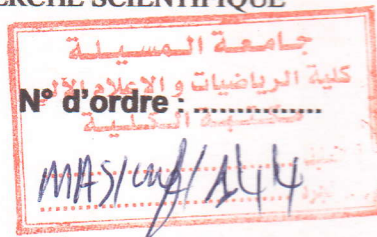




UNIVERSITE DE M'SILA



FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

**Département de Sciences et Technologies de l'information et de la
Communication**

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Technologies de l'information et de la Communication

Par : LAKHDARI Saâd

SUJET

Conception et réalisation d'un architecteur

MPLS VPN

Soutenu publiquement le: 14 /06/2015

Devant le jury composé de:

-
- Dr. BENOUIS Mohamed
-

Université de M'sila	Président
Université de M'sila	Rapporteur
Université de M'sila	Examineur

Promotion : 2014 /2015

TABLE DE MATIERES

INTRODUCTION GENERALE

CHAPITRE I : INTRODUCTION AUX RESEAUX NGN

I.1 Introduction.....	05
I.2 Definition.....	05
I.3 Motivations D'apparition De NGN.....	05
I.4 Architecture Du Reseau NGN.....	06
I.4.1 Couche Transport.....	06
I.4.1.1 La Couche Acces.....	06
I.4.1.2 La Couche Transit	06
I.4.2 Couche Contrôle.....	07
I.4.3 Couche Service.....	07
I.5 Principaux Equipements Du Reseaux NGN	08
I.5.1 Softswitch	08
I.5.2 Media Gateway.....	08
I.6 Avantages De Reseau NGN.....	09
I.7 Le Projet RMS D'algerie Telecom	09
I.8 Conclusion.....	11

CHAPITRE II GENERALITE SUR VPN

II.1. Introduction	13
II.2. Principe De Fonctionnement	13
II.2.1 Principe General	13
II.2.2 Fonctionnalités Des Vpn	14
II.2.2.1 Le VPN D'accès.....	14
II.2.2.2 L'intranet VPN	15
II.2.2.3 L'extranet VPN.....	16
II.3 Bilan Des Caracteristiques Fondamentales D'un VPN.....	17
II.4 Protocoles Utilises Pour Realiser Une Connexion VPN.....	17
II.4.1 Les Protocoles De Niveau 2.....	17
II.4.2 Les Protocoles De Niveau 3.....	18

II.5 Conclusion.....	18
CHAPITRE III : MPLS MULTI PROTOCOL LABEL SWITCHING	
III.1 Introduction	20
III.2 Technologie MPLS.....	20
III.2.1 Label Switch Router.....	20
III.2.2 ELSR.....	21
III.2.3 Label Switched Path (LSP).....	21
III.2.4 Classe D'équivalence D'acheminement (FEC).....	21
III.2.5 Label Distribution Protocol (LDP)	21
III.2.6 Upstream And Downstream.....	21
III.3. Principes MPLS.....	21
III.3.1 Etiquette Label.....	23
III.3.2. Architecture Du Protocole MPLS.....	25
III.3.2.1 Plan De Contrôle.....	25
III.3.2.1.A La Methode « Implicit Routing ».....	26
III.3.2.1.B La Methode « Explicit Routing ».....	27
III.3.2.1.C Protocole De Distribution Des Labels.....	27
III.3.2.1.D Différents Modes De Distribution De Labels.....	29
III.3.2.1.E Le Protocole De Routage OSPF.....	30
III.3.2.2 Plan De Données.....	32
III.3.2.2.A Table LIB.....	32
III.3.2.2.B Table LFIB.....	32
III.3.2.2.C FIB (Forwarding Information Base).....	32
III.3.2.2.D Transmission Des Données.....	32
III.4 Applications MPLS.....	33
III.4.1. Quality Of Service.....	33
III.4.2. L'application MPLS-TE.....	34
III.4.3. VPN/MPLS.....	34
CHAPITRE IV : MPLS VPN (PREVATE VERTUEL NETWORK)	
IV.1 Introduction	36
IV.2 MPLS VPN	36
IV.2.1 Routeurs P, PE et CE	36

IV.2.2 Routeurs Virtuels VRF	37
IV.2.3 Multi-Protocol Border Gateway Protocol (MP-BGP).....	38
IV.2.3.1 Notion De RD (Route Distinguisher)	38
IV.2.3.2 Notion De RT (Route Target)	39
IV.2.3.3 Impact Des Topologies Complexes De VPN sur VRF	40
IV.2.5 Propagation D'etiquette VPN	41
IV.3 Complementation De Mpls Par IPSEC	42
IV.3.1 Endroit Des Points D'arret D'IPSEC	43
IV.3.2 CE-CE IPSEC	43
IV.3.3 PE-PE IPSEC	45
IV.3.4 Acces Distant IPSEC Dans un MPLS VPN	48
IV.4 Conclusion	49
APPLICATION	
V.1 Introduction.....	51
V.2 Application sur la maquette RMS	51
V.2.1 Réalisation de la maquette	51
V.2.2 Description de la maquette	51
V.2.3 Plan d'adressage.....	51
V.2.4 logiciel utilisé pour la réalisation	52
V.2.4.1 GNS3	52
V.2.4.2 VMware Workstation	53
V.2.4.3 Wireshark	53
V.3 Configuration de la maquette.....	53
V.3.1 Activation du routage classique.....	53
V.3.2 Activation du MPLS	56
V.3.2.1 Configurer MPLS LDP dans le réseau du fournisseur de services.....	56
V.3.2.2 Analyse de paquette MPLS	58

V.3.3 Configuration VRF dans les PE Routeurs.....	61
V.3.3.1 Configurer VRF dans le fournisseur de bord (PE) Routeurs.....	61
V.3.3.2 Configurer BGP VPNv4 peering entre PE Alger et PE Oran.....	62
V.3.3.3 Configurez Peering entre les routeurs PE aux routeurs clients.....	63
V.3.3.4 Vérification de la connectivité.....	67
CONCLUSION	15
ABREVIATIONS	16
BIBLIOGRAPHIE	20
VIDEO TRAINING	22
RÉSUMÉ	23
Figure III.1 : L'Internet VPN	24
Figure III.2 : Principes de la commutation de label	25
Figure III.3 : MPLS au niveau des couches	26
Figure III.4 : Détails d'un label MPLS	27
Figure III.5 : Encapsulation pour ATM, Frame Relay, etc.	28
Figure III.6 : Architecture logique MPLS	29
Figure III.7 : Routage implicite des labels	30
Figure III.8 : Routage explicite des labels	31
Figure III.9 : Principe de fonctionnement d'un LDP	32
Figure III.10 : Etablissement d'une connexion LDP	33
Figure III.11 : Fonctionnement de mode « Downstream Unsolicited »	34
Figure III.12 : Fonctionnement du mode « Downstream on demand »	35
Figure III.13 : Organisation d'OSPF selon les zones	36
Figure IV.1 : Emplacement des routeurs dans une architecture MPLS	37
Figure IV.2 : les routeurs virtuels	38
Figure IV.3 : adresse VPNv4	39
Figure IV.4 : propagation de la route de customer	40
Figure IV.5 : impact des topologies complexes de VPN sur VRF	41
Figure IV.6 : transmission des paquets VPN à travers le backbone MPLS VPN	42
Figure IV.7 : propagation d'étiquettes VPN	43
Figure IV.8 : tunnel IPSec entre deux routeurs CE	44
Figure IV.9 : tunnel IPSec entre deux routeurs PE	45
Figure IV.10 : encapsulation IPSec entre deux routeurs PE	46

INTRODUCTION GENERALE

Un réseau public, comme le réseau téléphonique ou Internet, est un ensemble de points entre lesquels ont lieu des échanges plus ou moins libre d'informations. Les personnes qui ont accès à ce réseau sont susceptibles d'avoir un intérêt commun et utilisent le réseau pour communiquer les uns avec les autres.

Un réseau privé est composé d'ordinateurs appartenant à une même et unique organisation qui partage ses informations en interne avec la certitude que seuls leurs employés utiliseront le réseau et que les informations en transit sur ce dernier ne pourront être atteintes que par des membres du même groupe.

La ligne de séparation entre un réseau privé et un réseau public se trouve au niveau de la passerelle, où la compagnie place généralement un pare-feu pour éviter que des intrus d'un réseau public n'accèdent à leur réseau privé ou l'inverse. Cependant, comme de plus en plus de données étaient stockées sur ordinateurs, les entreprises ressentirent le besoin d'interconnecter leurs différents sites distants. Grâce à l'utilisation des lignes dédiées, une entreprise avait à la garantie que la connexion entre ses départements serait toujours disponible et privée.

Cette solution semble très couteuse, notamment si l'entreprise à plusieurs bureaux à travers tout un pays, de plus, les réseaux privés manque de souplesse par rapport aux situations que l'on peut rencontrer dans une entreprise. En effet, si un représentant a besoin d'accéder à distance au réseau privé de son entreprise alors qu'il est à des milliers de kilomètres de celle-ci, le coût devient extrêmement élevé.

Les entreprises cherchent toujours des solutions moins couteuses et efficaces, d'où vient l'idée des VPN (réseaux privés virtuelles), qui sont des concepts réalisés sous une infrastructure publique déjà existante telle qu'Internet, et l'exploiter pour des besoins privés, et puisque ce support est publique, il est plus vulnérable aux attaques malveillantes ce qui rend inutile d'utiliser cette liaison publique si elle n'est pas sécurisé.

Pour se protéger contre ces attaques, un VPN doit mettre en œuvre les fonctionnalités suivantes :

- ❖ **Authentification** : garantir que les données reçues proviennent de l'expéditeur déclaré.
- ❖ **Confidentialité** : Les données transportées ne peuvent être lues que par les tiers communicants.
- ❖ **Intégrité** : garantit que les données n'ont pas été modifiées durant leur transfert.
- ❖ **Anti-rejeu** : Le récepteur peut rejeter les anciens paquets ou les paquets dupliqués.

Cette étude est organisée sur 4 chapitres et une application :

- Le premier chapitre est une introduction aux réseaux de nouvelle génération (NGN), en suite une description du réseau « RMS d'Algérie Telecom »
- Le deuxième chapitre généralité sur les VPN (réseaux privés virtuelles).
- Dans Le troisième chapitre on a traité en premier lieu une introduction et des concepts de base de la technologie MPLS, puis les applications de cette technologie
- Le quatrième chapitre décrit L'une des applications les plus importantes du protocole MPLS est de pouvoir créer des réseaux privés virtuels VPN (réseaux privés virtuelles).
- Application décrit notre application pratique et les scénarios utilisés pour donner une valeur a l'étude théorique.

Chapitre I :

Introduction aux réseaux NGN

BIBLIOGRAPHIE:

- [1] : « Convergence Et Reseaux de Prochaine Generation » OCDE sur *l'avenir de l'économie de l'Internet* (17 et 18 juin 2008, Séoul, Corée).
- [2] : http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html
- [3] : Ahmed AIT ALI, these "Amelioration de la Mesure de la BandePassante dans un Reseau Base sur IP", Ecole doctorale IAEM Lorraine,2008
- [4] : *Walid Dabbous* , « Quelle architecture pour l'Internet du futur ? » , 4 février 2008 à l'INRIA Sophia Antipolis.
- [5] : CCNP Security VPN 642-647 Official Cert Guide Howard Hooper, CCIE No. 23470
- [6]: Danièle Dromard et Dominique Seret , « Architecture des réseaux », 2009 Pearson Education France
- [7]: L. Cittadini, G. Di Battista, M. Patrignani, "MPLS Virtual Private Networks", in H. Haddadi, O. Bonaventure (Eds.),Recent Advances in Networking, (2013), pp. 275-304. Licensed under a CC-BY-SA Creative Commons license.
- [8] : [http://www.intenseschool.com/GNS3 Lab Introduction to MPLS Layer 3 VPN Part 1 - Intense School.htm](http://www.intenseschool.com/GNS3%20Lab%20Introduction%20to%20MPLS%20Layer%203%20VPN%20Part%201%20-%20Intense%20School.htm)
- [9] :http://www.cisco.com/en/US/docs/ios/12_1/switch/configuration/guide/xcdtagc.html?referring_site=bodynav
- [10]: *Michael H. Behringer, Monique J. Morrow* "MPLS VPN Security"
- [11]: http://www.humanforcetunisie.com/Bibli/Loi-cnss-tunisie.php#_Toc72041853
- [12]: <http://fr.scribd.com/doc/80012946/Mpls-Cisco-by-Amichoo-Istanet>
- [13]:<http://www.memoireonline.com/03/11/4293/Mise-en-oeuvre-dun-coeur-dereseau->

IPMPLS.html

[14]: <http://fr.scribd.com/doc/76647205/MPLS-GMPLS>

[15]: <http://www.guill.net/index.php?cat=3&pro=3&wan=5>

[16]: <http://wapiti.telecomlille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exp-osesrio2002ttnfa03/Bordessoules-Bret/Site/MPLS.htm>

[17]: <http://www.invocom.et.put.poznan.pl/~invocom/C/INT/tcpip/fr/ch5.html>

[18]: <http://www.frameip.com/vpn/>

[19]: <http://www.memoireonline.com/12/10/4148/Mise-en-place-dune-architecture-VPN-MPLS-avec-gestion-du-temps-de-connexion-et-de-la-bande-passan.html>

[20]: <http://www.frameip.com/mppls/>

[21]: <http://www.frameip.com/mppls-cisco/>

[22]: <http://www-igm.univ-mlv.fr/~dr/XPOSE2006/marot/>

[23]: http://www-igm.univ-mlv.fr/~dr/XPOSE2007/ykarkab_MPLS/

[24]: http://www.bonnefoy.eu/25_OSPF

[25]: <http://www.dissertationsgratuites.com/dissertations/Microprocesseur-8086/495133.html>

[Y,D]: YEKACHE Yacine et DARAMAR Kouider, « Ingénierie de Trafic et QoS dans les réseaux NGN », 2008/ 2009

[B,S] : BELLI Abdelkader & SOUDANI Talha, « Sécurité de l'information par solution VPN (Virtual Private Network) » 2008/2009

[E,A] :El-mohri Omar & Abdellatif yahia « Architectures des réseaux VPN » 2006

[B,M] :BENMISSOUM Mohamed & METEGUELARD Mohamed, « IPsec dans les VPNs » 2009/2010

VIDEO TRAINING

- + “MPLS Technology”, by Ahmed Abdel Fatah Al hefni.
- + “MPLS Fundamentals”, CBT Nuggets, by KEITH Barker.
- + “project all routings protocols”, CCNAX.

Résumé :

Les outils de communication sont l'une des plus efficaces et les plus nécessaires pour une entreprise, donc comme il est nécessaire d'assurer la communication, son cout est aussi important.

Les VPN sont venus pour répondre à l'augmentation de la demande de connexion qui révèle très chère avec les méthodes anciennes. L'utilisation de l'infrastructure publique permet une réduction énorme des couts. Ce projet décrit les bases de VPN et réalisation des technologies les plus utilisées pour les installer.

ملخص :

إن وسائل الاتصال مهمة وضرورية لتواصل الشركات، وبما أنها ضرورية لنقل المعلومات وتبادل الاتصال فإن تكلفتها مهمة أيضا. جاءت الشبكات الوهمية الخاصة (VPN) نتيجة للطلبات المتزايدة على الاتصال والتي أظهرت التكلفة الباهظة جراء استعمال الطرق القديمة. فاستخدام بنيات وهمية كفيلة بتخفيض التكاليف. هذا المشروع يصف القواعد الأساسية للشبكات الوهمية الخاصة (VPN) واستيعاب التقنيات المتاحة لتنصيبها.

Abstract :

The communications tools are one of most effective and most necessary for a company, therefore as it is necessary to ensure the communication, its cost is also important. The VPN came to spread with the increase in the demand of connection which reveals very expensive with the old methods. The use of the public infrastructure allows an enormous reduction of the costs. This project describes the bases of VPN and realization of technologies the most used to install them.