-core 2.0 GHz or faster	Dual-core 2.0 GHz or faster
Memory (GB)	2	4	4 + n (n > 0)
Free disk space (GB)	1	2	2
Operating system	Windows XP Windows Server 2003 Windows 7	Windows XP Windows Server 2003 Windows 7	Windows XP Windows Server 2003 Windows 7
Maximum number of networking devices	4	8	8 + 4*n

(a) Pour un seul ordinateur

-	Item	Minimum Configuration	Recommended Configuration	Expanded Configuration
Server	CPU	Dual-core 2.0 GHz or faster	Dual-core 2.0 GHz or faster	Dual-core 2.0 GHz or faster
	Memory (GB)	2	4	4 + n (n > 0)
	Free disk space (GB)	1	2	2
	Operating system	Windows XP Windows Server 2003 Windows 7	Windows XP Windows Server 2003 Windows 7	Windows XP Windows Server 2003 Windows 7
	Maximum number of networking devices	4	8	8 + 4*n
Client	CPU	Dual-core 2.0 GHz or faster	Dual-core 2.0 GHz or faster	-
	Memory (GB)	1	2	
	Free disk space (GB)	0.1	0.2	
	Operating system	Windows XP Windows Server 2003 Windows 7	Windows XP Windows Server 2003 Windows 7	

(b) Pour plusieurs ordinateurs

FIGURE 3.4 : Configuration requise
[13]

3.3. Les équipements utilisés

Pour démarrer un élément actif tel qu'un routeur Cisco dans GNS3, il doit avoir une image réelle de Cisco IOS disponible dans ce dernier.
Les images IOS[1] prennent en charge différents packages tels que le routage, la commutation et l'interconnexion de réseaux, etc.

3.4. Besoins matériels du déploiement de la simulation virtuelle

Ce projet est réalisé avec 6 routeurs de type Provider (P), 10 routeurs de type Provider Edge (PE), 20 routeurs de type Customer Edge (CE).
Nous avons opté notre choix sur ces routeurs ci dessous car ces derniers sont adéquats aux besoins fonctionnels de la simulation.

- **Partie Huawei :**
  - **Router de type P : NE9000**
    Les routeurs NE9000 servent de nœuds centraux sur les grands

[1]Elles contiennent le code système de l'équipement utilisé pour fonctionner, ainsi que divers ensembles de fonctionnalités (facultatives ou spécifiques au routeur).[14]

réseaux DCI[2], comme dans le cas de la Sonatrach, les grands réseaux d'entreprise, mais aussi de super-nœuds centraux sur les réseaux dorsaux des opérateurs. En effet, ils sont dotés d'une grande fiabilité présentant une capacité élevée et une faible consommation d'énergie, parfaits dans le cas des Providers. Ils gèrent aussi l'OSPF, MPLS et BGP.
-Equipés du meilleur fond de panier 28G du secteur, qui peut être étendue à 56G, voire prochainement à 112G. Une telle capacité représente quatre fois la moyenne du secteur : 4T (évolutivité à 8T) par emplacement et 80T (évolutivité à 160T) par châssis.
-Interconnexion cloud sécurisée, intelligente, simple et très haut débit.
-Automatisent et optimisent le trafic réseau et, selon la bande passante et la latence, améliorent l'utilisation de la bande passante de 50 %. Ces routeurs offrent des fonctions de restauration et de planification multicouche IP + optique. [15]

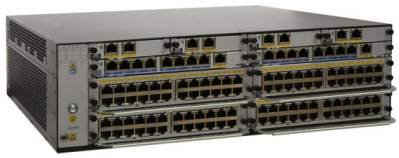
Performances de transmission :
14 464 Mpps - 36 160 Mpps
Capacité de commutation :
84 Tbit/s - 209 Tbit/s
Types de ports :
400GE, 100GE, 40GE et 10GE
Consommation d'énergie typique :
0,4 W/G [15]

– **Router de type PE : NE40E**
Servent principalement de nœuds périphériques sur les réseaux Backbone, les réseaux métropolitains, et les réseaux IP à grande échelle, ici, adéquatement utilisés dans en Provider Edge. Ils offrent des performances élevées, une faible consommation d'énergie, une technologie de canal IP rigide innovante et une capacité d'évolution rapide, les routeurs NE40E répondent aux exigences de faible latence et de haute fiabilité des services stratégiques. Ils s'appuient sur une architecture SDN.
Dotés des meilleures technologies MPLS et d'optimisation de réseau IP natif, ils peuvent résoudre les problèmes tels que la répartition inégale du trafic, la faible utilisation de la bande passante

[2]Une technologie qui relie au moins deux data centers sur des distances courtes, moyennes ou longues en utilisant une connectivité optique de paquets à haut débit.

et la faible convergence réseau engendrées par la répétition des calculs de topologie en cas de panne.
Performances de transfert :
540 Mpps - 14 464 Mpps
Capacité de commutation :
1,08 Tbit/s - 81,92 Tbit/s
Consommation électrique maximale :
920 W - 9040 W (480G) [16]

- **Router de type CE : AR3260**
  Généralement utilisés dans les entreprises, dans notre maquette, il représente les CE pour clients. AR3260 est un routeur de classe entreprise de nouvelle génération basé sur la plate-forme de routage polyvalente (VRP). Il intègre les fonctions de routage, de commutation, de 3G, de voix, et de sécurité. Il utilise le processeur multicœur, fournit une solution intégrée pour les réseaux d'entreprise, accélère la fourniture de plusieurs services et protège les investissements des clients.
  MPLS, mappage des priorités, régulation du trafic, mise en forme du trafic, évitement de la congestion, gestion de la congestion, OSPF, BGP.



Capacité de transfert :
2 Mpps (standard) - 3.5 Mpps
Capacité de commutation :
160Gbps
Vitesse WAN services :
1000Mbps **Ports WAN fixes :**
3*GE (deux ports combinés) [17]

- **Partie Gns3 :**
  - **Router de type P : Cisco c3745** Pour pouvoir implémenter MPLS dans les P, le choix du Routeur est très important car il y'a ceux qui ne supportent pas cette technologie.
    Nous allons utiliser le routeur Cisco de la gamme 3745 pour les raisons suivantes :
    C'est un routeur multiservices qui fournis une connectivité LAN/-

WAN et offrent un espace plus large pour les cartes d'interface.

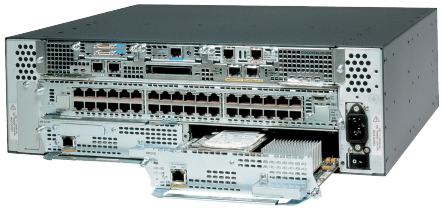


FIGURE 3.5 : Cisco 3745
[18]

– **Router de type PE :** Cisco c2691 Routeur, 2 ports Ethernet 10/100, 3 emplacements WAN, un emplacement pour module réseau et deux emplacements AIM (+ 100 % Fast Switching (PPS) par rapport au 2651XM.

FIGURE 3.6 : Cisco c2691
[19]

– **Router de type CE :** Cisco c1700
Le choix est mis sur ce routeur car il est idéale pour les petites filiales et les petites et moyennes entreprises qui ont besoin d'un accès 'sécurisé,rapide et fiable' aux applications professionnelles, aux ressources réseau et aux services Internet pour tous les utilisateurs. [20]

FIGURE 3.7 : Cisco 1720
[21]

3.5. Les protocoles de routage et les techniques utilisées

Pour acheminer le trafic vers un hôte ou un réseau non connecté, on doit définir une route vers l'hôte ou le réseau, à l'aide d'un routage statique ou dynamique.
Généralement, on doit configurer au moins une route statique.
Et lorsque nous parlons de routage, nous parlons de périphériques de couche 3, ils utilisent les protocoles de routage qui déterminent puis sélectionnent le meilleur chemin pour transmettre les paquets, à travers des WAN ou plusieurs LAN.[22]
A cet effet, la communication entre différents protocoles de routage dépend des algorithmes de routage qui se basent sur les nœuds à déterminer la route pour transmettre le paquet sur les réseaux. Le routage sur Internet joue un rôle important, c'est donc le battement de cœur d'internet.
Les protocoles de routage dynamique sont composés en deux catégories différentes : Protocoles de passerelle intérieure (IGP) et les protocoles de passerelle extérieure (EGP). Les IGP comme OSPF et EIGRP fonctionnent dans un routage de système autonome tandis que les EGP (tels que BGP) fonctionnent pour le routage entre plusieurs systèmes autonomes.[23]

3.6. Routage par défault

Son principe désigne toutes les plages d'adresse IP non configurées vers une route explicite.
Ce mécanisme, fait en sorte que le routeur ne supprime pas les paquets s'il n'y a pas de correspondance sur la table de routage. De plus, les routes par défaut ne sont placées que sur les routeurs stub, car on ne peut les pointer que dans une seule direction.[22]

3.7. Routage statique

Le routage statique est la configuration et la sélection manuelles d'un itinéraire réseau, généralement gérées par l'administrateur réseau.
Les routes statiques conviennent mieux aux petits réseaux, tels que les réseaux locaux, où les routes changent rarement. [24]

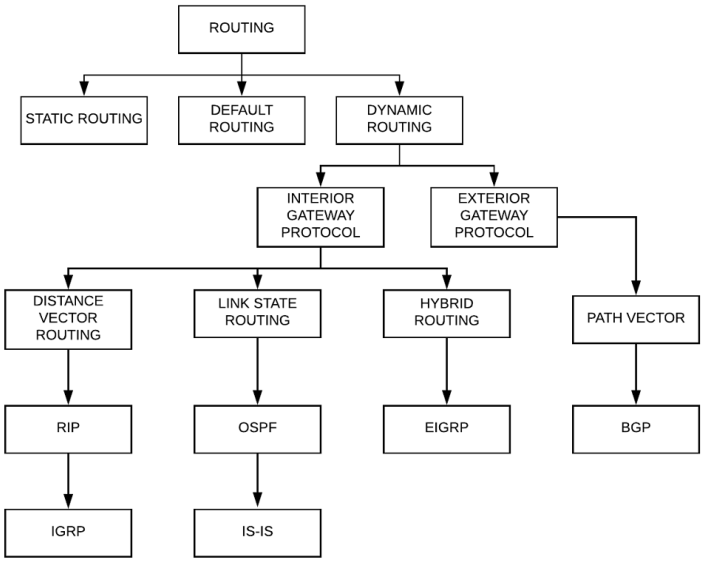


FIGURE 3.8 : Les routages
[25]

3.8. Routage Dynamique

Un protocole de routage est un ensemble de processus, d'algorithmes et de messages utilisés pour échanger des informations de routage, qui seront utilisées pour remplir la table de routage avec les meilleurs chemins vers les destinations sur le réseau. Lorsque les routeurs apprennent des changements de la topologie du réseau, ces informations seront transmises dynamiquement à d'autres routeurs.[26]

3.8.1 Protocoles IGP

IGP est appelé le protocol d'intérieur car il est responsable de l'acheminement du trafic au sein d'un système autonome.

- **OSPF :** C'est un protocole de routage dynamique développé par l'IETF qui est implémenté dans un seul Système autonome. Il s'agit d'un protocole non propriétaire de Cisco qui s'exécute sur n'importe quel fournisseur de routeur.
  Chaque routeur possède une base de données identique (LSDB). Il trouve l'itinéraire du plus court chemin basé sur l'algorithme de Dijkstra. Chaque élément de cette base de données décrit un routeur spécifique et son état actuel, qui inclut l'état des interfaces, les voisins joignables et d'autres informations. Le routeur distribue ces informations sur le Système Autonome par inondation (flooding). Chaque routeur exécute l'algorithme en parallèle avec d'autres routeurs SPF, et à partir de la base de données interne, il construit un arbre des chemins les plus courts avec lui-même comme racine. L'arborescence contient une route vers chaque destination dans le système autonome. Les routes externes sont ajoutées à l'arborescence en tant que "feuilles". OSPF permet le regroupement de réseaux en un ensemble, appelé une zone (area).[27]

  En outre, OSPF utilise le coût comme métrique, que le SPF fournira. Plus le lien est rapide, plus le coût est faible, ce qui signifie que plus le lien est lent, plus le coût est élevé. Mais, il y a toujours la possibilité de remplacer le calcul en utilisant la commande **ip ospf cost**, qui a une plage de 1 à 65 535.[22]

3.8.2 Protocoles EGP

- **Exterior Gateway Protocol (BGP) :**

  Le BGP est le seul protocole EGP qui existe, il effectue le routage entre les Autonomous System (AS), il est également connu sous le nom de protocole Internet càd que l'internet est une collection de systèmes autonomes.
  Le BGP est divisé en deux protocols : IBGP et EBGP [28]

  – **IBGP :** Les voisins fonctionnent autour du même système autonome et n'ont pas besoin d'être directement connectés les uns aux autres, ils leur faut seulement une communication TCP entre eux.
  Autre point à mentionner pour IBGP est que la mise à jour entre les pairs n'est pas fonctionnelle, cette restriction est placée dans le but de prévenir les boucles dans le même AS.[29]

  – **EBGP :** Les voisins sont connectés les uns aux autres dans différents systèmes autonomes (AS). Les voisins EBGP doivent être

directement connectés les uns aux autres.[29]

- **Autonomous System Number (ASN) :** Le numéro de système autonome est un numéro spécial attribué par l'IANA, il est utilisé principalement avec le BGP qui identifie de manière unique un réseau sous une seule administration technique, qui a une politique de routage unique ou qui est multi-hébergé sur l'Internet public.
  - **ASN Public :** Un ASN dans la plage publique est unique au monde et peut être annoncé sur l'Internet mondiale à votre FAI ou à un point d'échange Internet (point de peering) via BGP. Les ASN sont utilisés pour identifier de manière unique les réseaux ou les systèmes de réseaux qui semblent au monde extérieur, exécuter une seule politique de routage cohérente. Les préfixes sont "vus" comme provenant de ces ASN publics par le protocole de routage de la passerelle extérieure (BGP). Celà garantit que les routes ramènent à une source unique d'une plage d'adresses IP donnée.[30]
  - **ASN Privé :** L'ASN privé ne doit pas être vu sur l'Internet mondial (il ne doit pas être annoncé via le protocole de routage de la passerelle extérieure). [30]

3.9. MPLS

3.9.1 Introduction

Les processus d'analyse/recherche des paquets IP, l'obtention de l'adresse IP de destination, la comparaison avec les entrées de la table de routage, l'obtention de l'adresse du saut suivant et enfin de transfert du paquet vers le saut suivant, toutes ces étapes se répètent à chaque nœud/routeur, ce qui a augmenté le temps total nécessaire au paquet pour atteindre la destination. Ces mêmes processus sont aussi gourmands en CPU, ce qui entravait le fonctionnement des nœuds de réseau jusqu'à ce que l'idée du MPLS soit apparue en 1996 par un groupe d'ingénieurs de Ipsilon Networks dans le but de résoudre ces problèmes.[31]

La commutation multiprotocole par étiquette ou MPLS, bien qu'ancienne, reste l'une des technologies de routage les plus populaires utilisées aujourd'hui. Il aide à router/transmettre les paquets de données beaucoup plus rapidement sur le réseau par opposition au routage IP natif.[31]

3.9.2 Définition du MPLS

MPLS ou Multiprotocol Label Switching ce n'est un pas un protocole mais une technologie de transfert de paquets qui utilise des étiquettes afin de prendre des décisions de transfert de données.[32] Le nom multiprotocole a été donné parce que cette technologie peut prendre en charge et fonctionner avec différents types de protocoles comme VPN de couche 3, IPv4, IPv6, Ethernet et cela permet le développement de réseaux hautement efficaces, évolutifs et sécurisés qui garantissent des accords de niveau de service.[31]

3.9.3 Le réseau MPLS

Il se compose de divers nœuds et relie différents emplacements de divers clients d'entreprise. [33]

- **Routeur d'entrée (LER ou PE) :**
  Le routeur d'entrée est un nœud de réseau qui reçoit le paquet IP (la trame de données), effectue une recherche d'IP de destination, détermine la FEC, attache l'étiquette appropriée et la transmet au LSR.[31]
- **Routeur de commutation d'étiquette (LSR ou P) :**
  Est un nœud de réseau qui se trouve à l'intérieur du réseau Mpls, qui reçoit un paquet Mpls, vérifie les tables de routage, remplace l'étiquette et l'envoie au LSR suivant.[31]
- **Routeur de sortie (LER ou PE) :**
  C'est un nœud de réseau qui reçoit le paquet Mpls, supprime l'en-tête Mpls et transmet le paquet IP natif à la destination.[31]

3.9.4 Structure du paquet Mpls

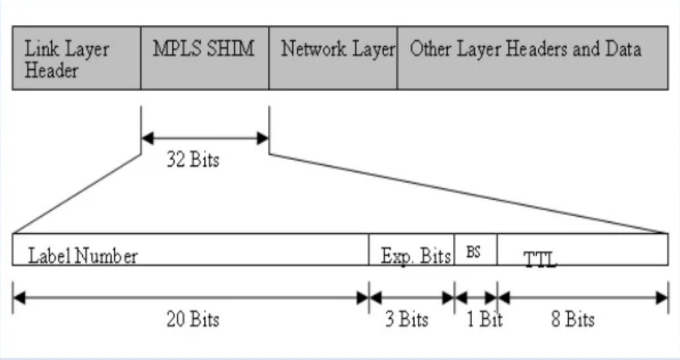


FIGURE 3.9 : Structure du paquet Mpls
[33]

3.10. VPN

C'est la connexion réseau entre des appareils qui ne partagent pas littéralement un câble physique est appelé VPN. C'est un moyen d'utiliser un réseau public pour des communications privées, entre un ensemble d'utilisateurs et/ou de sites. [34]

3.11. MPLS VPN Terminologie :

Cette terminologie est basée sur une distinction claire entre le fournisseur de services réseau (réseau P) qui est toujours topologiquement contigu alors que le réseau client (réseau C) est généralement clairement délimité en plusieurs sites[35] ; comme illustré à la Figure 3.12.

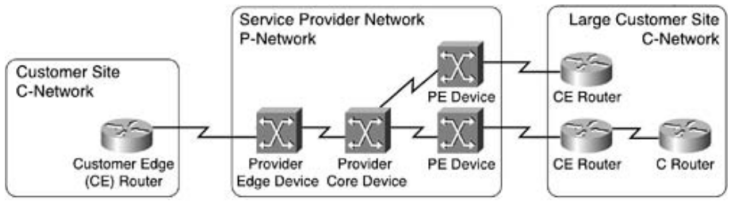


FIGURE 3.10 : Terminologie de VPN basé sur MPLS
[35]

Les technologies VPN ont évolué en deux approches majeures pour l'implementation des prestations de service VPN :
-VPN sans connexion : Les appareils PE participent au transport de données sans connexion entre les appareils CE. Il n'est pas nécessaire que le prestataire de services ou le client établir des VC dans ces VPN, sauf peut-être entre les routeurs PE et CE si le fournisseur de services utilise le WAN commuté comme technologie de réseau d'accès.
-Connexion VPN orientée : Les appareils PE fournissent des lignes louées virtuelles entre les appareils CE. Ces lignes louées virtuelles sont appelées circuits virtuels (VC). Les VCs peuvent être permanent, établi hors bande par l'équipe de gestion du réseau du fournisseur de services (appelés circuits virtuels permanents, ou PVC). Ils peuvent aussi être temporaires, établis sur demande par les dispositifs CE via un protocole de signalisation que les dispositifs PE comprennent. (Ces VCs sont appelés circuits virtuels commutés ou SVC[35].

3.12. VPN basé sur MPLS :

Cette technologie utilise une combinaison de services orientés connexion(réduit les frais généraux 'overhead' sur le P dispositifs) et sans connexion (minimisant la complexité de l'approvisionnement ainsi que le coût) :
- L'interface entre les routeurs CE et les routeurs PE est sans connexion.
-Aucune configuration supplémentaire est nécessaire sur les appareils CE.
- Les routeurs PE utilisent un paradigme de transfert IP modifié ; un routage IP distinct et table de transfert (appelée table virtuelle de routage et de transfert, ou VRF) est créée pour chaque client.
- Les adresses du client sont étendues avec des routes distinguishers 64 bits pour rendre les adresses IP 32 bits non uniques globalement uniques au sein du backbone des fournisseurs de services.
-Les adresses 96 bits résultantes sont appelées adresses VPNv4.
- Un seul protocole de routage est exécuté entre les routeurs PE pour tous les clients VPN est le BGP.
- Les routeurs PE utilisent des VC basés sur MPLS (appelés chemins à commutation d'étiquettes ou LSP) pour transporter les datagrammes du client entre les routeurs PE. Des étiquettes MPLS supplémentaires sont insérées devant les datagrammes IP du client pour assurer leur bonne transmission depuis le routeur PE d'entrée vers le routeur CE de destination.
- Les LSP entre tous les routeurs PE sont établis automatiquement en fonction de la topologie IP du réseau P. Il n'est pas nécessaire de configurer ou

d'établir manuellement ces chemins. Le mappage entre les adresses de destination du client et les LSP menant vers les routeurs PE de sortie sont exécutés automatiquement en fonction des prochains sauts BGP. [35]

3.13. VRF

C'est une technologie qui permet à plusieurs instances d'une table de routage de coexister au sein du même routeur en même temps.[36]
Une ou plusieurs interfaces physiques ou logiques peuvent avoir un VRF, mais aucun des VRF ne partage de routes. Les paquets sont transmis uniquement entre les interfaces sur le même VRF.[37]
Lors de la création de VRF supplémentaires, la table de routage d'origine existe toujours. Il s'agit du VRF par défaut, également connu sous le nom de table de routage globale.
Ils fournissent des chemins de réseau complètement isolés sans entrer en conflit les unes avec les autres. Rien ne peut être mappé de l'un à l'autre sans qu'un administrateur crée un lien. Les VRF sont les plus courants dans les réseaux MPLS des fournisseurs de services pour isoler différents clients.[38]

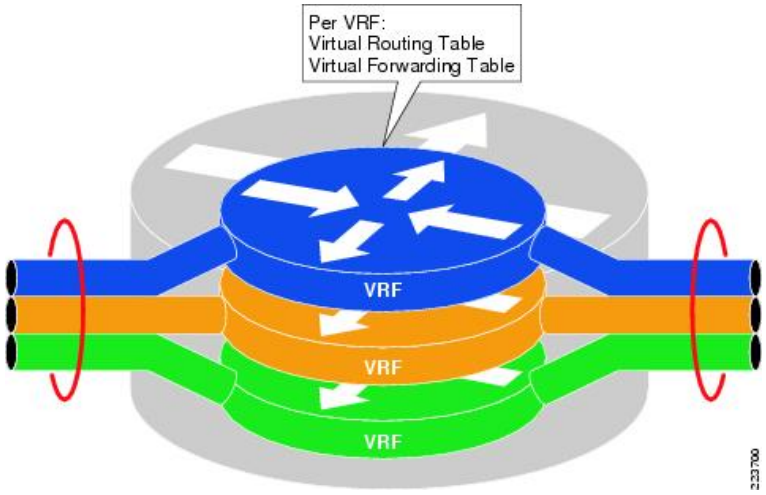


FIGURE 3.11 : Terminologie de VPN basé sur MPLS
[38]

- **Type de VRF :**
  Il existe essentiellement deux types de VRF :
  VRF dans sa forme complète et VRF lite.
  Voici les différences fondamentales.

- **Le VRF complet :** se concentre sur l'étiquetage du trafic de couche 3 via MPLS, une idée similaire aux VLAN de couche 2.
  La commutation d'étiquettes multiprotocoles ou cloud MPLS dans l'environnement cloud du fournisseur de services utilise le protocole de passerelle frontalière multiprotocole, ou MP BGP. VRF isole le trafic de la source à la destination via ce cloud MPLS. Pour séparer les routes qui se chevauchent et utiliser des services communs, le VRF intègre des Route Distinguisher (RD)[3]et des Route Target (RT)[4].[37]
- **Le VRF lite :** VRF sans l'utilisation d'MPLS et le BGP, est généralement utilisé dans l'environnement de réseau local de bureau ou de centre de données pour virtualiser diverses zones de sécurité et éléments de réseau.
  Le VRF complet est une solution hautement évolutive, tandis que le VRF lite n'est pas évolutif.[37]

[3]crée une adresse VPNv4 unique sur le réseau MPLS.[39]
[4]définit quels préfixes sont importés et exportés sur les routeurs PE.[39]

Chapitre 4

Justifications Et Comparaisons

4.1. Introduction

De nos jours, dans le réseau central (backbone) du fournisseur de services, nous n'utilisons pas le transfert IP, nous optons plutôt pour le MPLS car il permet une commutation plus efficace des paquets.
De plus, le MPLS VPN utilise la puissance de la commutation multi protocole par étiquette pour créer des réseaux privés virtuels (VPNs). Ces deux technologies combinées nous permettent de connecter géographiquement en toute sécurité des sites divers sur un réseau MPLS.
Les services MPLS peuvent être utilisés afin de connecter différents sites à un réseau backbone et assurer une meilleure performance pour les applications à faible latence telles que la voix sur IP (VoIP) et d'autres fonctions critiques pour l'entreprise. [34]

4.2. Topologie

Notre réseau consiste en un ensemble de sites qui sont interconnectés au moyen d'un réseau central de fournisseur MPLS. Sur chaque site, il y a diffirentes filiales (CE), qui se connectent à un ou plusieurs dispositifs de type (PE).

- **Conditions requises pour la mise en oeuvre de cette topologie :**
  - Accessibilité IP de base.
  - IGP en cours d'exécution (OSPF).

- Cisco Express Forwarding (CEF).
- MPLS.
- Protocole de distribution d'étiquettes (LDP).
- Session BGP VPNv4 entre les PE : IBGP est nécessaire dans le cloud pour échanger les routes VPNv4.[34]
- Simulateurs GNS3/Ensp pour exécuter et mettre en œuvre le VPN MPLS L3.
- 4 Go de RAM, au minimum, installés sur le PC/ordinateur portable exécutant GNS3 et Ensp.
- Images Cisco et huwaei IOS pour prendre en charge les fonctionnalités MPLS. [40]

4.3. Plan du routage

Notre réseau a été construit à travers une combination de routage différent ; statique et dynamique.
Les protocoles de routages dynamique sont : OSPF, BGP qui sont utilisés pour déterminer le meilleur chemin de la source à la destination, en fonction de leurs algorithmes particuliers.

1. **Le routage par défaut :** indique essentiellement au routeur qu'il n'y a pas de correspondance dans la table de routage pour ce réseau de destination et qui'il utilise la route par défaut et envoie au routeur suivant.
   - Ce routage est vraiment un mécanisme, de sorte que le routeur ne supprime pas les paquets s'il n'y a pas de correspondance sur la table de routage. De plus, les routes par défaut ne sont placées que sur les routeurs stub (CE dans notre cas), car on peut les pointer que dans une seule direction.
2. **Le routage statique :** les Ce sont des routeurs d'extrémité, la configuration des Protocol de routage, n'est pas essentielle donc on a ajouté manuellement les réseaux de destination pour les raisons suivantes :
   - Les routeurs n'enverra pas de mises à jour, moins de surcharge CPU/-ram et donc moins d'utilisation de la bande passante ; ce qui peut permettre d'économiser et d'acheter des routeurs moins chers en vrai.
   - Une couche de sécurité existe en utilisant des routes statiques puisque c'est l'administrateur qui construit la table de routage à partir de zéro

donc il aura un accès total sur les entrées et sorties du réseau.
- Les routes statiques sont utiles car elles peuvent être utilisées à l'unisson avec les protocoles de routage et agir comme des routes de secours.[22]

3. **Routage dynamique :**

- **OSPF comme IGP :**

- Les FAI essaient de répondre aux demandes de trafic avec les nouvelles technologies et enrichi les ressources existantes. Elles utilisent principalement l'OSPF pour déterminer le meilleur chemin des paquets.[23]
- Le comportement de l'OSPF est meilleur, plus intelligent et moins redondant que celui de l'EIGRP vu que sa performance est dû à l'échange de moins de mises à jour de routage, il s'appuie sur les informations précédentes, ce qui donne des étapes plus réduites alors qu'avec l'EIGRP a besoin des mêmes informations encore et encore, telles que les ajouts, les suppressions et les mises à jour et fait donc perdre plus de temps et de ressources comme le CPU.[23]
- Le meilleur service d'effort (best effort service) pour la transmission de paquets de données, OSPF fonctionne mieux que les autres protocoles (RIP, IGRP, EIGRP) pour le débit, délai de mise en file d'attente, utilisation et surcharge.[41]
- BGP n'a jamais été conçu pour une fonction IGP. En tant que tel, nous n'obtiendrons pas une convergence rapide avec BGP. Avec le protocole OSPF nous permet d'obtenir une convergence en moins d'une seconde ces jours-ci.[35]

- **IBGP sur les routeurs (PE) :**

- L'utilisation de l'MPLS necessite obligatoirement le IBGP.
- Le IBGP est nécessaire pour s'appairer entre d'autres routeurs PE, donc après sa configuration il annonce non seulement les valeurs RD/RT avec chaque préfixe, mais il annonce également l'étiquette VPN d'une façon plus correcte.[34]

4.3.1 Création des VRFs :

Le VPN de couche 3 utilise le VRF de couche 3 pour segmenter les tables de routage pour chaque filiale utilisant ce service (le routeur (CE) s'apparie avec le routeur du fournisseur de services (PE) et les deux routes d'échange, qui sont ensuite placés dans une table de routage spécifique à la filiale).[34]

4.4. Tableau comparatif sur les protocoles de routage dynamique

	Rip v1	Rip v2	Ospf	Eigrp	BGP
Distance administrative	120	120	110	90 (routes internes) 170(routes externes)	200 (routes internes) 20 (routes externes)
Élément et temps de mise à jour	Table entière chaque 30s	Table entière chaque 30s	**Les changements seulement**	Immédiat à chaque changement	-Préfixe -Immédiat / 30 secondes pour un même voisin et un même préfixe
Unité de Métrique	Saut	Saut	Cout=Rapport bande passante de référence / bande passante du lien	-Bande passante -Délais (Par défaut) -Fiabilité -Charge -MTU	Selon les IGP
Portée maximale de sauts (Scalabilité)	15	15	**Illimité**	225 (100 par défaut)	/
Adresse d'envoi de MAJ	Broadcast sur : 255.255.255.255	Multicast sur : 224.0.0.9	Multicast sur : 225.0.0.5 ou 225.0.0.6	Multicast sur : 224.0.0.100	Unicast vers le voisin
Système d'adressage	Par classe	Sans classe	Supporte-le VLSM/CIDR	Supporte-le VLSM/CIDR	Agrégation de routes
Algorithme de base	Bellman-Ford	Bellman-Ford	SPF (Dijkstra)	DUAL	Aucun
Protocole et port	UDP 520	UDP 520	IP	TCP 88	TCP 179
Convergence	Lent	Lent	Rapide	Rapide	Lent
Suits/pour	Petit réseau	Petit réseau	Réseau large	Réseau large	Réseau très large
Popularité	N'est plus utilisable	N'est plus utilisable	Le plus populaire en tant qu'IGP	Utilisable/moins populaire	Le seul EGP qui existe

FIGURE 4.1 : Comparaison entre les protocoles dynamique [42] [43]

Points forts de l'MPLS : Chaque périphérique MPLS utilise son propre espace d'étiquette local ; étiquettes uniques ou étiquette centralisée l'affectation n'est pas nécessaire, ce qui rend le MPLS extrêmement robuste et évolutif (scalable). Chaque étiquette attribuée par un appareil MPLS est inscrit comme étiquette d'entrée dans sa LFIB, qui est la table de transfert utilisée pour le changement d'étiquette [35]

4.5. Avantages du MPLS L3VPN :

Cette technologie a un certain nombre d'advantages pour les entreprises et les fournisseurs de services(SP).
-Offre une architecture extrêmement évolutive pouvant s'adapter à des milliers de sites clients et les VPNs. -Permet une connectivité universelle pour les sites clients d'entreprise et pour prendre en charge la qualité de service (QoS) en temps réel .
-Permet à une entreprise de simplifier son Routage WAN car les routeurs Customer Edge (CE) n'ont besoin que de faire le peering avec un ou plusieurs routeurs Provider Edge (PE) plutôt qu'avec tous les autres routeurs CE du VPN.
-peut être offert en tant que service géré par un fournisseur de services aux entreprises clientes, ou mis en œuvre par les entreprises elles-mêmes pour fournir des partitions entre unités ou services. [40]

4.6. Conclusion

Dans Le réseau MPLS-VPN , les routeurs CE et les routeurs PE échangent les routes client en utilisant n'importe quel protocole de routage IP approprié car ces routes serons insérées dans des VRF sur les routeurs PE, ce qui garantit l'isolement parfait entre les clients.
Cette topologie fournit des tunnels sécurisés entre les sites filiaux. Par cette implémentation nous montrons qu'il existe des tunnels transparents sur le réseau SP.

Nous évitons également l'implémentation BGP dans l'intégralité du backbone. Cette implémentation permet également d'économiser l'espace de la table de routage sur les routeurs (PE/P). Nous avons utilisé d'abord un IGP qui est l'OSPF pour éviter plus de sessions BGP et pour le rendre plus évolutif. [35]

Chapitre 5

Déploiement Du Réseau WAN

5.1. Introduction

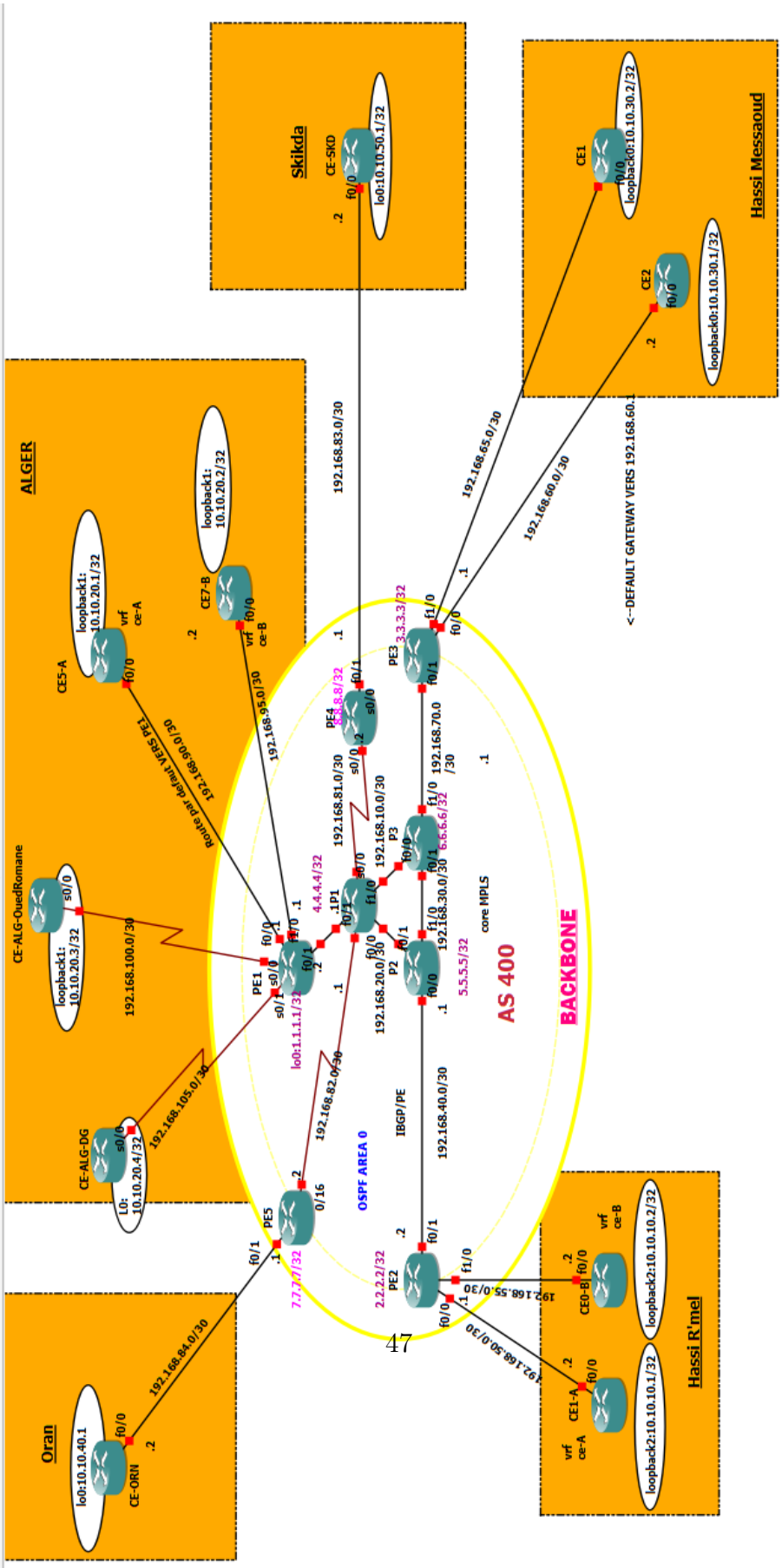
Dans le cadre de simulation du réseau WAN de la Sonatrach, menée sur deux logiciels de simulation Cisco et Huaweii, respectivement ; GNS3 et ENSP, nous considérons 6 P, 10 PE, 20 CE.

Nous mettons en place un "Backbone" composé de 6P et 10PE, reliés par des câbles formant la structure centrale de l'architecture de la Sonatrach. Ce même backbone qui sera lui-même un Système Autonome, n° 400.
Le reste des routeurs (CE), 20 en tout, seront reliés aux extrémités des routeurs (PE) du Backbone.
Ainsi que des loopbacks sur chacun des routeurs externes pour simuler les LANs de chaque région.
En ce qui concerne la configuration, dû à des différences dans le matériel, une séparation des illustrations sera faite en comparaison au fur et à mesure.

5.2. Techniques utilisées

Les routeurs(PE/P) se trouvant dans un cerle (Backbone), représentent des routeurs qui sont hebérgés chez l'opérateur (Service Provider) ;
Les P sont au coeur du réseau Mpls, et les PE sont aux extrémités, car ils représentent un pont entre le Backbone et les clients.
Les routeurs CE appartiennent aux filiales sud est-est ouest de l'entreprise.
L'ospf sera fait entierement sur les routeurs du backbone.
Le Mpls sera coonfiguré sur les PE et les P.
Le IBGP sera configuré.

5.3. Présentation de la maquette réalisée



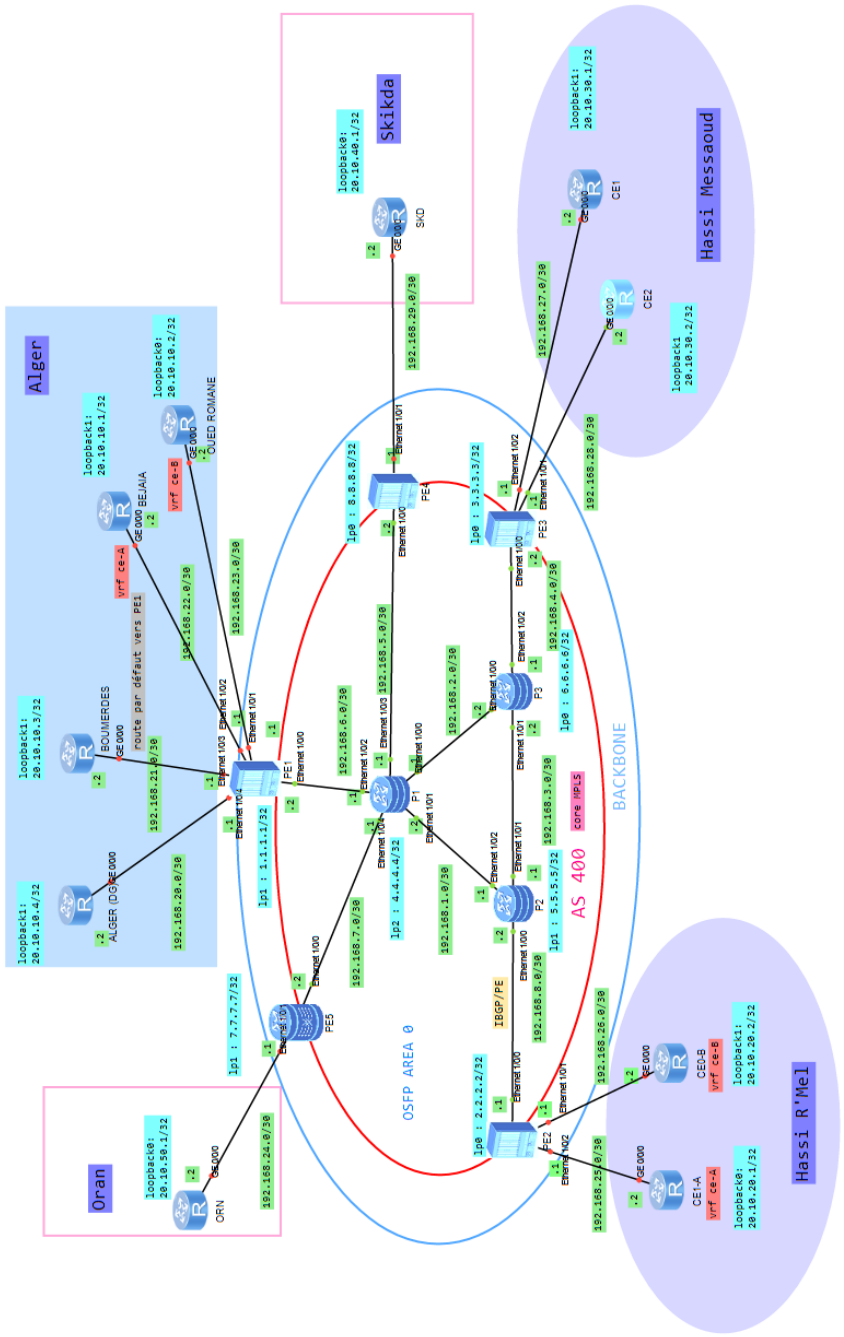


FIGURE 5.2 : Topologie sur eNSP

5.4. Plan d'adressage

Pour ne avoir du gâchis d'adresses, on a opté pour le VLSM dans chaque region. La répartition des adresses IP est fixée dans les deux tableaux ci-dessous :

- Plan d'adressage pour les équipements cisco :

Routeurs	Interfaces	Adresse IP	Adresse loopback
P1	F0/0	192.168.20.1 /30	4.4.4.4/32
	F0/1	192.168.80.1/30	
	F1/0	192.168.10.1/30	
	S0/0	192.168.81.1/30	
	S2/1	192.168.82.1/30	
P2	F0/0	192.168.40.1/30	5.5.5.5/32
	F0/1	192.168.20.2/30	
	F1/0	192.168.30.2/30	
P3	F0/0	192.168.10.2/30	6.6.6.6/32
	F0/1	192.168.20.1/30	
	F1/0	192.168.70.1/30	
PE1	S0/0	192.168.100.1/30	1.1.1.1/32
	S0/1	192.168.105.1/30	
	F0/0	192.168.90.1/30	
	F0/1	192.168.80.2/30	
	F1/0	192.168.95.1/30	
PE2	F0/0	192.168.50.1/30	2.2.2.2/32
	F0/1	192.168.40.2/30	
	F1/0	192.168.55.1/30	
PE3	F0/0	192.168.60.1/30	3.3.3.3/32
	F0/1	192.168.70./30	
	F1/0	192.168.65.1 /30	
PE4	S0/0	192.168.81.2/30	8.8.8.8/32
	F1/0	192.168.83.1/30	
PE5	F0/1	192.168.84.1/30	7.7.7.7/32
	S	192.168.82.2/30	
CE-ORN	F0/0	192.168.84.2/30	10.10.40.1/32
CE1-A Hassi R'mel	F0/0	192.168.50.2/30	10.10.10.1/32
CE0-B Hassi R'mel	F0/0	192.168.55.2/30	10.10.10.2/32
CE-ALG-DG	S0/0	192.168.105.2/30	10.10.20.4/32
CE-ALG-OuedRomane	S0/0	192.168.100.2/30	10.10.20.3/32
CE5-A	F0/0	192.168.90.2/30	10.10.20.1/32
CE7-B	F0/0	192.168.95.2/30	10.10.20.2/32
CE-SKD	F0/0	192.168.83.2/30	10.10.30.2/32
CE1 Hassi Messaoud	F0/0	192.168.65.2/30	10.10.30.2/32
CE2 Hassi Messaoud	F0/0	192.168.60.2/30	10.10.30.1/32

FIGURE 5.3 : Adressage(Gns3)

- Plan d'adressage pour les équipements huwaei :

Routeurs	Interfaces	Adresse IP	Adresse loopback
P1	Ethernet1/0/0	192.168.2.1/30	4.4.4.4/32
	Ethernet1/0/1	192.168.1.2/30	
	Ethernet1/0/2	192.168.6.1/30	
	Ethernet1/0/3	192.168.5.1/30	
	Ethernet1/0/4	192.168.7.1/30	
P2	Ethernet1/0/0	192.168.8.2/30	5.5.5.5/32
	Ethernet1/0/1	192.168.3.1/30	
	Ethernet1/0/2	192.168.1.1/30	
P3	Ethernet1/0/0	192.168.2.2/30	6.6.6.6/32
	Ethernet1/0/1	192.168.3.2/30	
	Ethernet1/0/2	192.168.4.1/30	
PE1	Ethernet1/0/0	192.168.6.2/30	1.1.1.1/32
	Ethernet1/0/1	192.168.23.1/30	
	Ethernet1/0/2	192.168.22.1/30	
	Ethernet1/0/3	192.168.21.1/30	
	Ethernet1/0/4	192.168.20.1/30	
PE2	Ethernet1/0/0	192.168.8.1/30	2.2.2.2/32
	Ethernet1/0/1	192.168.26.1/30	
	Ethernet1/0/2	192.168.25.1/30	
PE3	Ethernet1/0/0	192.168.4.2/30	3.3.3.3/32
	Ethernet1/0/1	192.168.28.1/30	
	Ethernet1/0/2	192.168.27.1/30	
PE4	Ethernet1/0/0	192.168.5.2/30	8.8.8.8/32
	Ethernet1/0/1	192.168.29.1/30	
PE5	GigabitEthernet1/0/0	192.168.7.2/30	7.7.7.7/32
	GigabitEthernet1/0/1	192.168.24.1/30	
CE Oran	GigabitEthernet0/0/0	192.168.24.2/30	20.10.50.1/32
CE Alger (DG)	GigabitEthernet0/0/0	192.168.20.2/30	30.10.10.4/32
CE Boumerdes	GigabitEthernet0/0/0	192.168.21.2/30	20.10.10.3/32
CE Béjaïa	GigabitEthernet0/0/0	192.168.22.2/30	20.10.10.1/32
CE Oued Romane	GigabitEthernet0/0/0	192.168.28.2/30	20.10.10.2/32
CE Skikda	GigabitEthernet0/0/0	192.168.29.2/30	20.10.40.1/32
CE Hassi Messaoud (CE1)	GigabitEthernet1/0/0	192.168.27.2/30	20.10.30.1/32
CE Hassi Messaoud (CE2)	GigabitEthernet1/0/0	192.168.28.2/30	20.10.30.2/32
CE Hassi R'Mel (CE1-A)	GigabitEthernet1/0/0	192.168.25.2/30	20.10.20.1/32
CE Hassi R'Mel (CE0-B)	GigabitEthernet1/0/0	192.168.26.2/30	20.10.20.2/32

FIGURE 5.4 : Adressage(Ensp)

5.5. Configuration des équipements

Les étapes ont été numérotées dans chaque partie pour préciser l'ordre de la configuration.

5.5.1 Partie Gns3 :

1. **Attribution des addresses (CE-ORN) :**
   La loopback[1] adresse est faite pour simuler le LAN d'Oran. Puisqu'elle est virtuelle et ne dépend d'aucune interface physique donc elle est toujours active, c'est pour cela nous n'avons pas besoin de donner la

[1]L'interface de bouclage est virtuelle, elle ne dépend d'aucune interface physique et peut être créée sur les routeurs d'une facon unique ou multiple. [44]

commande "no shutdown" après avoir donné l'adresse IP aux interfaces de bouclage.

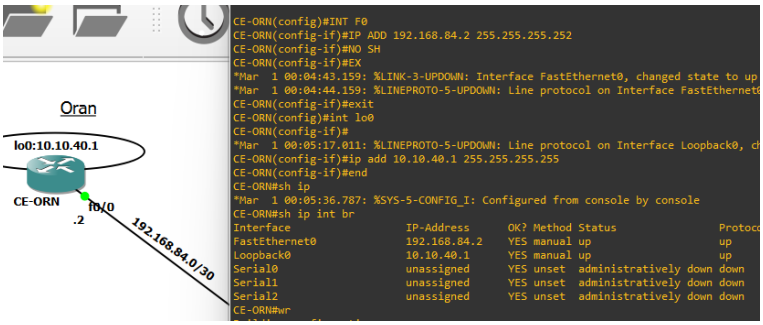


FIGURE 5.5 : CE-ORN.

2. **Attribution d'une route statique :**
   Cette route est attribué dans les 'CE' afin d'envoyer le trafic directement vers les PE, dans ce cas le routeur CE2 qui se situe à Hassi Messaoud envoie tous son traffic vers L'adresse 192.168.60.1.

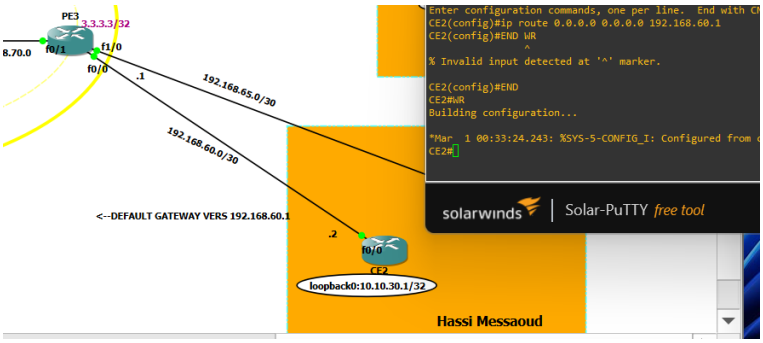


FIGURE 5.6 : CE2 de Hassi Messaoud.

3. **Protocoles de routage utilisé :** OSPF (PE<->P)
   Après avoir configuré toutes les adresses nécessaires sur la topologie, on passe aux routeurs qui se trouvent dans le backbone pour ajouter leurs réseaux directement connectés.
   Les adresses réseaux et les loopback de chaque routeur ont été ajoutés dans l'area 0, pour qu'ils puissent communiquer entre eux.
   Dans ce cas, PE5 est directement connecté avec le P1 ; donc dans le réseau 192.168.82.0 qui sera ajouté, le masque générique est mis a 0.0.0.3 car on avait utilisé un masque /30 et celui de la loopback est mis à 0.0.0.0 car son masque était en /32.

Dans ce cas Ospf est configuré en tant qu'IGP dans le backbone car il est plus rapide par rapport au bgp qui est un protocole assez lent.

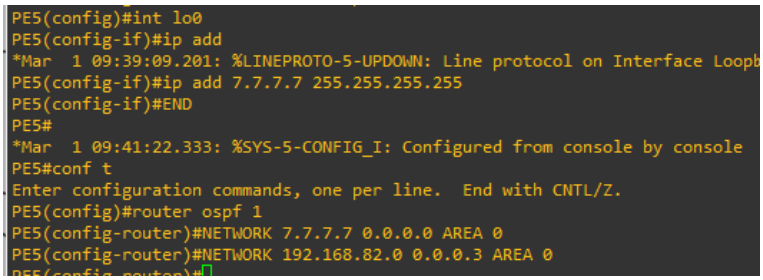


FIGURE 5.7 : Configuration de l'OSPF sur le routeur PE5

4. **Configuration de l'MPLS**
   Le Mpls se fait sur toutes les interfaces des noeuds P et ceux des PE qui sont a l'intérieur du backbone, le reste qui sont reliées avec les CE ne sont pas configurées.

   PE5#**conf t**
   PE5(config)#**ip cef** -> Permet d'activer le CEF [2].
   PE5(config)#**int S0/0** -> Ajout de l'interface s0/0 au Mpls.
   PE5(config-if)#**MPLS IP**
   PE5(config-if)#**MPLS LABEL protocol ldp** -> Permet d'activer le protocole LDP (qui est un protocole standard) au lieu du tag.
   Apres cette configuration, le routeur va construire une adjacence avec les routeurs qui sont en face.

5. **Configuration du BGP**
   Pour mettre en place le BGP, il faudrait d'abord que tous les routeurs puissent communiquer entre eux en utilisant un IGP (OPSF dans notre cas).
   L'ajout des voisins se fait dans chaque PE, chaque routeur doit connaître ses voisins qui sont dans le même IGP.
   Pour faire cela, le IBGP qui sera configuré ici et tous les voisins seront dans le même AS numéroté 400 (La partie interne est considérée comme un système autonome et chaque AS dispose d'un numéro qui lui est attribué par une autorité pour éviter les conflits).
   Cette configuration se fait au niveau des PE seulement, elle permet de

[2]Cisco Express Forwarding : pour une commutation rapide des paquets via les label et non plus via leur @ip.

faire passer les routes entre eux dans le backbone et d'apprendre par la suite les préfixes dans les VRF les uns des autres.

Configuration des voisins de PE5
-L'appairage iBGP à été configuré a l'aide d'adresses de bouclage.

PE5#**conf t**
PE5(config)#**router bgp 400** ->cette commande permet d'activer le bgp avec un AS 400. PE5(config-router)#**neighbor 1.1.1.1 remote-as 400** -> voisinage avec PE1.
PE5(config-router)#**neighbor 8.8.8.8 remote-as 400**
PE5(config-router)#**neighbor 3.3.3.3 remote-as 400**
PE5(config-router)#**neighbor 2.2.2.2 remote-as 400**

PE5(config-router)#**neighbor 2.2.2.2 update-source loopback 0** -> Pour la mise à jour des routes dans la table de routage.
PE5(config-router)#**neighbor 3.3.3.3 update-source loopback 0**
PE5(config-router)#**neighbor 8.8.8.8 update-source loopback 0**
PE5(config-router)#**neighbor 1.1.1.1 update-source loopback 0**

PE5(config-router)#**address-family vpnv4** -> BGP ne transporte que des routes IPv4 alors que Les routes échangées entre les routeurs PE sont des routes VPN, c'est pour cela on a du changer vers cette famille d'adresse VPN4 après la config d'IBGP c'est pour transiter les routes d'une façon unique d'une vrf à une autre, elle supporte les préfixes et les rd.

PE5(config-router-af)#**neighbor 1.1.1.1 activate** ->Active l'annonce des voisins de la famille d'adresses IPv4.
PE5(config-router-af)#**neighbor 8.8.8.8 activate**
PE5(config-router-af)#**neighbor 2.2.2.2 activate**
PE5(config-router-af)#**neighbor 3.3.3.3 activate**

6. **Création des VRF**
On veut que le traffic utilise ces tunnels

Création de la vrf sur PE5 et PE3 : (fil-1) PE5(config)#ip vrf fil-1 PE5(config-vrf)#rd 20 :1 PE5(config-vrf)#route-target both 20 :1 PE5(config-vrf)#end

meme adressage
La vrf fil-1 va etre crée sur les deux routeurs PE5 et PE3
L'ajout de l'interface f0/1 au vrf
PE5(config)#int f0/1
PE5(config-if)#ip vrf forwarding fil-1
% Interface FastEthernet0/1 IP address 192.168.84.1 removed due to enabling VRF fil-1 -> aprés ce message on doit remettre l'adresse ip a son interface.
PE5(config)#int f0/1
PE5(config-if)#ip add 192.168.84.1 255.255.255.252

Configuration d'une route d'échange(exchange route) : Cela nous permet d'échanger des routes entre les ce et pe.

```
PE1(config)#ip route vrf ce-A 10.10.20.1 255.255.255.255 192.168.90.2
PE1(config)#
```

FIGURE 5.8 : exchange static route 1

```
PE2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE2(config)#ip route vrf ce-A 10.10.10.1 255.255.255.255 192.168.50.2
PE2(config)#END
```

FIGURE 5.9 : exchange static route 2

5.5.2 Partie ensp :

Respectivement sur eNSP ;
Tout d'abord, nous configurons l'infrastructure de base, les adresses IP des routeurs P, PE, CE ;
Commandes :
system-view
int Ethernet/GigabitEthernet [Nom de l'interface]
ip address [Adresse IP] [masque sous-réseau]
undo shutdown

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]int GigabitEthernet 0/0/0
[Huawei-GigabitEthernet0/0/0]ip address 192.168.23.2 30
[Huawei-GigabitEthernet0/0/0]undo shutdown
Info: Interface GigabitEthernet0/0/0 is not shutdown.
[Huawei-GigabitEthernet0/0/0]quit
[Huawei]
```

FIGURE 5.10 : Exemple de configuration des adresses IP

Ainsi que les adresses de leurs loopbacks ;
system-view
int loopback [Nom de l'interface]
ip address [Adresse IP loopback] [masque sous-réseau loopback]

```
[Huawei]int loopback0
[Huawei-LoopBack0]ip address 20.10.10.2 32
[Huawei-LoopBack0]quit
[Huawei]
```

FIGURE 5.11 : Exemple de configuration d'une loopback

Puis nous configurons les routes statiques par défaut, de chaque CE vers son PE auquel il est relié ; La création d'une route statique vers un réseau 0.0.0.0 0.0.0.0 est une autre façon de définir la passerelle de dernier recours sur un routeur.
Commandes :
system-view
ip route-static 0.0.0.0 0.0.0.0 [adresse next hop]

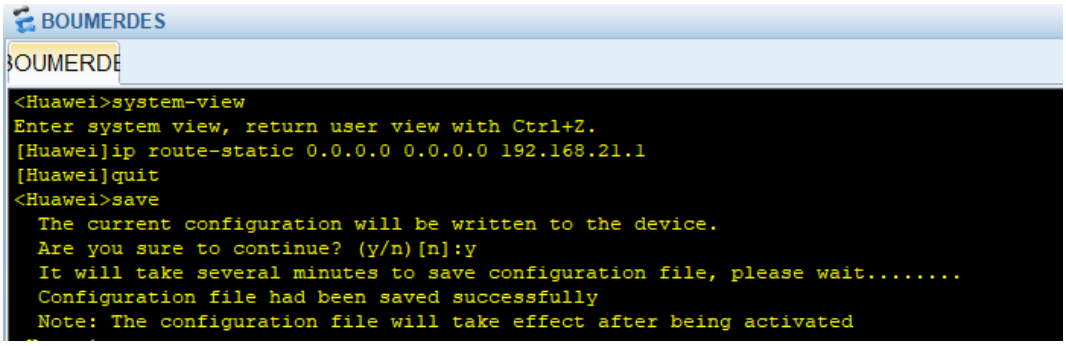


FIGURE 5.12 : Default route CE Boumerdes

- **OSPF :**
  Le premier objectif du déploiement d'un réseau central est de faire en sorte que les boucles communiquent, c'est la principale raison pour laquelle nous avons besoin d'un IGP. Ici dans notre cas, nous utiliserons OSPF.
  Commandes :
  ospf [process id]
  area [area id]
  network [adresse ip réseau] [masque sous-réseau]
  Configuration OSPF :

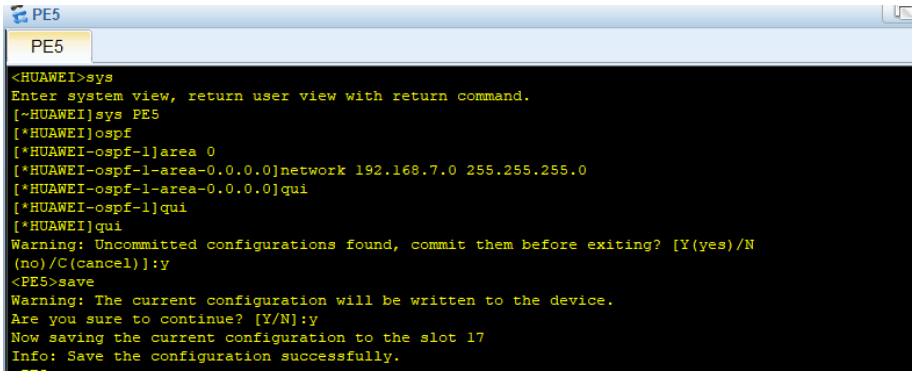


FIGURE 5.13 : Exemple de configuration ospf sur le routeur PE5

- **Mpls :**
  Une fois que nous avons fait fonctionner l'IGP, nous pouvons maintenant exécuter Mpls, dans notre cas, nous sommes sur LDP. Après son execution, nous aurons des tunnels actifs entre les différents routeurs. Pour arriver à l'adresse de bouclage d'un des routeurs faisant partie

d'un tunnel, nous allons savoir quelle étiquette pousser, et encapsuler le paquet IP à l'intérieur.

Commandes :
mpls lsr-id [id]
mpls
quit
mpls
lsp-trigger all
mpls
mpls ldp
quit
ospf [id]
mpls ldp auto-config
quit

- Configuration de l'Mpls :

```
[*P1]mpls lsr-id 4.4.4.4
[*P1]mpls
[*P1-mpls]quit
[*P1]mpls
[*P1-mpls]mpls ldp
[*P1-mpls-ldp]quit
[*P1]ospf 1
[*P1-ospf-1]mpls ldp auto-config
[*P1-ospf-1]quit
```

FIGURE 5.14 : Exemple de configuration Mpls sur le routeur P1

- **BGP :**
Maintenant que Mpls fonctionne et que avons créé des tunnels pour le trafic, nous voulons que les data-centers puissent se parler, c'est là que BGP entre en jeu.

Ce que nous allons faire, c'est exécuter BGP, en faisant passer des préfixes à partir de différents centres de données. Désormais, tous les préfixes sont partagés.

Commandes :
bgp [Numéro AS]

router-id [Identifiant du routeur]
peer [Adresse de l'interface / Adresse Loopback - du routeur voisin] as-number [Numéro AS]
import-route direct
commit

PE1

```
[~PE1]bgp 400
[~PE1-bgp]router-id 1.1.1.1
[*PE1-bgp]peer 192.168.8.1 as-number 400
[*PE1-bgp]peer 192.168.4.2 as-number 400
[*PE1-bgp]peer 192.168.5.2 as-number 400
[*PE1-bgp]peer 192.168.7.2 as-number 400
[*PE1-bgp]
[*PE1-bgp]import-route direct
[*PE1-bgp]commit
[~PE1-bgp]
[~PE1-bgp]quit
[~PE1]
```

FIGURE 5.15 : Configuration de iBGP sur PE1

PE2

```
<PE2>
<PE2>sys
Enter system view, return user view with return command.
[~PE2]bgp 400
[*PE2-bgp]router-id 2.2.2.2
[*PE2-bgp]peer 192.168.6.2 as-number 400
[*PE2-bgp]peer 192.168.5.2 as-number 400
[*PE2-bgp]peer 192.168.7.2 as-number 400
[*PE2-bgp]peer 192.168.4.2 as-number 400
[*PE2-bgp]commit
[~PE2-bgp]
```

FIGURE 5.16 : Configuration de iBGP sur PE2

5.6. Conclusion

Le IGP (OSPF) nous a permis d'exécuter BGP tout comme il nous a permis d'exécuter Mpls.
Sans Mpls, nous avons un réseau central simple où nous ferons du routage IP, sans tunneling et autres protocoles.
Sans BGP, nous ne pouvons pas envoyer de trafic significatif.
Mpls et BGP se complètent.

Chapitre 6

Verification Et Test De Validation

6.1. Introduction

Dans le présent chapitre nous présenterons les résultats du déploiement du réseau WAN et démarches qui ont contribué à la réalisation de notre maquette.

6.2. Test et verification des résultats à travers les commandes

- Mpls :
  PE5#sh mpls ldp neighbor
  Cette commande nous permet de vérifier que le mpls fonctionne.

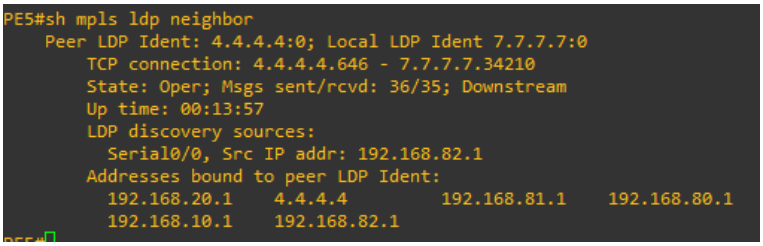


FIGURE 6.1 : Test de validation de l'mpls sur le PE5

PE5#sh mpls ldp discovery
Local LDP Identifier : 7.7.7.7 :0 Discovery Sources : Interfaces : Serial0/0 (ldp) : xmit/recv LDP Id : 4.4.4.4 :0

-> Comme résultat le PE5 a découvert comme voisin le 4.4.4.4 qui est au niveau du P1.

PE5#sh mpls ldp bindings

On obtient la table qui se trouve ci-dessous ; permet de montrer que chaque paquet reçoit une étiquette et est ensuite transmis en fonction de la valeur de cette étiquette. Les informations d'échange d'étiquettes sont construites sur la base de liaisons locales et distantes.

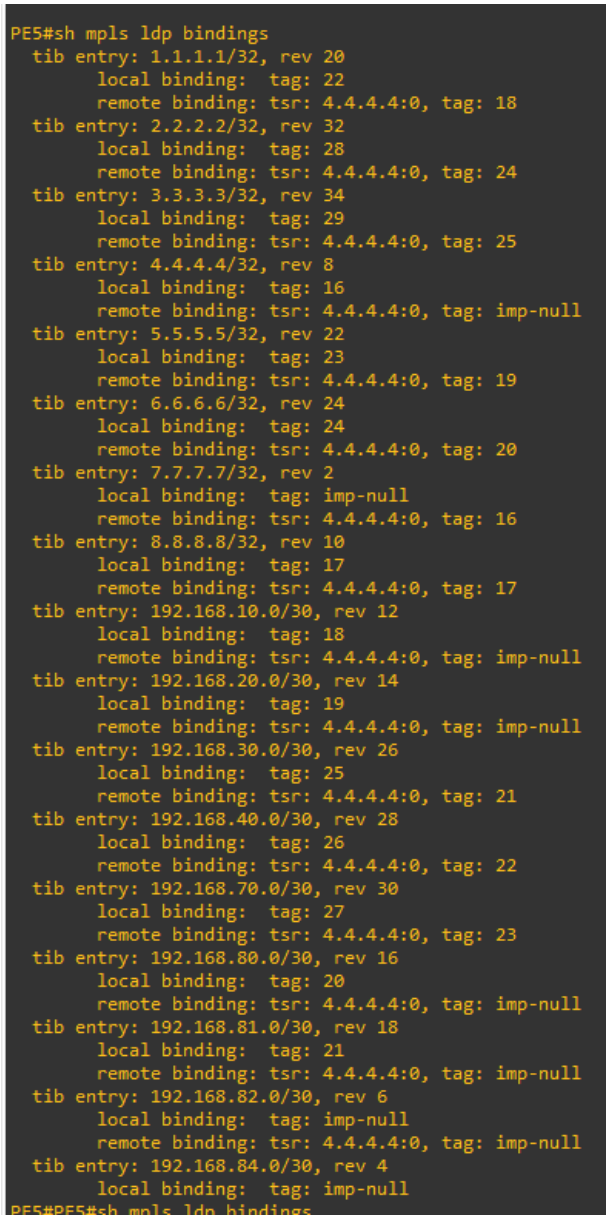


FIGURE 6.2 : Table de MPLS LDP bindings

- BGP :
  La colonne UP/Down : fait référence a la durée de communication entre les voisins PE.

```
PE4#SH BGP vpnv4 unicast all summ
BGP router identifier 8.8.8.8, local AS number 400
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1         4   400      57      54        1    0    0 00:46:05        0
2.2.2.2         4   400      56      54        1    0    0 00:45:54        0
3.3.3.3         4   400      44      44        1    0    0 00:35:36        0
7.7.7.7         4   400      54      54        1    0    0 00:45:37        0
PE4#
```

FIGURE 6.3 : Table de voisins BGP

Aprés la config de la route exchange entre ce et pe :

```
PE2#ping VRF ce-A 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/28/64 ms
PE2#
```

FIGURE 6.4 : résultat de ping

- VRF : Le ping ne marche pas car cette interface est ajoutéà la vrf donc il faut déclarer explicitement apres le ping 'vrf' + le nom du vrf.

```
PE1#ping vrf ce-A 192.168.90.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.90.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/53/132 ms
PE1#
```

FIGURE 6.5 : vrf1

Aprés déclaration :

Echange établie entre les filiales d'Alger de Hassi R'mel (traffic passé par le tunnel de vrf)

```
CE1-A#ping 10.10.20.1 source loopback0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/344/844 ms
CE1-A#
```

FIGURE 6.6 : résultat de ping

```
CE5-A#ping 10.10.10.1 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/120/136 ms
CE5-A#
```

FIGURE 6.7 : résultat de ping

- Protocole OSPF :
  Vérifions que les relations de voisinage sont bonnes dans le backbone :

```
P1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/11] via 192.168.80.2, 00:04:03, FastEthernet0/1
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/21] via 192.168.20.2, 00:04:03, FastEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/3] via 192.168.10.2, 00:04:03, FastEthernet1/0
     192.168.30.0/30 is subnetted, 1 subnets
O       192.168.30.0 [110/11] via 192.168.20.2, 00:04:03, FastEthernet0/0
                     [110/11] via 192.168.10.2, 00:04:03, FastEthernet1/0
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/11] via 192.168.20.2, 00:04:04, FastEthernet0/0
     192.168.10.0/30 is subnetted, 1 subnets
C       192.168.10.0 is directly connected, FastEthernet1/0
     192.168.40.0/30 is subnetted, 1 subnets
O       192.168.40.0 [110/20] via 192.168.20.2, 00:04:06, FastEthernet0/0
     6.0.0.0/32 is subnetted, 1 subnets
O       6.6.6.6 [110/2] via 192.168.10.2, 00:04:06, FastEthernet1/0
     7.0.0.0/32 is subnetted, 1 subnets
O       7.7.7.7 [110/65] via 192.168.82.2, 00:04:06, Serial2/1
     8.0.0.0/32 is subnetted, 1 subnets
O       8.8.8.8 [110/65] via 192.168.81.2, 00:04:06, Serial0/0
     192.168.81.0/30 is subnetted, 1 subnets
C       192.168.81.0 is directly connected, Serial0/0
     192.168.80.0/30 is subnetted, 1 subnets
C       192.168.80.0 is directly connected, FastEthernet0/1
     192.168.20.0/30 is subnetted, 1 subnets
C       192.168.20.0 is directly connected, FastEthernet0/0
     192.168.82.0/30 is subnetted, 1 subnets
C       192.168.82.0 is directly connected, Serial2/1
     192.168.70.0/30 is subnetted, 1 subnets
O       192.168.70.0 [110/2] via 192.168.10.2, 00:04:07, FastEthernet1/0
P1#
```

FIGURE 6.8 : Test de validation du voisinage ospf

Chapitre 7

Conclusion Générale Et Perspectives

Parvenu au terme de la réalisation de notre maquette, et suite à l'étude du réseau de la Sonatrach, et des bugs techniques qui peuvent ressurgir sur le terrain à partir des expériences précédentes. Il était question pour nous de pouvoir proposer des recommandations d'amélioration ou de changement de certaines charactéristiques des réseaux.

À l'origine, les solutions d'optimisation WAN permettaient de :
-Réduire les besoins en bande passante et les coûts liés au WAN en optimisant ses conditions d'utilisation ;
-Accélérer le transfert de données dans le but d'améliorer la productivité et l'expérience utilisateur ;

Les principales clés d'optimisation d'un WAN sont ;

La visibilité (monitorer le WAN) : Cette étape consiste à passer à la

loupe les applications installées sur le WAN, mais aussi à observer les volumes de données, les temps de latence ou la perte de paquets. Il ne peut être que bénéfique d'avoir la possibilité d'observer le comportement du WAN en temps réel ou à travers des rapports. Cela permet en effet d'effectuer des analyses précises autour d'un éventuel problème de performance.

La QoS (maîtrise des applications) : Permet d'optimiser un WAN grâce au contrôle et à la priorisation des applications. Les caractéristiques de chacune des applications installées sur le réseau (débit, temps de latence, lenteur, temps d'exécution) sont prises en compte, et des paramètres spécifiques sont donc mis en place pour prioriser les flux métier.

Le réseau hybride : (sécurisation du WAN et maitrise des coûts) : Un réseau hybride a la particularité d'être composé de plusieurs liens de différents types (Mpls, Internet...). On définit alors des liens spécifiques pour chacune des applications en fonction de leur criticité ; les liens Internet ont un débit plus élevé et sont moins coûteux que les liens MPLS, ils sont plus adaptés à une application qui exige beaucoup de bande passante pour fonctionner de manière optimale. Ils conviennent également à une application moins sensible au délai et à la perte de paquets.
Dans le cas où un des liens du réseau ne fonctionne pas, les flux sont redirigés automatiquement vers un autre lien.

Ainsi, le contrôle et la mesure des flux d'un réseau permettent de faire des économies car la bande passante est optimisée de manière objective. [45]
Le réseau hybride permet aussi une meilleure sécurité du réseau, et de la flexibilité, étant donné la diversité matérielle et logicielle des réseaux WAN.

En ce qui est concerne la QoS ;

SD-WAN : Est la Nième génération de réseaux informatiques et télécom étendus dans le monde après ATM, MPLS, etc. Son objectif est de dépasser les contraintes et les coûts du MPLS en communiquant de façon optimisée sur le réseau Internet grâce à un mécanisme d'identification et de priorisation intelligente et dynamique des flux.

Les points positifs majeurs qu'il peut rassembler pour la Sonatrach ;

– **Baisse des coûts**

Optimise les coûts de connectivité en diminuant les dépenses d'exploitation courantes. Il rompt la dépendance des entreprises vis-à-vis de lignes MPLS lentes et coûteuses, et s'oriente plutôt vers des services proposant une large bande passante tels que la fibre, le câble, l'ADSL ou encore la 4G/5G. Les réductions des coûts réseaux peuvent aller de 40% à 65% par site.

– **La fiabilité du réseau**

Les réseaux WAN traditionnels, ont en généralement une seule liaison entrante pour chaque site (pour une raison de rationalisation des coûts). Inversement, le SD-WAN permet d'activer plusieurs liens provenant de différents FAI et de différentes technologies. Ce qui naturellement, permet d'assurer aussi une continuité de service dans le cas où un des liens tomberaient, en basculant directement vers d'autres liens, il assure donc la redondance, et offre donc aux utilisateurs un accès permanent au réseau.

– **Performance**

Grâce à l'association de la gestion centralisée, différentes technologies de connexion et plusieurs FAI, le SD-WAN vient améliorer les performances globales du réseau sur chaque site de l'entreprise. Son contrôleur perçoit l'ensemble des liens qui composent le réseau, reçoit en même temps les informations des applications et est ainsi capable de diriger le trafic vers le chemin le plus performant et le moins coûteux. Ce qui garantit un débit de données conforme aux exigences de chaque application et tient donc toutes ses promesses en termes de bande passante et d'optimisation dans l'utilisation des ressources.

– **Agilité**

Grâce à la gestion par logiciel qu'offre le SD-WAN, on peut facilement déployer le réseau vers un nouvel établissement ou un nouveau site (il faut moins de 30 minutes pour connecter et configurer un site distant). On peut configurer rapidement des réseaux fiables, en utilisant les FAI les plus adaptés à chaque site, mais aussi sécurisés, en déployant des stratégies d'accès globales et facilement applicables (plutôt que de gérer manuellement chaque appareil WAN).

– **Sécurité**

Le SD-WAN permet la gesion de plus de 1500 sites distants via une seule interface centralisée et de propager partout des niveaux de sécurité personnalisés grâce aux fonctionnalités intégrées de firewalls avancés. Ce qui permet aux entreprises d'améliorer la performance et la flexibilité de leur réseau sans

en compromettre la sécurité. Le réseau est donc non seulement protégé vis à vis des connexions extérieures avec Internet, mais également en interne avec un chiffrement des données entre chaque site.[46]

Route maps :

Les route maps, sont comme des Access List plus sophistiquées, elles utilisent une logique algorithmique de conditions If/Then/Else. Les Access Lists/Prefix Lists peuvent seulement faire correspondre des adresses ip/routes dans le cas du routage. Alors que les route-maps, peuvent faire correspondre, par exemple dans le cas d'EIGRP, des routes internes et externes, le type du routage(interne/externe), Metric Type, Next Hop, et même les attributs BGP.. Elles permettent donc une meilleure flexibilité en termes de filtrage. Chaque entrée de route-map a des paramètres correspondants sous-jacents, configurés avec la commande "match". Elle permet d'autoriser ou de refuser l'accès basée sur ces critères, et comme les "prefix lists", elle sont traitées manière séquentielle. Les route-maps permettent une meilleure sécurité du réseau WAN, en offrant un systme de filtrage plus évolué qu'avant.

Firewall externes, vers les CE :

Le rôle du Firewall est de servir de barrière afin de protéger le réseau des dangers externes : virus, attaques par « cheval de Troie », divulgation non autorisée d'informations sensibles, suppression non autorisée de fichiers importants, etc.

Nous différencions deux grandes catégories de pare-feu en fonction du filtrage qu'ils effectuent : filtrage par paquets IP et filtrage applicatif.[47]
Un pare-feu périphérique/périmétrique est un système de sécurité réseau,

matériel ou logiciel, qui contrôle le trafic entrant et sortant en fonction d'un ensemble de règles de sécurité prédéterminées afin de protéger les data-center. Il fournit une défense de périmètre avec état pour les flux de trafic nord-sud entre les réseaux virtuels et physiques. Il est utilisé sur le routeur logique et fournit une traduction d'adresse réseau (NAT) ainsi que des fonctionnalités IPsec et VPN SSL de site à site.
Le pare-feu Edge peut être géré avec les mêmes outils de gestion que pour le pare-feu distribué. Permet la gestion multiple dans lequel, par exemple, des équipes individuelles au sein d'une organisation peuvent configurer leurs propres pare-feu sans avoir besoin d'accéder à l'ensemble du réseau.[48]

Nous tenons à préciser, qu'il ne faut pas oublier qu'en termes de design réseau, il est souvent question de compromis (trade-offs), on peut améliorer une partie du réseau et en impacter une autre, c'est pour cette raison qu'il faut rester très vigilant dans le paramétrage de ces options : Le réseau doit être conçu pour les applications et non le contraire.

Pour finir, nous pensons que cette mise en œuvre que nous proposons est d'une importance capitale pour le bon fonctionnement du réseau WAN de la Sonatrach. Cette architecture pourra faire l'objet d'améliorations et de modification en fonction des besoins futur de la structure.

Bibliographie

[1] Rapport donné par la direction de sonatrach.

[2] Elmoudjahid Economie. Réalisations de sonatrach en 2021 : Bon bilan malgré la crise. https://www.elmoudjahid.dz/fr/economie/realisations-de-sonatrach-en-2021-bon-bilan-malgre-la-crise-177853#:~:text=S\%27agissant\%20de\%20la\%20production,\%2C1\%20millions\%20de\%20m3. [18 :55, 31-01-2022].

[3] Sonatrach. https://fr.wikipedia.org/wiki/Sonatrach. maj le 1 septembre 2022 à 17 :22.

[4] Gaz naturel liquéfié. https://fr.wikipedia.org/wiki/Gaz_naturel_liqu\%C3\%A9fi\%C3\%A9.

[5] Rapport annuel de la sonatrach. https://sonatrach.com/wp-content/uploads/2021/12/Rapport-Annuel-2020-1.pdf, 2020.

[6] Energy Industry Review. Eni signe de nouveaux accords avec sonatrach lors du sommet algérien sur l'énergie future. https://energyindustryreview.com/oil-gas/eni-signs-new-agreements-with-sonatrach-at-the-algeria-future-energy-summit/ 2018.

[7] Lélio Motta. Simulez des architectures réseaux avec gns3. https://openclassrooms.com/fr/courses/2581701-simulez-des-architectures-reseaux-avec-gns3/4823141-emuler-simuler-virtualiser-de-quoi-parle-t-on, 2020. Mis à jour le 15/12/2020.

[8] Quelle est la différence entre la simulation continue et la simulation discrète ? https://mulloverthing.com/what-is-the-difference-between-continuous-simulation-and-discrete-simulation 2019.

[9] Qu'est-ce que la simulation de réseau : types et ses avantages. https://fr.jf-parede.pt/what-is-network-simulation.

[10] RedNectar Chris Welsh. *Gns3 Network Simulation Guide*. Packt, 2013.

[11] Gns3 windows install. https://docs.gns3.com/docs/getting-started/installation/windowshttps://docs.gns3.com/docs/getting-started/installation/windows.

[12] François Goffinet. Installer et configurer gns3. https://cisco.goffinet.org/ccna/cisco-ios-cli/installer-et-configurer-gns3/#11-pr\%C3\%A9sentation-de-gns3.

[13] thunder link. Un guide simple sur huawei ensp. https://www.thunder-link.com/blog/a-straightforward-guide-to-huawei-ensp/.

[14] Chapter 2. ios images and configuration files. https://www.oreilly.com/library/view/cisco-ios-in/0596008694/ch02.html#:~:text=IOS\%20image\%20files\%20contain\%20the,or\%20router\%2Dspecific\%20features.

[15] Routeur backbone convergent ne9000. https://e.huawei.com/fr/products/enterprise-networking/routers/ne/ne9000.

[16] https://e.huawei.com/fr/products/enterprise-networking/routers/ne/ne40e.

[17] https://www.4gltemall.com/huawei-ar3260-s-enterprise-router.html.

[18] Cisco 3700 series multiservice access routers. https://www.ict-hardware.com/product/cisco-3745/.

[19] c2690. https://www.cisco.com/c/en/us/td/docs/ios/12_4/12_4x/release/notes/rn2600xe.html, 2008.

[20] Cisco 1700 series router hardware view. https://www.cisco.com/web/ANZ/cpp/refguide/hview/router/1700.html.

[21] Cisco 1720 router. https://productz.com/fr/cisco-1720-router/p/pxbdX.

[22] Lazaro (LAZ) Diaz. *CCNA Routing and Switching 200-125 Certification Guide : The Ultimate Solution for Passing the CCNA Certification and*

Boosting Your Networking Career. Packt Publishing, Limited, Birmingham, 2018.

[23] Muhammad Kashif Hanif, Ramzan Talib, Nafees Ayub, Muhammad Umer Sarwar, and Sami Ullah. Ospf vs eigrp : A comparative analysis of cpu utilization using opnet. *International Journal of Advanced Computer Science and Applications*, 2017.

[24] Silviu Angelescu. *CCNA Certification All In One For Dummies*. 2010.

[25] Forensics. Protocole de routage ospf. `https://malware.news/t/routing-protocols/29329`, 2019. Routing Protocols.

[26] Routage dynamique : Protocoles de routage dynamique. `https://formip.com/protocoles-de-routage-dynamique/`. Publié le 6 juillet 2018.

[27] KUMAR JASWINDER, SAMIKSHA, BHAGAT SUSIL, and KAUR KARANJIT. Route redistribution between eigrp and ospf routing protocol in computer network using gns3 sofware. *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)*, 5, 2015.

[28] Bgp (border gateway protocol). `https://ipcisco.com/lesson/bgp-border-gateway-protocol/`.

[29] Harris Andrea. Le protocole de l'internet - tutoriel et configuration ebgp et ibgp. `https://www.networkstraining.com/cisco-bgp-configuration-tutorial/`.

[30] Bgp autonomous system number. `https://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/autonomous_system_number.shtml`, 2018.

[31] Ayush Pandya. Quick reference guide – multiprotocol label switching. `https://theunprecedentedcult.in/articles/technology/multiprotocol-label-switching/`, 2020.

[32] Cisco officiel web site : What is multi-protocol label switching (mpls) ? `https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html#anc4`, 2016.

[33] `https://talent.huaweiuniversity.com/portal/courses/HuaweiX+EBGTD9033/about`.

[34] Ravi Kumar Cv, C Dhanumjayulu, Annasamy Bagubali, and Kala Praveen Bagadi. Architecture for mpls l3 vpn deployment in service provider network. *Journal of Telecommunications System Management*, April 2017.

[35] Jeff Apcar Ivan Pepelnjak, Jim Guichard. Mpls and vpn architectures, volume ii. *Cisco Press*, June 2003.

[36] Amit Bhardwaj. What is vrf? vrf complete guide 2022. https://ipwithease.com/vrf-basics/.

[37] Virtual routing and forwarding (vrf). https://avinetworks.com/glossary/virtual-routing-and-forwarding-vrf/.

[38] Introduction to virtual routing and forwarding (vrfs). https://technologyordie.com/introduction-to-virtual-routing-and-forwarding-vrf.

[39] https://www.rogerperkin.co.uk/ccie/mpls/route-distinguisher-vs-route-target/.

[40] Pooja Ahlawat Akshay. Implementation of mpls l3vpn using gns3. *International Journal of Scientific Engineering and Research (IJSER)*, April 2014.

[41] Pankaj Rakheja, Prabhjot Kaur, Anjali Gupta, and Aditi Sharma. Performance analysis of rip, ospf, igrp and eigrp routing protocols in a network. *International Journal of Computer Applications*, June 2012.

[42] Elyes Ben Salah. Réseau ip routage comparaison entre les différents protocoles de routage rip v1 rip v2 ospf eigrp.

[43] Vince. Les protocoles de routage. https://zestedesavoir.com/tutoriels/2789/les-reseaux-de-zero/dans-les-basses-couches-du-modele-osi/les-protocoles-de-routage/, 2022.

[44] Loopback interface in gns3. https://o7services.com/2018/09/07/loopback-interface-in-gns3-how-to-create/.

[45] Optimiser votre réseau wan pour garantir la performance de vos applications : quels enjeux? https://www.e-qual.fr/2016/06/03/optimisation-wan-garantir-la-performance-de-vos-applications/#:~:text=La\%20compression\%2C\%20l'acc\%C3\%A9l\%C3\%A9ration\%20et,donn\%C3\%A9es\%20sans\%20perte\%20d'information.

[46] Anthony LEMARCHANT. Réseau sd-wan : définition et avantages pour les entreprises. https://www.a2com.fr/blog/reseau-sd-wan-definition-et-avantages-pour-les-entreprises/, 2019.

[47] Qu'est-ce qu'un firewall ? https://www.hosteur.com/ressources/articles/firewall#:~:text=Le\%20r\%C3\%B4le\%20du\%20Firewall\%20est,autoris\%C3\%A9e\%20de\%20fichiers\%20importants\%2C\%20etc, 2019.

[48] Sarthak Varshney. https ://tutorialslink.com/articles/what-is-edge-firewall-and-nsx-logical-firewall/1478. https://tutorialslink.com/Articles/What-is-Edge-Firewall-and-NSX-Logical-Firewall/1478, 2020.