Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE ABOU BEKR BELKAID TLEMCEN
FACULTE DE TECHNOLOGIE

DEPARTEMENT DE GENIE ELECTRIQUE ET ELECTRONIQUE

Laboratoire STIC

Ecole doctorale des
Sciences et Technologies de l'Information et Télécommunication

Mémoire de Magister en
Systèmes et Réseaux de Télécommunication

THEME

PLANIFICATION, INGENIERIE DES RESEAUX DE NOUVELLE GENERATION - NGN

Présenté par

Ghefir Mohamed El Amine

Soutenu en Décembre 2013 devant le jury composé de :qhj

Président :	Mr Kameche Samir	Maître de Conférences	UABB Tlemcen
Examinateur :	Mr Merzougui Rachid	Maître de Conférences	UABB Tlemcen
Examinateur :	Mr Mana Mohamed	Maître de Conférences	CU Ain Temouchent
Encadreur :	Mr FEHAM Mohammed	Professeur	UABB Tlemcen

Remerciement

Je tiens tout particulièrement, à remercier mon encadreur, Monsieur M.FEHAM professeur à l'Université Abou-Bekr Belkaïd Tlemcen pour avoir su m'orienter avec toute l'attention et la gentillesse requise pendant ces années, Ses qualités scientifiques et humaines, son encouragement et ses remarques ont largement contribué à l'aboutissement de ce mémoire. Qu'il trouve ici l'expression de ma profonde et pleine gratitude.

Je tiens également à adresser mes plus vifs remerciements à Mr S.KAMECHE Maître de Conférences à l'Université Abou-Bekr Belkaïd Tlemcen, qui m'a fait l'honneur de présider le jury.

Je remercie aussi Messieurs, Mr. M.MANA, Maître de Conférences à l'Université d'Ain Temouchent, ainsi que Mr R.MERZOUGUI Maître de Conférences, Qu'ils trouvent ici le témoignage de mes sincères remerciements pour avoir accepté d'examiner le présent travail.

Enfin j'adresse tous mes remerciements les plus sincères à tous ceux qui ont contribué de près ou de loin à la concrétisation de ce travail.

M.GHEFIR

Résumé

Durant ces dernières années, l'architecture de l'internet s'est développée, par l'introduction des nouvelles technologies, et ce afin d'assurer une adaptation aux nouveaux besoins.

L'introduction du protocole MPLS (Multi-Protocol Label Switching) a contribué au routage internet, à l'ingénierie du trafic et à la qualité de service requise pour l'introduction des nouveaux services.

Il serait intéressant de comparer les performances QoS des réseaux MPLS et MPLS / DiffServ, en prenant en compte leurs contraintes particulières.

Dans cette thèse, nous avons évalué les mesures de performance QoS tels que la variation de retard, le retard, temps de réponse, le débit pour différents types de trafics (voix, données et vidéo) pour les deux plateformes MPLS et MPLS / DiffServ.

L'objectif de cette thèse est de comparer les performances des réseaux MPLS et MPLS / DiffServ à l'aide d'une application de simulation de réseau bien connu «OPNET Modeler v14.5 », qui permettra de reproduire un véritable scénario de réseau réel, en utilisant les dernières techniques de simulation, où les différents paramètres de QoS peuvent être mesurés pour comparer les performances des réseaux.

Notre approche dans cette thèse, s'est de concevoir et de construire un cœur de réseau de type opérateur pour simuler un scénario réel qui véhicule les différents types de trafics (voix, données et vidéo).

Les résultats de la thèse sont présentés suivant le temps de simulation et la charge du réseau. Les résultats de la comparaison démontrent l'avantage sur la performance des réseaux MPLS avec diffserv par rapport aux réseaux MPLS traditionnelles.

Mots clés : OPNET, MPLS, réseau de nouvelle génération NGN

Abstract

In the recent years, the Internet architecture has evolved, incorporating new technologies and adapting to the changing needs of its use. The introduction of Multi-Protocol Label Switching (MPLS) as a part of the Internet forwarding architecture has immediate applications in traffic engineering (TE) and Quality of Service (QoS). It would be interesting to compare QoS performance of MPLS networks and MPLS/DiffServ networks, given their particular constraints. In this thesis, we evaluated the QoS performance measures such as delay variation, delay, page response time, throughput, for different types of traffics (data, voice, and video) for both MPLS and MPLS/DiffServ platforms. The aim of this thesis is to compare the performance of MPLS and MPLS/DiffServ networks using the well known network simulator application "OPNET Modeler". OPNET Modeler, v14.5, provides a platform to replicate a real world network scenario using latest simulation techniques, where different QoS parameters can be measured to compare networks performance. Our approach in this thesis is that, we have designed and built a National Carrier based core and edge network to simulate a real live scenario that spans in the Algeria , Some of the results in the thesis are presented against simulation time and some against network load. The results of comparing and evaluating these two core networks (MPLS and MPLS/DiffServ) through well know QoS parameters show that complimenting MPLS by Diffserv give better results than MPLS alone.

keys word: OPNET, MPLS, NGN,

ملخص الرسالة

في السنوات الأخيرة، تطورت الانترنت من ناحية تكوين البنية التحتية و ذلك عن طريق دمج بعض التقنيات الجديدة و تكييفها لاستيعاب حاجة التقنية وتوافقها مع التغيرات المستمرة المتسارعة في العالم.

تقوم هذه الأطروحة بمقارنة شبكات MPLS مع شبكات MPLS with DiffServ من حيث الأداء باستخدام بعض المعايير المشهورة من معايير أداء الخدمة . QoS وتشمل هذه المعايير الاختلاف في التأخير في الرزم المرسلة، التأخير في الرزم المرسلة، زمن استجابة الصفحة، الانتاجية، باستخدام رزم من عدة انواع (بيانات عادية، فيديو، و صوت.)

وللقيام بهذه المقارنة ، جاءت الحاجة للبحث عن برنامج محاكاة يتيح لنا دراسة هذه

الشبكات،حيث تم اختيار و استخدام برنامج المحاكاة المشهور OPNET :

MODELER Release 14.5 .

تُقدم الأطروحة مُقدمة إلى تقنيات OPNET ، MPLS و MPLS/DiffServ ، وتصف منهجية المحاكاة ومقاييس الأداء.

في هذه الاطروحة تم بناء شبكة مشابة لشبكات ناقلي البيانات في الجزائر ،

ليتم عمل مقارنة للأداء بين كُلٍ من شبكات MPLS و MPLS/DiffServ عن طريق

مقاييس الاداء QoS ، و تبين لنا ان اداء شبكات MPLS/DiffServ افضل من اداء شبكاتMPLS

الكلمات المفتاحية : OPNET, MPLS, NGN

Table des matières

CHAPITRE II : EVOLUTIONS TECHNOLOGIQUE DES CŒURS DE RESEAUX

CHAPITRE III : IP/MPLS

CHAPITRE IV : LES RÉSEAUX DE TRANSPORT OPTIQUES

CHAPITRE V : Les Différentes phases pour un déploiement d'un réseau de Télécommunication

CHAPITRE VI : Etude Comparatif de Performance réseau MPLS et MPLS_diffserv sous OPNET MODELER

Listes des figures

Liste des tableaux

Introduction générale

Un réseau peut être vu comme un ensemble de ressources mise en place pour offrir un ensemble de services. C'est l'évolution des services et des trafics qui en découlent qui a piloté, dans les dernières années, l'évolution technologique permettant d'augmenter la capacité et les fonctionnalités des ressources des réseaux. Ainsi, par exemple, le succès des services de l'Internet a engendré une explosion de trafic ; ce qui a mené les opérateurs à utiliser de nouvelles technologies dans le cœur des réseaux telles que l'IP sur ATM, le PoS, l'IP sur WDM et le MPLS.

Les évolutions récentes ont également été fortement influencées par la dérégulation. La concurrence a amené une baisse des prix de la plupart des services classiques, ce qui a réduit les revenus des opérateurs. Dès lors que la différenciation par les prix devient difficile, celle- ci ne peut se faire que par les services et leur qualité. L'offre de services innovants et l'amélioration de la qualité des services existants, tels que la navigation du Web, requièrent souvent une évolution de la bande passante à l'accès. Ainsi, des technologies comme le xDSL, la BLR et les réseaux HFC, se sont développées.

Un point essentiel dans l'évolution de l'offre des services concerne la capacité à regrouper l'ensemble des services dont le client a besoin et de les lui offrir, si possible de manière convergente, à travers une interface unique. Cela pousse les opérateurs à bâtir des réseaux multiservices avec convergence entre services.

Dans cette situation, le terme "convergence" (des techniques et des services) est largement utilisé pour désigner la fusion des services et des techniques. La convergence s'observe ainsi entre la télévision et les télécommunications, les réseaux fixes et les réseaux mobiles, les télécommunications et l'information, les ordinateurs et l'électronique grand public. De la convergence découle la nécessité de disposer d'architectures, de réseaux, d'équipements et d'outils de gestion permettant de répondre aux besoins des consommateurs, en ce qui concerne les services proposés, et aux besoins techniques observés au niveau des réseaux pour ce qui est des interfaces entre les équipements, les réseaux et les services. La nouvelle génération d'architectures de réseaux: NGN (Next Generation Networks) semblent bien adaptées pour la mise en place de la convergence voix/données.

Dans ce contexte l'objectif de notre recherche est de présenter en premier lieu les caractéristiques de l'architecture des réseaux NGN, ainsi de faire une étude détaillée pour la mise en œuvre d'un cœur de réseau basé sur une plateforme IP/MPLS.

Le présent rapport est organisé en six (06) chapitres :

- Le premier chapitre représente une introduction aux réseaux NGN, qui trace les principales caractéristiques des réseaux NGN, les principales couches, les entités fonctionnelles pour enfin citer les services offerts par les NGN.
- Le deuxième chapitre, présente l'évolution technologique des cœurs de réseaux.
- Le troisième chapitre, présente le mécanisme de fonctionnement de l'architecture MPLS.
- Le quatrième chapitre est consacré à la présentation des réseaux de transport optiques
- Le cinquième chapitre, nous avons décrit les solutions et les étapes à suivre pour le dimensionnement d'un réseau NGN.
- Le sixième chapitre - Simulation sous Opnet « Etude Comparatif de Performance réseau MPLS et MPLS_diffserv sous OPNET MODELER».

Chapitre I

INTRODUCTION AUX RESEAUX NGN

I.1 Introduction

L'évolution progressive du monde des télécommunications vers des réseaux et des services de nouvelle génération est aujourd'hui une tendance forte qui suscite l'intérêt d'une majorité d'acteurs. Elle résulte de la conjonction d'un ensemble de facteurs favorables dont:

- Les évolutions profondes du secteur des télécommunications.
- Le développement de gammes de services nouveaux.
- Les progressions technologiques d'envergure dans le domaine des réseaux de données.

Il en résulte de ce contexte et afin de s'adapter aux grandes tendances qui sont la recherche de souplesse d'évolution de réseau, la distribution de l'intelligence dans le réseau, et l'ouverture à des services tiers, une évolution vers un nouveau modèle de réseaux et de services appelé NGN (Next Generation Networks).

I.2 Définition du NGN

NGN ou *Next Generation Network* en anglais (littéralement "Réseau de Nouvelle Génération") est une expression fréquemment employée dans l'industrie des télécommunications, notamment depuis le début des années 1990. Il n'existe pas de définition unique. Le sens varie en fonction du contexte et du domaine d'application. Toutefois, le terme désigne le plus souvent le réseau d'une compagnie de télécommunications dont l'architecture repose sur un plan de transfert en mode paquet, capable de se substituer au réseau téléphonique commuté et aux autres réseaux traditionnels. L'opérateur dispose d'un cœur de réseau unique qui lui permet de fournir aux abonnés de multiples services (voix, données, contenus audiovisuels...) sur différentes technologies d'accès fixes et mobiles. Autrement, "NGN" est également utilisé très souvent à des fins marketings par les opérateurs et les fabricants pour rendre compte de la nouveauté d'un réseau ou d'un équipement de réseau.[01]

Les réseaux de la prochaine génération, avec leur architecture répartie, exploitent pleinement des technologies de pointe pour offrir de nouveaux services sophistiqués et augmenter les recettes des opérateurs tout en réduisant leurs dépenses d'investissement et leurs coûts d'exploitation.

Les NGN sont basés sur une évolution progressive vers le « tout IP » et sont modélisés en couches indépendantes dialoguant via des interfaces ouvertes et normalisées. Afin d'offrir aux

fournisseurs de services ainsi qu'aux opérateurs une plateforme évolutive pour créer, déployer et gérer des services multimédias innovants, ainsi les services doivent être évolutifs et accessibles indépendamment des réseaux d'accès.

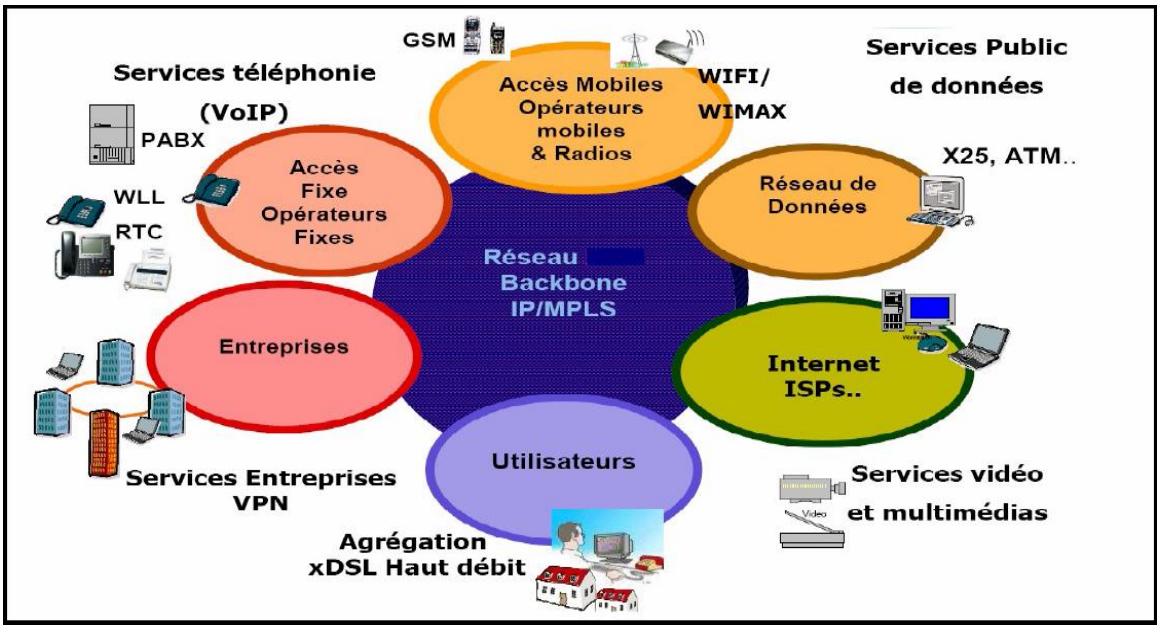

Figure I-1: Principe de consolidation du réseau

I.3 Les exigences de tourner vers NGN

Depuis quelques années, les laboratoires des constructeurs et les organismes de standardisation se penchent sur une nouvelle architecture réseau les Next Generation Networks (NGN) pour répondre aux exigences suivantes |01]:

- Les réseaux de télécommunications sont spécialisés et structurés avant tout pour la téléphonie fixe.
- Le développement de nouveaux services, évolution des usages du réseau d'accès fixe et l'arrivée du haut débit.
- La migration des réseaux mobiles vers les données.
- Difficulté à gérer des technologies multiples (SONET, ATM, TDM, IP) Seul un vrai système intégré peut maîtriser toutes ces technologies reposant sur la voix ou le monde des données.
- Prévision d'une progression lente du trafic voix et au contraire une progression exponentielle du volume de données => baisse de la rentabilité des opérateurs.

I.4 Nouvelles orientations du protocole IP

La convergence Voix/Données/Image est devenue une réalité technique et commerciale. Elle entraîne une mutation significative de la base de compétences des Ingénieurs qui la mettent en œuvre au sein des opérateurs, des constructeurs et des entreprises utilisatrices.

Les deux « piliers » de cette convergence sont d'une part le protocole Internet (IP), et d'autre part le très haut débit.

En effet, IP s'impose comme protocole unificateur des réseaux de nouvelle génération (NGN). Chez les opérateurs et dans les entreprises, la migration vers le tout IP est engagée. La téléphonie traditionnelle, principale source de revenus jusqu'à aujourd'hui, est en perte de vitesse au profit de la téléphonie sur IP. Les services de données traditionnels sont eux aussi en forte régression devant les nouvelles offres technologiques (VPN-IP, MPLS) garantes de la qualité de service (QoS) exigée.

Le très haut débit notamment sur fibre optique s'impose partout car lui seul peut offrir aux nouveaux services convergents la qualité requise. Après d'être définitivement imposée dans les cœurs de réseaux, le très haut débit est partie à la conquête de l'accès. Les déploiements se multiplient (FTTH) et les nouveaux acteurs, que constituent les collectivités locales, contribuent largement à ce succès.

I.5 Caractéristiques du réseau NGN

I.5.1 Une nouvelle génération de commutation

Les solutions de commutation de nouvelle génération fournissent une gamme complète de la catégorie de commutation, voix over IP adaptée aux besoins des abonnés complétées par des applications convergées de voix/données pour établir un réseau de nouvelle génération (une commutation par paquets). [01]

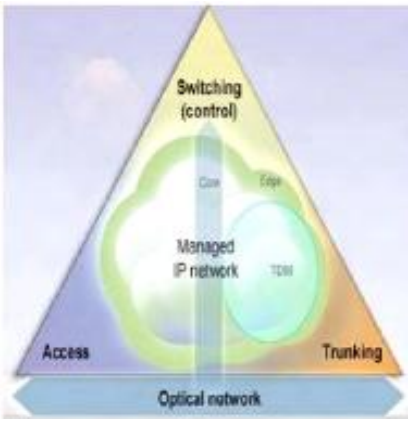

Figure I-2 : Caractéristiques du réseau NGN

I.5.2 Une nouvelle génération de réseaux optiques

Les solutions de système optique de nouvelle génération rassemblent les deux réseaux optiques existants y compris celui du multiplexage DWDM et les réseaux optiques SDH. Avec la nouvelle génération de systèmes optiques, des réseaux IP optimisés peuvent être déployés. Les fonctions de données et Ethernet sont ajoutées aux dispositifs classiques de transport.

I.5.3 Une nouvelle génération de type d'accès

Les nouvelles technologies d'accès sont une composante très importante car elles influencent la rapidité d'introduction et les modalités techniques de mise en œuvre des cœurs de réseau NGN. Elles ont donc chacune un rôle à jouer dans le développement des services IP multimédia de nouvelle génération et sont caractérisées par :

- leur niveau de maturité (existence de produits)
- la commutation utilisée (interface vers le cœur de réseau)
- le débit

La multitude et la montée en charge de ces technologies devenant ingérable en matière de qualité de service sur le mode de fonctionnement actuel, l'intégration de MPLS s'est avérée urgente dans la couche transport. Ce protocole permet de prendre en compte différentes classes de services afin d'assurer qualité et sécurité.

I.5.4 Une nouvelle génération de gestion

Des solutions de gestion de réseaux de nouvelle génération sont optimisées pour la gestion des alarmes, gestion de configuration et d'exécution et de sécurité des modules du réseau NGN. Basé sur un concept modulaire de gestion d'éléments et de domaines de gestion et d'applications, le réseau NGN supporte pleinement les opérations d'exploitation, d'administration et de maintenance (OA&M), la configuration de réseau et l'approvisionnement de service comprenant un déploiement de masse, ayant des interfaces ouvertes pour une intégration facile.

I.6 Architecture en couche

Les réseaux NGN reposent sur une architecture en couches indépendantes (transport, contrôle, services) communiquant via des interfaces ouvertes et normalisées. Les services doivent être évolutifs et accessibles indépendamment du réseau d'accès utilisé [01].

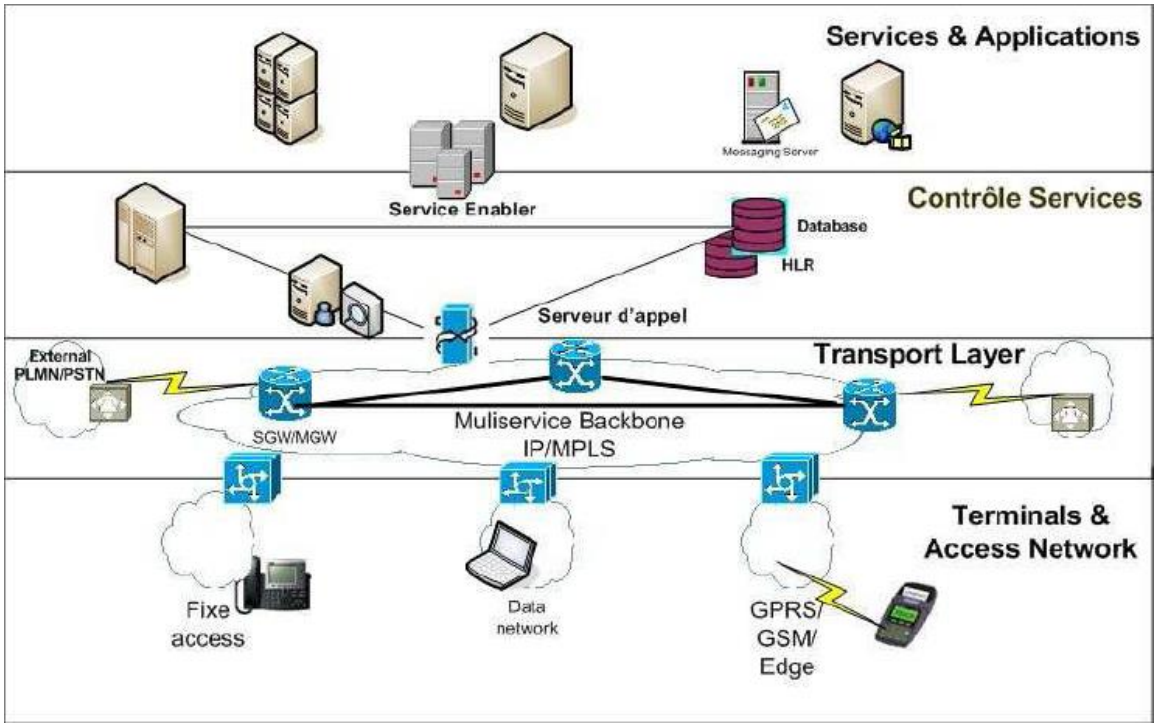

Figure I-3 : Principe général d'architecture d'un réseau NGN

I.6.1 Couche transport

C'est la partie responsable de l'acheminement du trafic voix ou données dans le cœur de réseau, selon le protocole utilisé.

Cette couche se divise en deux sous-couches

- **La couche accès :** qui regroupe les fonctions et les équipements permettant de gérer l'accès des équipements utilisateurs au réseau, selon la technologie d'accès (téléphonie commutée, DSL, câble). Cette couche inclut par exemple les équipements DSLAM (DSL Access Multiplexer) fournissant l'accès DSL.
- **La couche Cœur de réseau :** c'est la partie responsable de l'acheminement du trafic voix ou données dans le cœur de réseau IP, selon le protocole utilisé. L'équipement important à ce niveau dans une architecture NGN est le « Media Gateway » (MGW) qui est responsable de l'adaptation des protocoles de transport aux différents types de réseaux physiques disponibles (TDM, IP, ATM, SDH, DWDM).

I.6.2 Couche contrôle

Cette couche gère l'ensemble des fonctions de contrôle des services en général, et de contrôle d'appel en particulier pour le service voix. L'équipement important à ce niveau dans une architecture NGN est le serveur d'appel, plus communément appelé «softswitch », qui fournit, dans le cas de services vocaux, l'équivalent de la fonction de commutation [01].

I.6.3 Couche service

L'ensemble des fonctions permettant la fourniture de services dans un réseau NGN. En termes d'équipements, Cette couche regroupe deux types d'équipement les serveurs d'application (ou application servers) et les « enablers », qui sont des fonctionnalités, comme la gestion de l'information de présence de l'utilisateur, susceptibles d'être utilisées par plusieurs applications. Cette couche inclut généralement des serveurs d'application SIP (Session Initiation Protocol), car il est utilisé dans une architecture NGN pour gérer des sessions multimédias en général, et des services de voix sur IP en particulier.

Ces couches sont indépendantes et communiquent entre elles via des interfaces ouvertes. Cette structure en couches est sensée garantir une meilleure flexibilité et une implémentation de nouveaux services plus efficace. La mise en place d'interfaces ouvertes facilite l'intégration de nouveaux services développés sur un réseau d'opérateur mais peut aussi s'avérer essentielle pour assurer l'interconnexion d'un réseau NGN avec d'autres réseaux qu'ils soient NGN ou traditionnels. L'impact majeur pour les réseaux de téléphonie commutée traditionnels est que le commutateur traditionnel est scindé en deux éléments logiques distincts : le media Gateway

pour assurer le transport et le softswitch pour assurer le contrôle d'appel. Une fois les communications téléphoniques « empaquetées » grâce aux media Gateway, il n'y a plus de dépendance des services vis-à-vis des caractéristiques physiques du réseau. Un cœur de réseau paquet unique, partagé par plusieurs réseaux d'accès constitue alors une perspective attrayante pour des opérateurs. Bien souvent, le choix se porte sur un cœur de réseau IP/MPLS commun au niveau de la couche de transport du NGN afin de conférer au réseau IP les mécanismes de qualité de service suffisants pour assurer une fourniture de services adéquate.

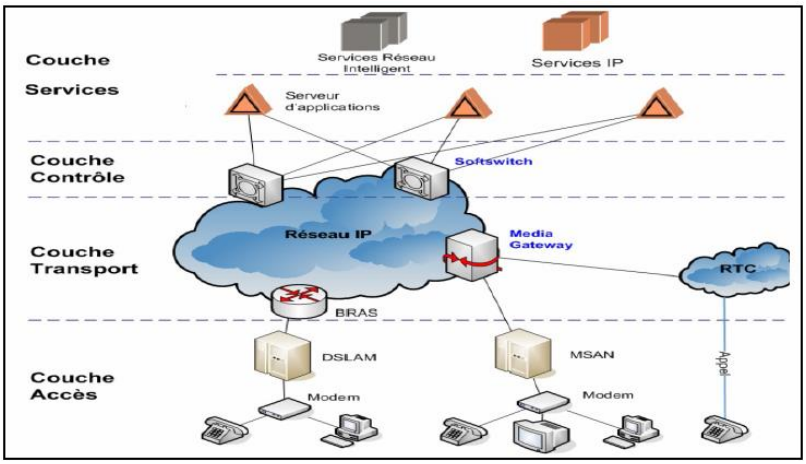

Figure I-4 : Architecture en couche d'un réseau NGN

I.7 Principaux équipements du réseau NGN

I.7.1 Le Media Gateway Controller (MGC)

Le serveur d'appel dits aussi « softswitch » n'est autre qu'un serveur informatique, doté d'un logiciel de traitement des appels vocaux, gérant d'une part les mécanismes de contrôle d'appel (pilotage de la couche transport, gestion des adresses), et d'autre part l'accès aux services (profils d'abonnés, accès aux plates-formes de services à valeur ajoutée).

Dans un réseau NGN, c'est le MGC qui possède « l'intelligence ». Il gère :

- L'échange des messages de signalisation transmise de part et d'autre avec les passerelles de signalisation, et l'interprétation de cette signalisation.
- Le traitement des appels : dialogue avec les terminaux H.323, SIP voire MGCP, communication avec les serveurs d'application pour la fourniture des services.
- Le choix du MG de sortie selon l'adresse du destinataire, le type d'appel, la charge du réseau, etc.
- La réservation des ressources dans le MG et le contrôle des connexions internes au MG (commande des Media Gateways).

I.7.2 La Media Gateway (MG)

Les Gateways ont un rôle essentiel : elles assurent non seulement l'acheminement du trafic, mais aussi l'interfonctionnement avec les réseaux externes et avec les divers réseaux d'accès. La Media Gateway est située au niveau du transport des flux média entre le réseau RTC et les réseaux en mode paquet, ou entre le cœur de réseau NGN et les réseaux d'accès. Elle a pour rôle le codage et la mise en paquets du flux média reçu du RTC et vice-versa (conversion du trafic TDM IP). Et aussi la transmission, suivant les instructions du Media Gateway Controller, des flux média reçus de part et d'autre

I.7.3 La Signalling Gateway (SG)

La fonction Signalling Gateway a pour rôle de convertir la signalisation échangée entre le réseau NGN et le réseau externe interconnecté selon un format compréhensible par les équipements chargés de la traiter, mais sans l'interpréter (ce rôle étant dévolu au Media Gateway Controller). Notamment, elle assure l'adaptation de la signalisation par rapport au protocole de transport utilisé. Cette fonction est souvent implémentée physiquement dans le même équipement que la Media Gateway, d'où le fait que ce dernier terme est parfois employé abusivement pour recouvrir les deux fonctions MG + SG.

I.8 Les services offerts par les NGN

Les NGN offrent les capacités, en termes d'infrastructure, de protocole et de gestion, de créer et de déployer de nouveaux services multimédia sur des réseaux en mode paquet.
La grande diversité des services est due aux multiples possibilités offertes par les réseaux NGN en termes de :

- Support multimédia (données, texte, audio, visuel).
- Mode de communication, Unicast (communication point à point), Multicast (Communication point-multipoint), Broadcast (diffusion).
- Mobilité (services disponibles partout et tout le temps).
- Portabilité sur les différents terminaux.

Parmi ces services offerts nous citons :

I.8.1 La voix sur IP

La voix sur IP est un service directement lié à l'évolution vers les réseaux NGN. C'est une application qui est apparue depuis longtemps mais qui n'a pas encore eu le succès escompté, et cela pour différentes raisons :

- La jeunesse des protocoles de signalisation (SIP, H.323, MEGACO) de voix sur IP et la gestion de la qualité de service qui commence seulement maintenant à être mature ne permettaient pas de déployer de services téléphoniques sur IP.
- Le seul fait de transporter la voix sur IP n'apporte pas de valeur ajoutée pour L'utilisateur final, par rapport au service de voix classique. Les services associés à la voix sur IP n'ont pas encore la maturité nécessaire pour pousser l'évolution vers ces nouveaux réseaux.
- La nécessité d'interconnecter les réseaux IP aux réseaux TDM/SS7 implique des coûts liés aux équipements d'interconnexion (passerelles) et le prix des terminaux (IP phones).
- Le coût des terminaux IP reste encore supérieur à celui des équipements classiques (pas encore d'économies d'échelle suffisantes).

Cependant l'évolution de la technologie et des protocoles et l'apparition de services associés au monde IP devraient permettre l'émergence de la voix sur IP. De plus, l'évolution des terminaux communicants multimédia est un argument supplémentaire à l'évolution des réseaux téléphoniques vers la voix sur IP, ainsi l'UMTS, dans la release 5, généralise le transport en IP au réseau voix.

I.8.2 La diffusion de contenus multimédia

La diffusion de contenu multimédia regroupe deux activités, l'une focalisée sur la mise en forme des contenus multimédia, l'autre centrée sur l'agrégation de ces divers contenus via des portails.

Les outils technologiques, tels que le multimédia streaming (gestion d'un flux multimédia en termes de bande passante et de synchronisation des données) et le protocole multicast, doivent permettre de fournir un service de diffusion de contenu aux utilisateurs finaux.

I.8.3 La messagerie unifiée

Le service de messagerie unifiée est l'un des services les plus avancés, c'est le premier exemple de convergence et d'accès à l'information à partir des différents moyens d'accès. Le principe est de centraliser tous les types de messages, vocaux (téléphoniques), écrits (email, SMS), multimédia sur un serveur, ce dernier ayant la charge de fournir un accès aux messages adapté au type du terminal de l'utilisateur. Ainsi un email peut être traduit en message vocal par une passerelle « text-to-speech » ou inversement un message vocal sera traduit en mode texte.

I.8.4 Le stockage de données

L'augmentation de capacité des réseaux et la gestion des flux permettent de proposer des services de stockage de données, en tant que sauvegarde de données critiques sur des sites protégés, mais aussi en tant qu'accès « local » à un contenu (serveur « proxy » ou « cache »).

En effet, les volumes de données évoluant de façon exponentielle, la nécessité d'offrir les services à partir des serveurs « locaux » semble indispensable. Cet aspect semble notamment indispensable pour les applications de télévision interactive et de video on demand (VoD).

I.8.5 La messagerie instantanée

Cette application a déjà un grand succès auprès des internautes : elle permet de dialoguer en temps réel, à plusieurs, sur un terminal IP (généralement un PC) ayant accès à Internet via une interface texte. Cependant, il est nécessaire d'installer sur son terminal un logiciel propriétaire permettant de se connecter à un fournisseur d'accès ; il n'est alors possible de communiquer qu'avec les utilisateurs souscrivant au même service. L'évolution des réseaux devrait permettre la standardisation de cette application et la communication entre tous (ouverture du service) à partir de n'importe quel terminal.
C'est l'évolution du service SMS, par l'apport de l'interactivité et du multimédia (MMS).

I.8.6 Services associés à la géolocalisation

La possibilité de localiser géographiquement les terminaux mobiles a été rapidement perçue comme une source de revenus supplémentaires. En effet, la géolocalisation permet de proposer

aux utilisateurs finaux des services très ciblés à haute valeur ajoutée liés au contexte (exemple : horaire, climat et au lieu).

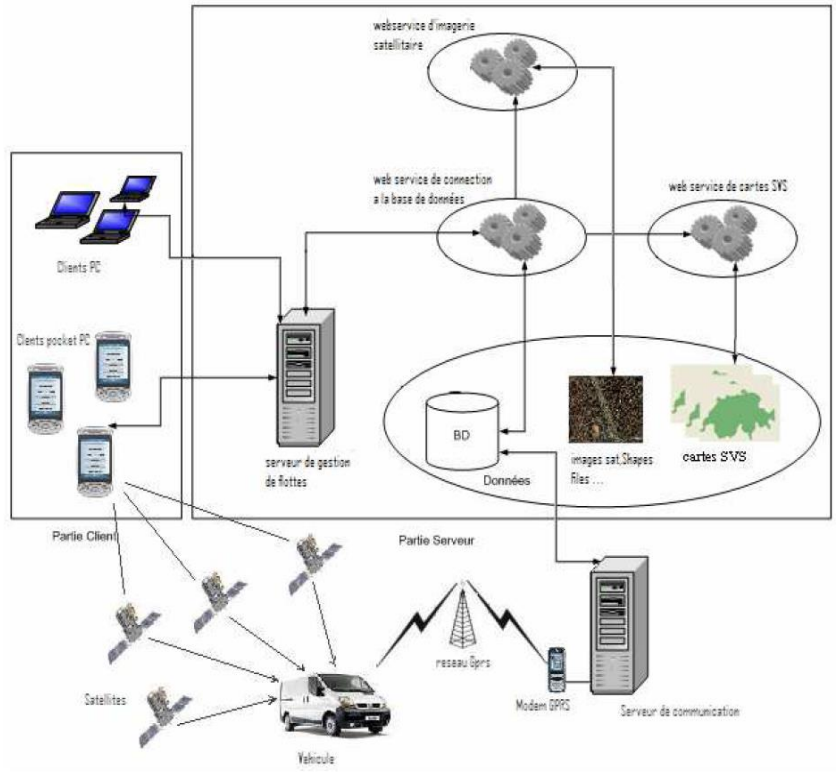

Figure I-5 : Architecture de la plateforme de Géolocalisation

Actuellement plusieurs solutions techniques existent et sont même en cours d'implémentation dans les réseaux d'opérateurs mobiles. Cependant, si ces solutions offrent la capacité de localiser les terminaux mobiles, il n'existe pas encore d'interfaces permettant l'exploitation de ces données par les applications de services, ou de réelle volonté des opérateurs d'ouvrir leurs serveurs de localisation à des fournisseurs de services tiers, afin d'utiliser cette fonction de localisation comme « service capability server » (élément de base servant de support à la réalisation des services).

I.9 Conclusion

Dans ce chapitre nous avons introduit les **NGN** et présenté l'intérêt de leurs mises en œuvre, caractéristiques et hiérarchie. Ainsi que la présentation des principaux équipements d'un réseau NGN et les services offert par les réseaux NGN.

Dans le chapitre suivant on va décrire l'évolution des cœurs de réseaux.

CHAPITRE II

EVOLUTIONS TECHNOLOGIQUE DES CŒURS DE RESEAUX

VI.1 Introduction

Les techniques employées et utilisées dans les cœurs de réseaux et les réseaux backbone ont subi une grande évolution jusqu' à l'arrivée de la normalisation du protocole MPLS et leur développement. Dans ce chapitre nous allons d'écrire quelques technologies, leurs limites et développements, par la suite nous allons citer les étapes de l'évolution de standards MPLS

.

II.2 Frame Relay et X25

VI.2.1 le protocole X25

A la fin des années 1970 et au début des années 1990, la technologie des réseaux étendus reliant deux sites utilisait généralement le protocole X.25. Bien que considère actuellement comme un protocole d'ancienne génération, le X.25 a été une technologie de commutation de paquets très répandue car elle permettait d'obtenir une connexion très fiable sur des infrastructures câblées non fiables. Ce résultat était obtenu grâce à des contrôles de flux et d'erreurs supplémentaires. Ces contrôles alourdissaient cependant le protocole. Celui-ci trouvait son application principale dans le traitement des autorisations de carte de crédit et dans les guichets automatiques. Dans cette partie de chapitre, nous ne citons le protocole X.25 qu'à des fins historiques [01].

VI.2.2 le protocole Frame Relay

Lorsqu'on construit un réseau étendu, quel que soit le mode de transport choisi, deux sites sont toujours relies par un minimum de trois composants ou groupes de composants de base. Chaque site doit avoir son propre équipement (ETTD) pour accéder au central téléphonique local (DCE). Le troisième composant se trouve entre les deux, reliant les deux points d'accès. Dans la figure, il s'agit de la partie fournie par le réseau fédérateur Frame Relay [01].

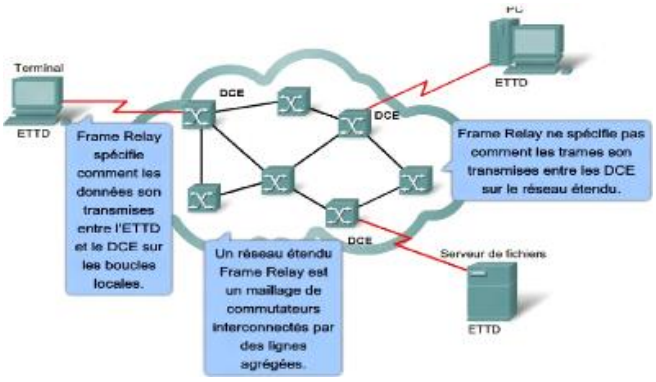

Figure II-1 : réseau étendu frame Relay

Le protocole Frame Relay demande moins de temps de traitement que le X.25, du fait qu'il comporte moins de fonctionnalités. Par exemple, il ne fournit pas de correction d'erreur, car les réseaux étendus actuels permettent d'obtenir des connexions plus fiables que les anciens. Lorsqu'il détecte des erreurs, le nœud Frame Relay abandonne tout simplement les paquets sans notification. Toute correction d'erreur, telle que la retransmission des données, est à la charge des composants d'extrémité. La propagation des données d'une extrémité client à une autre est donc très rapide sur le réseau.

Frame Relay permet un traitement efficace en volume et en vitesse, en réunissant les fonctions des couches liaison de données et réseau en un seul protocole simple. En tant que protocole de liaison de données, Frame Relay permet d'accéder à un réseau, il délimite et fournit les trames dans l'ordre approprié et détecte les erreurs de transmission par un contrôle de redondance cyclique standard. En tant que protocole de réseau, il fournit plusieurs liaisons logiques sur un même circuit physique et permet au réseau d'acheminer les données sur ces liaisons jusqu'à leurs destinations respectives.

Le protocole Frame Relay demande moins de temps de traitement que le X.25, du fait qu'il comporte moins de fonctionnalités. Par exemple, il ne fournit pas de correction d'erreur, car les réseaux étendus actuels permettent d'obtenir des connexions plus fiables que les anciens. Lorsqu'il détecte des erreurs, le nœud Frame Relay abandonne tout simplement les paquets sans notification. Toute correction d'erreur, telle que la retransmission des données, est à la charge des composants d'extrémité. La propagation des données d'une extrémité client à une autre est donc très rapide sur le réseau [01].

II.3 Réseaux multiservices

II.3.1 Les réseaux ATM

La technologie ATM a été adoptée par l'Union Internationale des Télécommunications (UIT) à la fin des années 80 pour répondre à la demande des opérateurs de télécommunication d'un « Réseau Numérique à Intégration de Service Large Bande » unifiant dans un même protocole leurs mécanismes de transport des données, d'images et surtout de la voix, et garantissant la qualité de service.

L'ATM est une technique de transfert asynchrone fondée sur la commutation de paquets de taille fixe (les cellules). Elle repose sur un multiplexage statistique des trafics pour bénéficier des fluctuations des sources de trafics et utiliser au mieux la bande passante de ses liens haut débit. A chaque demande de connexion d'un utilisateur, on lui associe un circuit virtuel (VC), qui est tracé à l'intérieur du réseau ATM par des «marques» laissées dans chaque nœud traversé. Les informations émises par l'utilisateur sont alors transmises par paquets de tailles fixes, appelés cellules, composés de 48 octets pour les données et de 5 octets pour l'entête. Cet entête permet d'identifier le chemin virtuel que devront emprunter les cellules. Ces cellules sont transmises au réseau de manière asynchrone,
Réparties dynamiquement dans le temps dans des slots ne pouvant contenir qu'une seule cellule.

Un réseau ATM est constitué de commutateurs reliés par des liens physiques nommés conduits de transmission. Les commutateurs sont chargés :

- d'acheminer les cellules reçues sur les ports d'entrée vers le bon port de sortie selon les informations de routage contenues dans l'entête de la cellule.
- d'effectuer le multiplexage des cellules sur la sortie requise.
- de contrôler l'établissement et la libération des connexions.

Même si chaque client est amené à négocier directement et spécifiquement la QoS avec l'opérateur, les connexions sont en général regroupées en grandes classes de services (CoS, Class of Service). Les classes de services ATM les plus courantes sont les suivantes

CBR (Constant Bit Rate) : cette classe de trafic est utilisée pour émuler la commutation de circuit. L'émulation de circuit est un flux de trafic constitué de codes d'impulsion modulés envoyés à intervalles réguliers. Le débit d'émission est alors constant. Cette classe de service peut être utilisée pour les connexions exigeant un débit de transfert constant garanti et tolérant

des délais de transfert minimes comme les communications vocales ou vidéo en temps réel. Lors de la négociation d'une connexion CBR, on spécifie en général le taux de perte.

VBR (Variable Bit Rate) : ce service permet aux utilisateurs d'émettre un trafic nécessitant une perte minimale de cellules mais pouvant tolérer une variation au niveau de la bande passante (taux de transfert maximum) pour permettre des périodes de transfert en rafales. On utilise dans ce cas le multiplexage statistique. Selon la sensibilité du trafic à la variation du délai de transmission (CDV), on considère deux sous-catégories : VBR-RT (real-time VBR) et VBR-NRT (non real-time VBR). Ces deux catégories nécessitent la prise en compte du délai moyen de transmission pour la négociation du contrat, mais seul VBR-RT spécifie la variation de délai. Par exemple, la vidéo interactive compressée ferait partie de la classe VBR-RT, et l'e-mail multimédia serait considéré comme trafic VBR-NRT.

ABR (Available Bit Rate) : cette classe est mise en place pour le trafic de données comme le transfert de fichier et l'e-mail ou aux connexions plus tolérantes vis-à-vis des trafics très imprévisibles ou en rafale. Il est possible dans ce genre de contrat de spécifier un débit minimum. Selon l'occupation de la bande passante, la connexion peut être acceptée ou rejetée. Le temps de réponse n'est plus garanti pour cette classe de trafics.

	Garantie de la bande passante	**Garantie de la gigue**	**Garantie du débit**	**Retour d'indication de congestion**
CBR	Oui	Oui	Oui	non
VBR	Oui	Oui	Oui	non
ABR	Non	Non	Oui	oui
UBR	Non	Non	Non	oui

Tableau 1 : Classe de service dans un réseau ATM

UBR (Unspecified Bit Rate) : cette CoS regroupe les connexions nécessitant l'établissement d'un itinéraire mais aucune bande passante garantie, par exemple les transferts de fichiers par lots et les messages électroniques de faible priorité envoyés en bloc. Cette CoS peut être utilisée par les connexions destinées aux programmes qui n'ont pas de contraintes de remise et effectuent eux-mêmes la vérification d'erreurs et le contrôle de flux. Ni le débit moyen, ni le délai, sont garantis pour les trafics UBR.

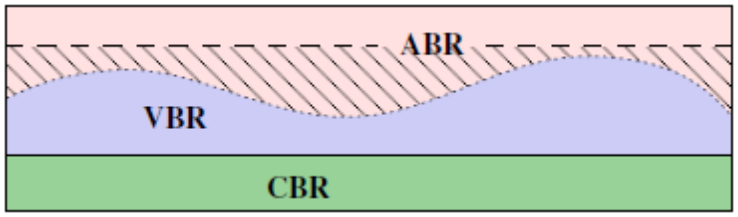

Figure. II-2 : Répartition de la bande passante pour les classes de services CBR, VBR et ABR dans les réseaux ATM.

La zone hachurée correspond à la bande passante réservée aux trafics VBR mais utilisée par des trafics ABR.

Un tel partage de la bande passante permet d'offrir de fortes garantie de QoS pour les services CBR et VBR mais ne garantit rien pour les services ABR, en particulier vis-à-vis du temps de réponse ou des pertes. C'est pourquoi, des méthodes réactives de contrôle de flux ABR sont généralement proposées par les opérateurs, permettant à la source d'adapter son débit à l'aide d'un retour d'information sur la congestion le long du chemin emprunté. Cela permet en particulier de contrôler les pertes sur les trafics ABR.

VI.2.1 IP/ATM

La figure II.3 illustre deux architectures potentielles pour IP sur ATM. L'architecture de gauche (IP over ATM) est celle qui a été retenue par la quasi-totalité des constructeurs et des opérateurs. L'architecture de droite est une solution non implémentée, qui consiste à mettre en parallèle une infrastructure ATM et une pile TCP/IP. L'idée est de faire passer la signalisation par le plan TCP/IP et les données par le plan ATM. L'intérêt de cette solution est d'utiliser l'universalité de l'adressage IP et la puissance de transfert de l'ATM. Son inconvénient est de devoir mettre sur pied un double réseau et de ne pas avoir d'interface native ATM.

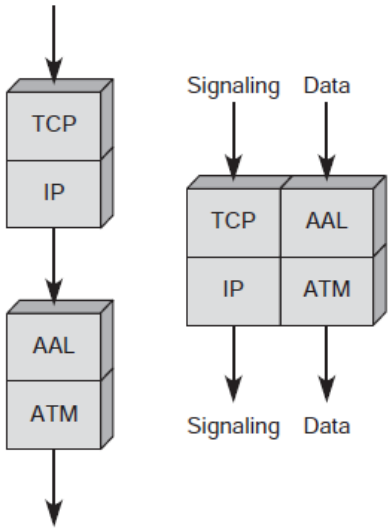

Figure II-3 : Deux architectures IP sur ATM

IP sur ATM était l'approche privilégiée dans les réseaux IP opérationnels aux Etats-Unis entre 1994 et 1998 pour des débits de 155 puis 622 Mbit/s.

C'est sur des prévisions qui, à l'époque, voyaient dans l'augmentation du trafic téléphonique la source principale de croissance du trafic sur les réseaux d'opérateurs de télécommunication existants, aux Etats-Unis et surtout en Europe, pour investir massivement dans ATM comme technologie de leurs réseaux à 155 Mbit/s à partir de la première moitié des années 90. Malheureusement, si ATM est approprié lorsque le trafic est constitué majoritairement de voix, il est inadapté lorsque le trafic est majoritairement constitue de données, ce qui sera de plus en plus le cas avec l'explosion du trafic lie à l'Internet.
D'où les opérateurs historiques se trouvent pris en porte-à-faux par des investissements élevés et des offres inadaptées.

VI.2.2 Convergence vers MPLS

Multiprotocol Label Switching (MPLS) est souvent considéré comme une des technologies majeures pour mettre en œuvre la qualité de service dans les réseaux à commutation de paquets. Toutefois, MPLS a été initialement développé par l'IETF, avec pour objectif d'établir une norme commune pour transporter des paquets IP sur des sous-réseaux travaillant en mode commuté.

Les réseaux MPLS sont des réseaux orienté «connexion» permettant une ingénierie du trafic (Traffic Engineering, MPLS-TE) de réseaux à commutation de paquets. À ce titre, ils peuvent

garantir de la bande passante pour divers flots, ce qui constitue la première condition pour fournir une garantie.

Avec le remplacement progressif des réseaux IP par les réseaux IP/MPLS, les meilleures techniques des réseaux de routage et de commutation se trouvent réunies. Les réseaux IP/MPLS sont capables de s'adapter aux besoins de forte croissance de l'internet, et de prendre la place de l'ATM en faisant face aux très grandes exigences du trafic professionnel.
De plus, les réseaux IP/MPLS sont prêts pour la convergence des données, de la voix et de la vidéo sur IP. Il n'est donc pas surprenant que l'IP/MPLS soit considéré par la majorité des opérateurs de réseau comme le réseau cible à long terme.

Le développement de standard MPLS est passé par les étapes suivantes :

1ère étape :

- Normalisation de la MPLS (Multi Protocol Label Switching) Basé sur le trafic IP.

2ème étape :

- Ajout du service «Traffic Engineering» (MPLS-TE).

3ème étape :

- Développement de MPλS (Multi Protocol Lambda Switching) Basé sur les longueurs d'ondes et ajout d'un nouveau protocole, LMP (Link Management Protocol) pour la gestion des liens et des erreurs.

4ème étape:

- GMPLS (Generalized MPLS), extension de MPLS-TE qui permet aux LSR de supporter Plusieurs types de commutation, Paquets, TDM (SDH/SONET), Lambdas, Fibres etc..., généralisation de la définition d'un label, ajout de la signalisation via le protocole RSVP-TE, et amélioration des protocoles de routage pour décrire la topologie du réseau : OSPF et IS-IS.

II.4 Conclusion

Le but de MPLS est de donner aux routeurs IP une plus grande puissance de commutation, en basant la décision de routage sur une information de label (ou tag) inséré entre le niveau 2 (Data-Link Layer) et le niveau 3 (Network Layer).

La transmission des paquets était ainsi réalisée en commutant les paquets en fonction du label, sans avoir à consulter l'entête de niveau 3 et la table de routage. Alors, MPLS combinait la souplesse du niveau 3 et la rapidité du niveau 2.

Dans le chapitre suivant nous allons développer le protocole MPLS, leur concept et mécanisme.

CHAPITRE III

IP/MPLS

III.1 Introduction

A la fin de l'année 2001, MPLS (Multi Protocol Label Switching) est le sujet d'un grand nombre d'articles et de conférences, mais il est aussi l'objet d'un nombre croissant d'annonces de la part des constructeurs de matériel réseau. À l'heure où les premiers services commerciaux s'appuyant sur un cœur de réseau IP/MPLS apparaissent, l'intérêt de la technologie semble démontré par leur bon fonctionnement. Il reste nécessaire de bien comprendre MPLS pour être capable de faire la part des choses. C'est pourquoi, au-delà des effets de mode, les motivations ayant présidé à la définition de MPLS et les réels apports de MPLS et des technologies associées dans les cœurs de réseaux modernes doivent être compris.

Nous allons, le long de ce chapitre, faire le tour de la technologie MPLS. Nous commencerons par expliquer son principe de fonctionnement. Nous détaillerons ensuite les concepts relatifs aux labels et à leurs distributions. Nous finirons par donner un aperçu des applications que MPLS permet de réaliser.

III.2 Principe de fonctionnement de MPLS

III.2.1 Architecture de MPLS

L'architecture du réseau MPLS utilise des LSR (Label Switch Router) et des LER (Label Edge Router) [02] :

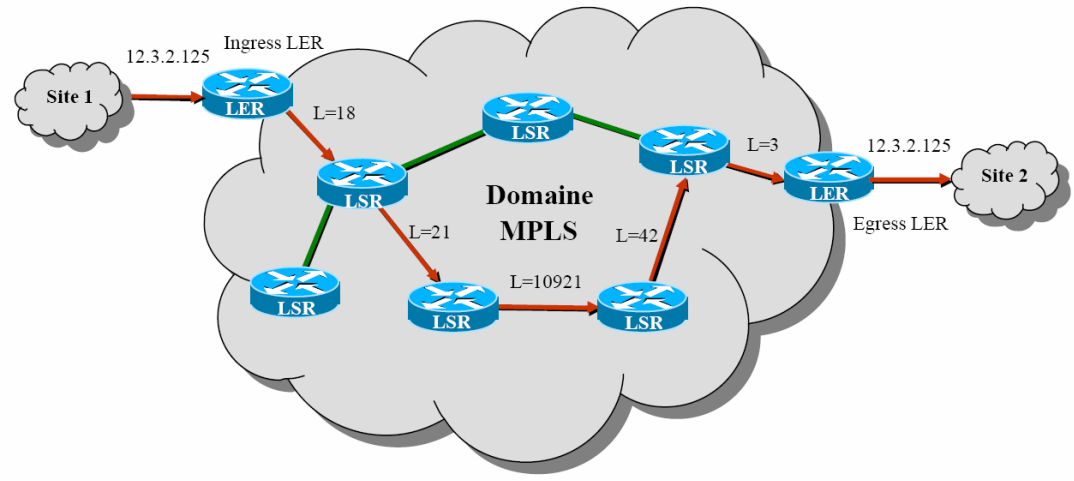

Figure III-1 : Exemple d'un réseau MPLS

III.2.1.1 LSR (Label Switch Router)

Le LSR est un équipement de cœur du réseau MPLS de type routeur, ou commutateur qui effectue la commutation sur les labels et qui participe à la mise en place du chemin par lequel les paquets sont acheminés. Lorsque le routeur LSR reçoit un paquet labélisé, il le permute avec un autre label de sortie et expédie le nouveau paquet labélisé sur l'interface de sortie appropriée. Le routeur LSR, peut jouer plusieurs rôles à savoir :

- l'échange d'informations de routage
- l'échange des labels
- l'acheminement des paquets

III.2.1.2 LER (Label Edge Router)

LER est un LSR qui fait l'interface entre un domaine MPLS et le monde extérieur. En général, une partie de ses interfaces supportent le protocole MPLS et l'autre un protocole de type IP traditionnelles. Les deux types de LER qui existent sont :

- Ingress LER est un routeur qui gère le trafic qui entre dans un réseau MPLS.
- Egress LER 'est un routeur qui gère le trafic qui sort d'un réseau MPLS.

Avant d'examiner le fonctionnement d'un réseau MPLS, on va passer en revue le principe d'acheminement des paquets dans un réseau IP classique et ainsi pouvoir faire une comparaison des deux techniques.

Dans un réseau IP classique, il y a mise en œuvre d'un protocole de routage (RIP, OSPF, IS-IS, etc.). Ce protocole sera exécuté indépendamment par chaque nœud. A la convergence du protocole de routage, chaque nœud aura une vision plus ou moins complète du réseau et pourra du coup calculer une table de routage contenant l'ensemble des destinations. Chaque destination sera associée à un "prochain saut" ou "Next Hop" [02].

Voyant maintenant le cas d'un réseau MPLS : La mise en œuvre de MPLS repose sur la détermination de caractéristiques communes à un ensemble de paquets et dont dépendra l'acheminement de ces derniers. Cette notion de caractéristiques communes est appelée **Forwarding Equivalence Class (FEC)**.

Une FEC est la représentation d'un ensemble de paquets qui sont transmis de la même manière, qui suivent le même chemin au sein du réseau et ayant la même priorité.

- Le routage IP classique distingue les paquets en se basant seulement sur les adresses des réseaux de destination (préfixe d'adresse).
- MPLS constitue les FEC selon de nombreux critères : adresse destination, adresse source, application, QoS, etc [02].

Quand un paquet IP arrive à un ingress LER, il sera associé à une FEC. Puis, exactement comme dans le cas d'un routage IP classique, un protocole de routage sera mis en œuvre pour découvrir un chemin jusqu'à l'egress LER (Voir Figure III-1, les flèches en rouges). Mais à la différence d'un routage IP classique cette opération ne se réalise qu'une seule fois. Ensuite, tous les paquets appartenant à la même FEC seront acheminés suivant ce chemin qu'on appellera Label Switched Path (LSP).

Ainsi on a eu la séparation entre fonction de routage et fonction de commutation : Le routage se fait uniquement à la première étape. Ensuite tous les paquets appartenant à la même FEC subiront une commutation simple à travers ce chemin découvert.

Pour que les LSR puissent commuter correctement les paquets, le Ingress LER affecte une étiquette (appelée aussi Label) à ces paquets (label imposition ou label pushing). Ainsi, si on prend l'exemple de la Figure III-1. Le LSR1 saura en consultant sa table de commutation que tout paquet entrant ayant le label L=18 appartient à la FEC tel et donc doit être commuté sur une sortie tel en lui attribuant un nouveau label L=21 (label swapping). Cette opération de commutation sera exécuter par tous les LSR du LSP jusqu'à aboutir à l'Egress LER qui supprimera le label (label popping ou label disposition) et routera le paquet de nouveau dans le monde IP de façon traditionnelle.
L'acheminement des paquets dans le domaine MPLS ne se fait donc pas à base d'adresse IP mais de label (commutation de label).

Il est claire qu'après la découverte de chemin (par le protocole de routage), il faut mettre en œuvre un protocole qui permet de distribuer les labels entre les LSR pour que ces derniers puissent constituer leurs tables de commutation et ainsi exécuter la commutation de label adéquate à chaque paquet entrant. Cette tâche est effectuée par "***un protocole de distribution*** de label" tel que LDP ou RSVP TE (Reservation Protocol-Traffic Engineering). Les protocoles de distribution de label seront repris plus loin dans un paragraphe à part.

Les trois opérations fondamentales sur les labels (Pushing, swapping et popping) sont tout ce qui est nécessaire pour MPLS. Le Label pushing/popping peut être le résultat d'une classification en FEC aussi complexe qu'on veut. Ainsi on aura placé toute la complexité aux Extrémités du réseau MPLS alors que le cœur du réseau exécutera seulement la fonction simple de label swapping en consultant la table de commutation [02].

III.2.2 Structure fonctionnelle MPLS

Le protocole MPLS est fondé sur les deux plans principaux :

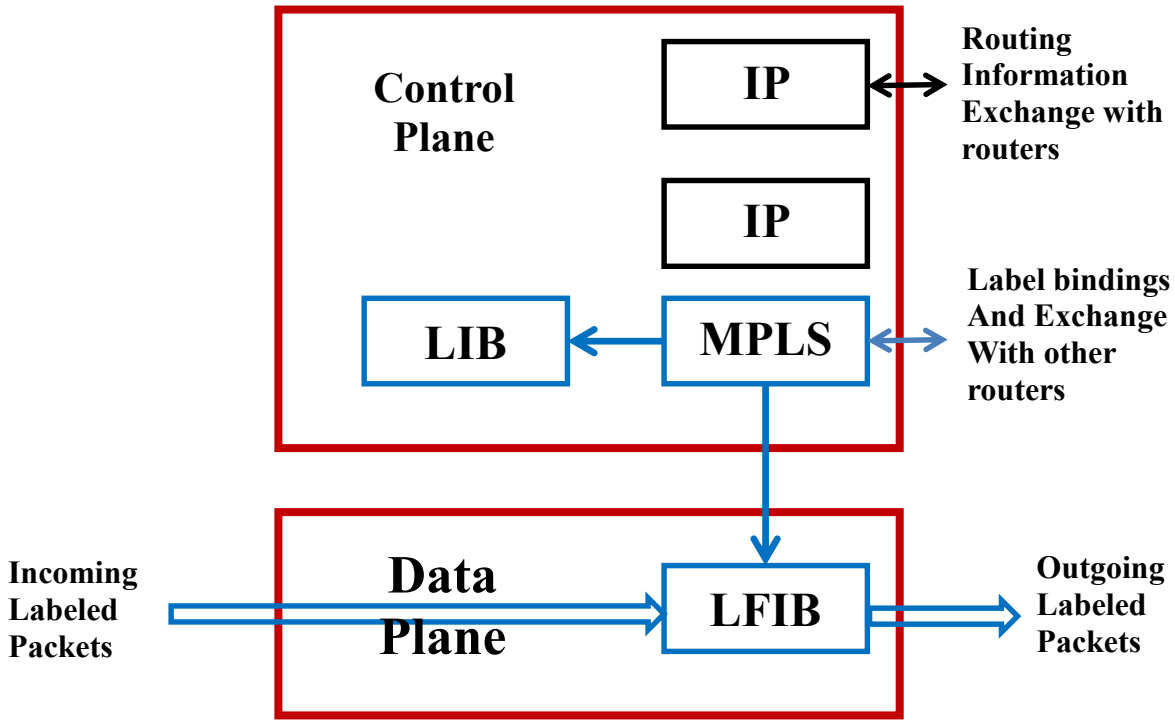

Figure III-2 : Architecture d'un Nœud MPLS.

III.2.2.1 Le plan de contrôle

Le plan de contrôle est composé d'un ensemble de protocoles de routage classique et des protocoles de signalisation. Il est chargé de la construction, du maintien et de la distribution des tables de routage et des tables de commutations. Pour ce faire, le plan de contrôle utilise des protocoles de routages classiques, tels qu'IS-IS ou OSPF afin de créer la topologie des nœuds du réseau MPLS, ainsi que des protocoles de signalisations spécialement développés pour le réseau MPLS comme Label Distribution Protocol (LDP), MPBGP (utilisé par MPLS VPN) ou RSVP (utilisé par MPLS TE).

Dans un réseau MPLS, il existe deux méthodes pour créer et distribuer les labels. Ces méthodes sont « Implicit routing » et « Explicit routing ». Ces deux méthodes sont celles utilisées pour définir les chemins Label Switching Path (LSP) dans le réseau MPLS. La méthode implicit routing est celle du routage implicite, saut par saut (hop by hop) où chaque paquet contenant un LSP choisit indépendamment le saut suivant pour une FEC de données. Le routage explicite est la méthode explicit routing où le premier routeur ELSR détermine la liste des nœuds ou des routeurs LSR à suivre pour délivrer le paquet.

III.2.2.2 Le plan de données

Le plan de données permet de transporter les paquets labélisés à travers le réseau MPLS en se basant sur les tables de commutations. Il correspond à l'acheminement des données en accolant un entête SHIM aux paquets arrivant dans le domaine MPLS. Le plan de données est indépendant des algorithmes de routages et d'échanges de Label. Il utilise une table de commutation appelée Label Forwarding Information Base (LFIB) pour transférer les paquets labélisés avec les bons labels. Cette table est remplie par les protocoles d'échange de label comme le protocole LDP.

A partir des informations de labels apprises par le protocole LDP, les routeurs LSR construisent deux tables, la LIB et la LFIB. De manière générale, la LIB contient tous les labels appris des voisins LSR, tandis que la LFIB est utilisée pour la commutation proprement dite des paquets labélisés. La table LFIB est un sous-ensemble de la base LIB.

Exemple

- Réception du label 17 pour les paquets à destination du 10.0.0.0/8
- Génération d'un label 24 pour ces paquets et expédition de l'information aux autres routeurs
- Insertion de l'information dans la LFIB

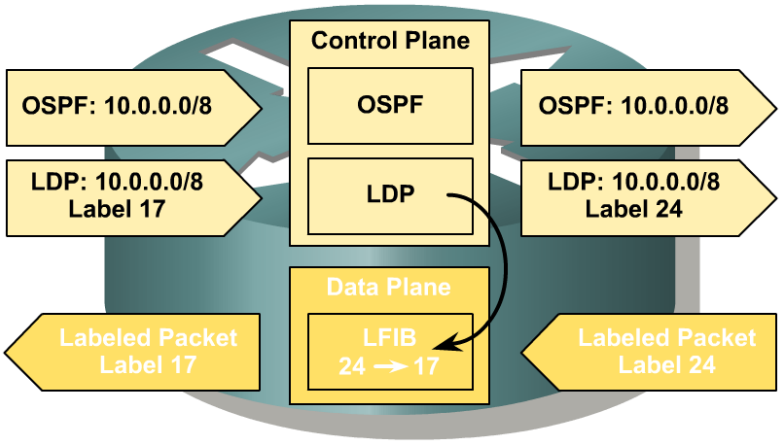

Figure III-3 : structure fonctionnelle du routeur

III.2.3 Structures de données des labels

Le protocole MPLS utilise les trois structures de données LIB, LFIB et FIB pour acheminer les paquets :

III.2.3.1 LIB (Label Information Base)

C'est la première table construite par le routeur MPLS est la table LIB, c'est la base de donnée utilisée par LDP. Elle contient pour chaque sous-réseau IP la liste des labels affectés par les LSR voisins. Il est possible de connaître les labels affectés à un sous-réseau par chaque LSR voisin et donc elle contient tous les chemins possibles pour atteindre la destination [01].

III.2.3.2 FIB (Forwarding Information Base)

Appartient au plan de donnée, c'est la base de donnée utilisé pour acheminer les paquets non labellisés (routage IP classique). Un paquet à acheminer est labellisé si le label du saut suivant est valable pour le réseau de destination IP [01].

III.2.3.3 LFIB (Label Forwarding Information Base)

A partir de la table LIB et de la table de routage IP du réseau interne au backbone, chaque routeur LSR construit une table LFIB (Label Forwarding Information Base), qui sera utilisée pour commuter les paquets labélisés. Dans le réseau MPLS, chaque sous-réseau IP est appris par un protocole IGP, qui détermine le prochain saut (le next-hop) pour l'atteindre. Donc pour atteindre un sous-réseau IP donné, le routeur LSR choisit le label d'entrée de la table LIB qui correspond à ce sous-réseau IP et sélectionne comme label de sortie le label annoncé par le routeur voisin (correspondant au next hop) déterminé par le protocole IGP (plus court chemin) [01].

III.2.4 Construction des structures de données

La construction des structures de données effectuées par chaque routeur LSR doivent suivre les étapes suivantes :

- Élaboration des tables de routages par les protocoles de routage.
- Allocation indépendamment d'un label à chaque destination dans sa table de routage par le LSR.
- Enregistrement dans la LIB des labels alloués ayant une signification locale.
- Enregistrement dans la table « LFIB » avec l'action à effectuer de ces labels et leur prochain saut.
- Envoi par le LSR les informations sur sa « LIB » à ces voisins.
- Enregistrement par chaque LSR des informations reçues dans sa « LIB ».
- Enregistrement des informations reçues des prochains sauts dans la « FIB ».

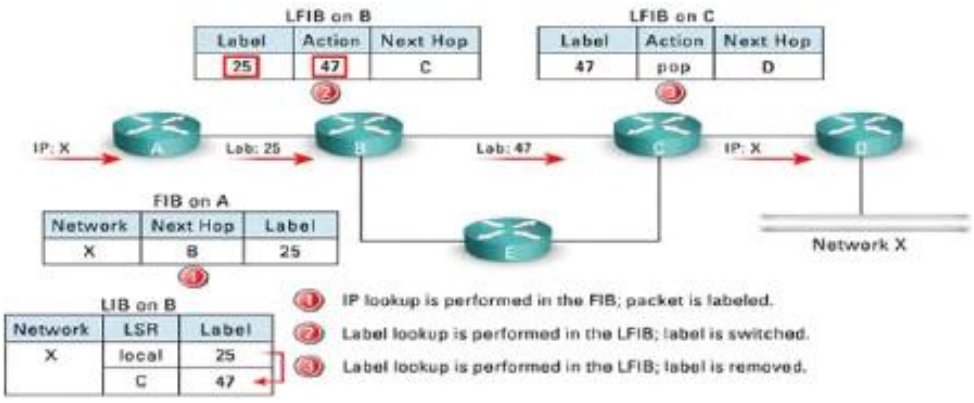

Figure III-4: Utilisation des structures de données pour l'acheminement

III.3 Paradigme de la commutation dans MPLS

Un LSR peut effectuer l'un des trois scénarios d'acheminement d'un paquet :

- Le paquet arrivant à l'entrée du domaine MPLS (I-LSR) ne contient que les adresses IP, l'acheminement est basé sur la table FIB en ajoutant « Push »un Label.
- Le paquet arrivant a la sortie du domaine MPLS (E-LSR) contient que des adresses IP, l'acheminement est basé sur la FIB sans l'utilisation d'un label (routage IP).
- Le paquet arrivant contient un label, dans ce cas l'acheminement sera basé sur la table LFIB et le label sera échangé (Swapping).

La figure ci-dessous représenté le Paradigme de commutation dans MPLS [01].

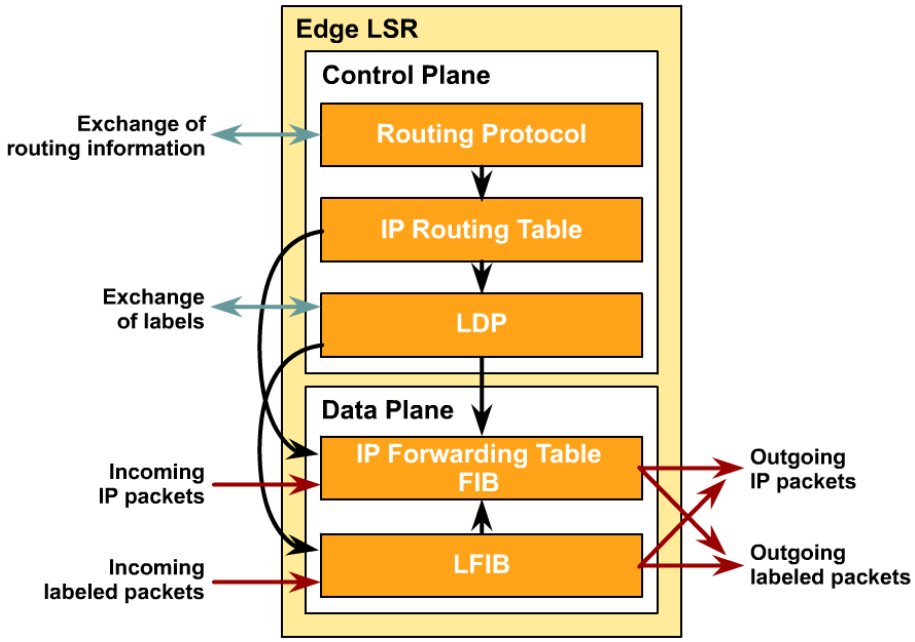

Figure III-5 : Paradigme de commutation dans MPLS

III.4 Les labels

III.4.1 L'encapsulation Label MPLS dans différentes technologies

Le protocole MPLS, basé sur le paradigme de changement de label, dérive directement de l'expérience acquise avec l'ATM (étiquettes VPI/VCI). Ce mécanisme est aussi similaire à celui de Frame Relay ou de liaisons PPP. L'idée de MPLS est de rajouter un label de couche 2 aux paquets IP dans les routeurs frontières d'entrée du réseau.

Un label a une signification d'identificateur local d'une FEC entre 2 LSR adjacents et mappe le flux de trafic entre le LSR amont et le LSR aval. La Figure III-6, illustre la mise en œuvre des

labels dans différentes technologies. Ainsi, MPLS fonctionne indépendamment des protocoles de niveau 2 (ATM, FR, etc.) et des protocoles de niveau 3 (IP, etc.). C'est ce qui lui vaut son nom de "MultiProtocol Label Switching"[02].

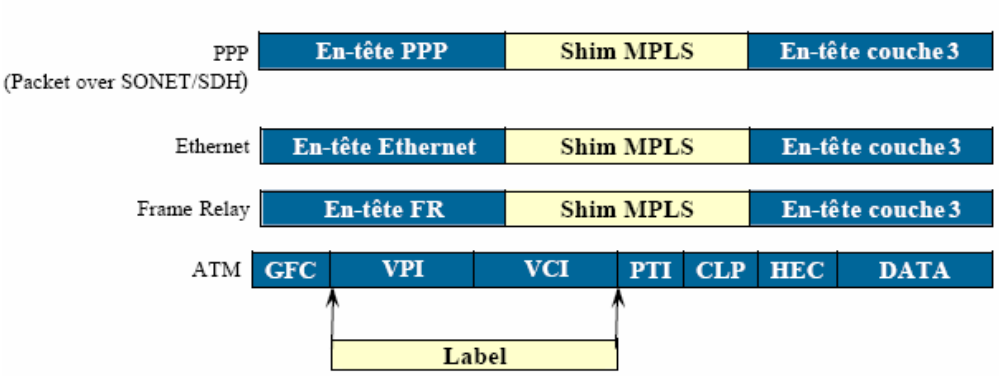

Figure III-6 : L'encapsulation MPLS dans différentes technologies

III.4.2 L'entête MPLS

L'entête MPLS se situe entre les entêtes des couches 2 et 3, où l'entête de la couche 2 est celle du protocole de liaison et celle de la couche 3 est l'entête IP. L'entête est composé de quatre champs :

- Le champ Label (20 bits), valeur représentant le label, il fournit les informations sur le protocole de la couche 2 et d'autres informations pour transférer les données.
- Le champ Exp ou CoS (3 bits) pour la classe de service (Class of Service).
- Un bit Stack pour supporter un label hiérarchique (empilement de labels).
- Et un champ TTL (Time To Live) pour limiter la durée de vie du paquet (8 bits). Ce champ TTL est le même que pour IP.

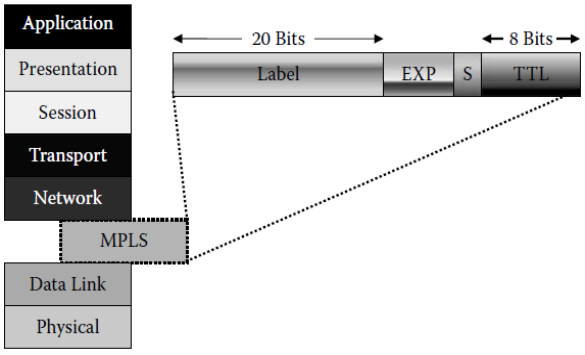

Figure III-7 : Figure Entête MPLS

III.4.3 Pile de labels (Label Stack)

Comme on l'a déjà évoqué, il est commun d'avoir plus qu'un label attaché à un paquet. Ce concept s'appelle empilement de label. L'empilement de label permet en particulier d'associer plusieurs contrats de service à un flux au cours de sa traversée du réseau MPLS.
Les LSR de frontière de réseau auront donc la responsabilité de pousser ou tirer la pile de labels pour désigner le niveau d'utilisation courant de label.
Les applications suivantes l'exigent :

- MPLS VPN : MP-BGP (MultiProtocol Border Gateway Protocol) est utilisé pour propagé un label secondaire en addition à celui propagé par TDP ou LDP.
- MPLS TE : MPLS TE utilise RSVP TE (Ressource Reservation Protocol TE) pour établir un tunnel LSP (Label Switched Path). RSVP TE propage aussi un label en addition de celui propagé par TDP ou LDP.

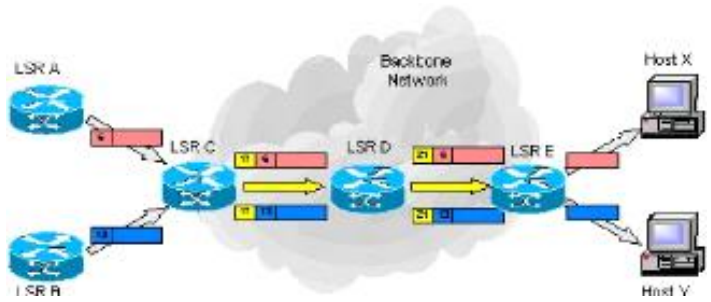

Figure III-8 : Pile de labels

III.5 Distribution des labels

Les LSR se basent sur l'information de label pour commuter les paquets au travers du cœur de réseau MPLS. Chaque routeur, lorsqu'il reçoit un paquet taggué, utilise le label pour déterminer l'interface et le label de sortie. Il est donc nécessaire de propager les informations sur ces labels à tous les LSR. Pour cela, suivant le type d'architecture utilisée, différents protocoles sont employés pour l'échange de labels entre LSR, en voici quelques exemples :

- TDP/LDP (Tag/Label Distribution Protocol) : mapping des adresses IP unicast.
- CR-LDP, RSVP-TE : utilisés en Traffic Engineering pour établir des LSP en fonction de critères de ressources et d'utilisation des liens.
- MP-BGP (MultiProtocol Border Gateway Protocol pour l'échange de routes VPN.

Chaque paquet MPLS est susceptible de transporter plusieurs labels, formant ainsi une pile de labels, qui sont empilés et dépilés par les LSR. Cela permet entre autre d'interconnecter plusieurs réseaux, chacun possédant son propre mécanisme de distribution des labels [05].

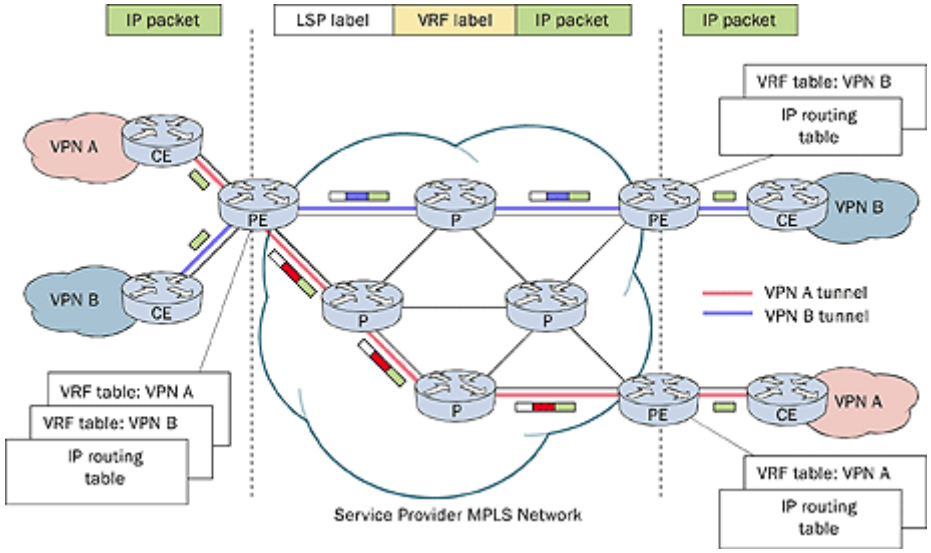

Figure III-9 : Liens MPLS/VPN

Lorsqu'un LSR commute un paquet, seul le premier label est traité. Cette possibilité d'empiler des labels, désignée sous le terme de Label Stacking, est aussi utilisée par le Traffic Engineering et MPLS / VPN**.**

III.5.1 Le protocole LDP

Le protocole LDP est un protocole de signalisation (plus précisément, de distribution des labels) héritier du protocole propriétaire TDP (Tag Distribution Protocol). Pour en décrire le fonctionnement, rappelons la notion de l'arbre de plus court chemin : pour un préfixe d'adresse, le protocole de routage classique définit implicitement un arbre de plus court chemin, arbre ayant pour racine le LSR de sortie (celui qui a annoncé le préfixe) et pour feuilles les différents routeurs d'entrée. Le routeur de sortie va annoncer le préfixe à ses voisins, tout y en associant un label. Les messages de signalisation vont « monter » jusqu'aux routeurs d'entrée, permettant à chaque LSR intermédiaire d'associer un label au préfixe.

III.5.2 Le protocole CR-LDP

CR-LDP est une version étendue de LDP, où CR correspond à la notion de « routage basé sur les contraintes des LSP ». Tout comme LDP, CR-LDP utilise des sessions TCP entre les LSR, au cours desquelles il envoie les messages de distribution des étiquettes. Ceci permet en particulier à CR-LDP d'assurer une distribution fiable des messages de contrôle [05].
Les échanges d'informations nécessaires à l'établissement des LSP utilisant CR-LDP sont décrits dans la figure suivante :

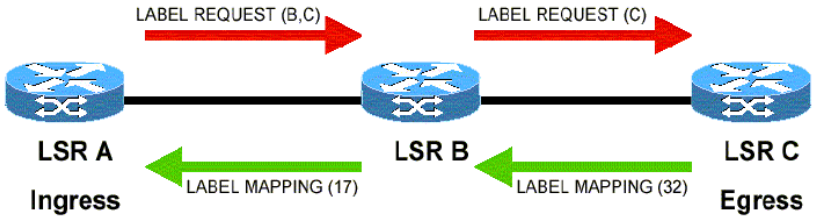

Figure III-10 : Etablissement d'un LSP par CR-LDP

III.5.3 Le protocole RSVP – TE

Le protocole RSVP utilisait initialement un échange de messages pour réserver les ressources des flux IP à travers un réseau. Une version étendue de ce protocole RSVP-TE, en particulier pour permettre les tunnels de LSP, autorise actuellement RSVP à être utilisé pour distribuer des étiquettes MPLS.

RSVP est un protocole complètement séparé de la couche IP, qui utilise des datagrammes IP ou UDP (User Datagram Protocol) pour communiquer entre LSR. RSVP ne requiert pas la maintenance nécessaire aux connexions TCP, mais doit néanmoins être capable de faire face à la perte de messages de contrôle [05].

Les échanges d'informations nécessaires à l'établissement de LSP permettant les tunnels de LSP et utilisant RSVP sont décrits dans la figure suivante :

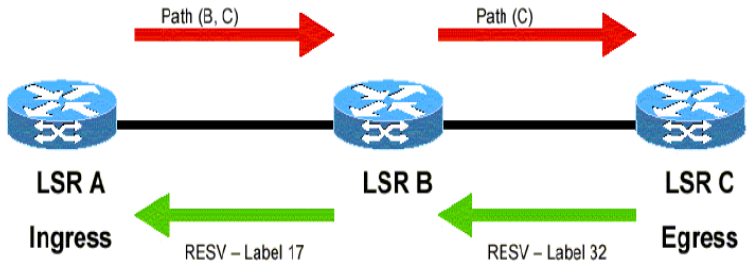

Figure III-11 : Etablissement LSP par RSVP-TE

III.6 Les Applications De La Technologie MPLS

La motivation primaire de MPLS était d'accroître la vitesse de traitement des paquets au niveau des nœuds intermédiaires. Les routeurs actuels sont équipés avec des circuits et des algorithmes permettant un acheminement (forwarding) des paquets extrêmement rapide.
Donc, traiter des paquets sur la base de label de 20 bits de MPLS n'est plus significativement rapide par rapport à traiter des paquets sur la base d'adresse de 32 bits de IP [02].

Aujourd'hui, les motivations réelles pour déployer des solutions MPLS sont les applications que MPLS permet, et qui étaient très difficiles voire impossibles à mettre en œuvre avec IP traditionnel. Ces applications sont très importantes pour les opérateurs et les ISP (Internet Service Provider), tout simplement parce qu'elles peuvent être vendues.

Il existe aujourd'hui quatre applications majeures de MPLS. Ces applications supposent la mise en œuvre de composants adaptés aux fonctionnalités recherchées. L'implémentation de MPLS sera donc différente en fonction des objectifs recherchés. Cela se traduit principalement par une façon différente d'assigner et de distribuer les labels (Classification, protocoles de distribution de labels). Le principe d'acheminement des paquets fondé sur l'exploitation des labels étant le mécanisme de base commun à toutes les approches [02].

Les principales applications de MPLS concernent :

- Any Transport over MPLS (AToM).
- Le support des réseaux privés virtuels (MPLS VPN, Virtual Private Network).
- Le support de la qualité de service (MPLS QoS).
- Le Traffic Engineering (MPLS TE).

III.6.1 Any Transport over MPLS (AToM)

Ce service traduit l'indépendance de MPLS vis-à-vis des protocoles de couches 2 et 3. AToM est une application qui facilite le transport du trafic de couche 2, tel que Frame Relay, Ethernet, PPP et ATM, à travers un nuage MPLS [02].

III.6.2 Le support des réseaux privés virtuels (MPLS VPN)

Un réseau privé virtuel (VPN) simule le fonctionnement d'un réseau étendu (WAN) privé sur un réseau public comme Internet. Afin d'offrir un service VPN fiable à ses clients, un opérateur ou un ISP doit alors résoudre deux problématiques essentielles.

- Assurer la confidentialité des données transportées.
- Prendre en charge des plans d'adressage privé, fréquemment identiques.

La construction de VPN repose alors sur les fonctionnalités suivantes :

- Systèmes de pare-feu (Firewall) pour protéger chaque site client et permettre une interface sécurisée avec Internet.
- Système d'authentification pour vérifier que chaque site client échange des informations avec un site distant valide ;
- Système de cryptage pour empêcher l'examen ou la manipulation des données lors du transport sur Internet.
- Tunneling pour permettre un service de transport multi-protocole et l'utilisation de plans d'adressage privés.

MPLS permet de résoudre efficacement la fonctionnalité de tunneling, dans la mesure où l'acheminement des paquets n'est pas réalisé sur l'adresse de destination du paquet IP, mais sur la valeur du label assigné au paquet. Ainsi, un ISP peut mettre en place un VPN, en déployant un ensemble de LSP pour permettre la connectivité entre différents sites du VPN d'un client donné. Chaque site du VPN indique à l'ISP l'ensemble des préfixes (adresses) joignables sur le site local. Le système de routage de l'ISP communique alors cette information vers les autres sites distants du même VPN, à l'aide du protocole de distribution de labels. En effet, l'utilisation d'identifiant de VPN permet à un même système de routage de supporter multiples VPN, avec un espace d'adressage éventuellement identique. Ainsi, chaque LER place le trafic en provenance d'un site dans un LSP fondé sur une combinaison de l'adresse de destination du paquet et l'appartenance à un VPN donné [02].

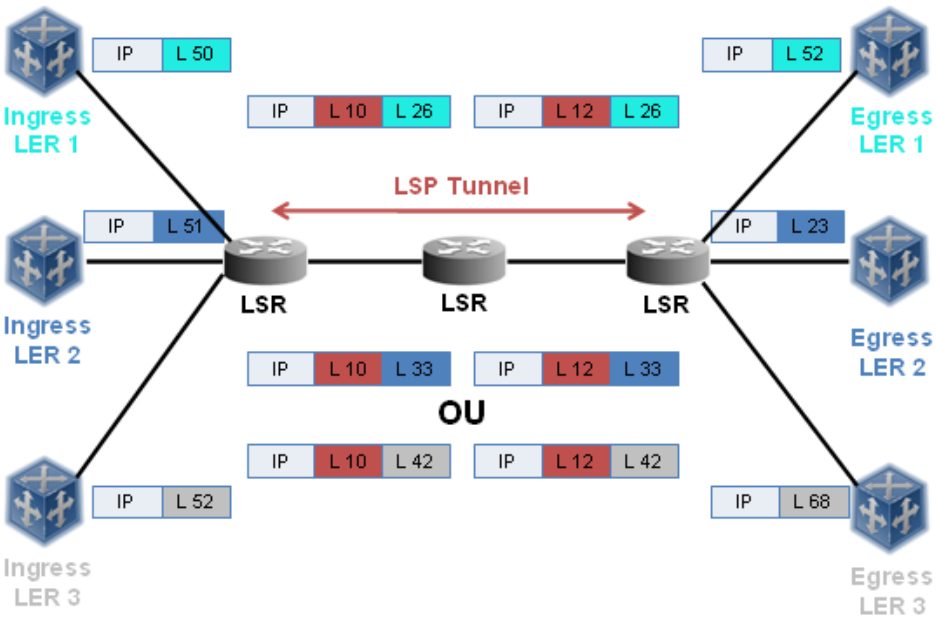

Figure III-12 : MPLS VPN

Il existe une autre approche permettant de mettre en œuvre des VPN sur les réseaux IP : IPSec, IPSec privilégie la sécurisation des flux d'information par encryptage des données, alors que MPLS se concentre plutôt sur la gestion de la qualité de service et la priorité des flux.

Le problème de sécurité dans MPLS VPN est minimal dans le cas où le réseau est propriétaire (non Internet). Cependant, si cette garantie n'est pas suffisante, il existe des solutions qui permettent d'utiliser en même temps MPLS et IPSec et ainsi construire des VPN disposant des avantages des deux approches en même temps : la souplesse de MPLS et la sécurisation de l'IPSec.

III.6.3 Le support de la qualité de service (MPLS QoS)

Avec la technologie MPLS, la QoS est un élément crucial pour un réseau d'opérateur. En effet, l'opérateur doit pouvoir garantir à ses clients le transport de leurs flux en garantissant différentes contraintes, La qualité de service se décline principalement en quatre paramètres : débit, délai, gigue et perte.

- Le débit représente les ressources de transmission occupées par un flot. Un flot est un ensemble de paquets résultant d'une application utilisatrice.
- Le délai correspond au temps de transfert de bout en bout d'un paquet.
- La gigue correspond aux variations de latence des paquets. La gigue provient essentiellement des variations de trafic sur les liens de sorties des routeurs.

- Des pertes de paquets peuvent être dues à des erreurs d'intégrité sur les données ou des rejets de paquets en cas de congestion.

Le support de la QoS peut être mise en œuvre de deux façons sur MPLS [02] :

- Diffserv (Differentiated Services) : Les trafics sur un même LSP peuvent se voir affecter à différentes files d'attente dans les routeurs LSR, selon la valeur du champ EXP de l'en-tête MPLS.
- L'utilisation du Traffic Engineering.

III.6.3.1 La differentiation des services (MPLS Diffserv)

Le modèle de différenciation des services semble être plus adéquat pour les réseaux multiservices tels que l'Internet. Ce modèle signifie en d'autres termes donner la priorité à une classe de service au dépend d'une autre classe au moment de congestion. Le modèle DiffServ (Differentiated Services) définit une approche totalement différente en comparaison avec le modèle IntServ (Integrated Services). Il ne nécessite ni une réservation de bout en bout ni signalisation. Il permet d'affecter chaque paquet à une classe de service. La complexité est reléguée dans les extrémités du réseau. Les services différenciés de l'architecture DiffServ permettent de diminuer substantiellement les informations d'état que chaque nœud du réseau doit mémoriser.

Dans l'architecture DiffServ, le traitement différencié des paquets s'appuie sur 3 opérations fondamentales :

- La classification des flux en classes de services.
- L'introduction de priorités au sein des classes (Scheduling).
- La gestion du trafic dans une classe donnée (Queue management).

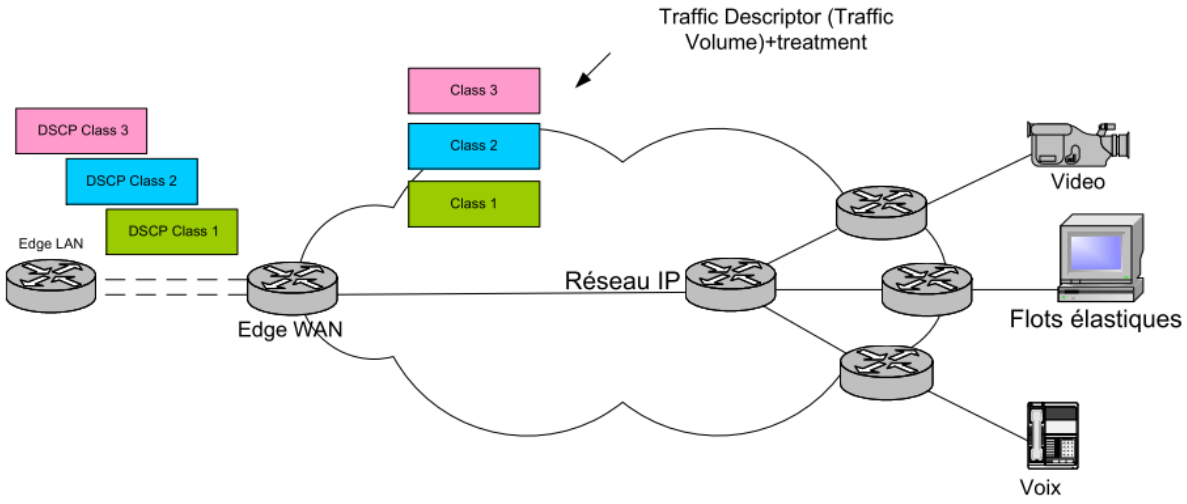

Figure III-13 : Classification, marquage et conditionnement du trafic dans le domaine DiffServ

Les paquets DiffServ sont marqués à l'entrée du réseau et les routeurs décident en fonction de cette étiquette de la file d'attente dans laquelle les paquets vont être placés.

Cette architecture convient à des réseaux pour lesquels il n'est pas raisonnable d'envisager une signalisation flux par flux. Elle ne considère donc que des agrégats de flux pour lesquels une signalisation avec réservation de ressources peut être envisagée.

En fait un routeur de cœur ne conserve pas d'état pour un flux ou un agrégat donné, mais traite tous les paquets d'une classe donnée de la même manière. Les données sont identifiées grâce à un marquage dans le champ ToS (Type of Service, champ spécifique réservé dans l'en-tête IP de 8 bits), qui fixe les priorités.

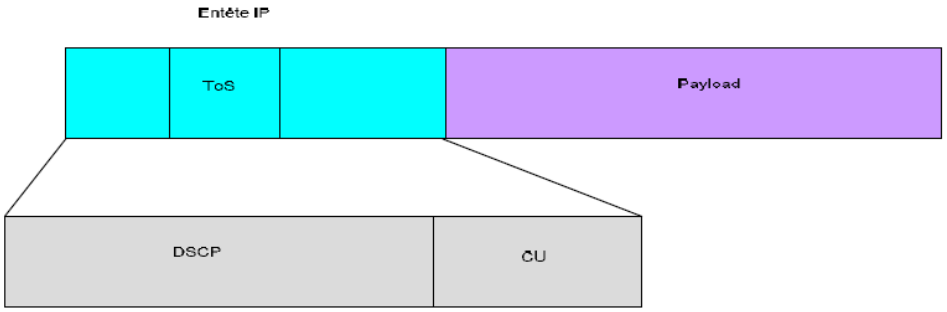

Figure III-14 : Insertion du champ DSCP

Au contraire du modèle Intserv qui traite indépendamment chaque flot, les routeurs DiffServ traitent les paquets en fonction de la classe codée dans l'entête IP (champ DS) selon un comportement spécifique : le PHB (Per Hop Behaviour).

Chaque ensemble de paquets défini par une classe reçoit alors un même traitement et chaque classe est codée par un DSCP (DiffServ Code Point). Un PHB est défini par les priorités qu'il a sur les ressources par rapport à d'autres PHB.

Diffserv définit quatre PHB ou classes de service :

- ✓ Best Effort (priorité basse) :
- ✓ Expedited Forwarding (EF) ou Premium Service (RFC 2598) : correspondant à la priorité maximale et a pour but de garantir une bande passante avec des taux de perte, de délai et de gigue faible en réalisant le transfert de flux à fortes contraintes temporelles comme la téléphonie sur IP par exemple.
- ✓ Assured Forwarding (AF) (RFC 2597) : regroupant plusieurs PHB garantissant un acheminement de paquets IP avec une haute probabilité sans tenir compte des délais.
- ✓ Default Forwarding (DF), utilisé uniquement pour les flux Internet qui ne nécessitent pas un trafic en temps réel.

Cette notion de PHB permet de construire une variété de services différenciés. Les PHB sont mis en œuvre par les constructeurs dans les routeurs en utilisant des mécanismes de gestion de files d'attente (Custom Queuing, Weighted Fair Queuing, ...) et de régulation de flux.

- **Best Effort**

PHB par défaut et dont le DSCP vaut 000000. Le principe du Best Effort se traduit par une simplification à l'extrême des équipements d'interconnexion. Quand la mémoire d'un routeur est saturée, les paquets sont rejetés. Le principe de bout en bout de l'Internet est aussi adopté pour le contrôle de flux grâce à différents algorithmes comme le Congestion Avoidance introduit dans TCP.

Les principaux inconvénients de cette politique de contrôle de flux sont un trafic en dents de scie composé de phases où le débit augmente puis est réduit brutalement et une absence de garantie à long terme.

- **Expedited Forwarding**

La classe Expedited Forwarding correspond à la valeur 101110 pour le DSCP et l'objectif est de fournir un service de transfert équivalent à une ligne virtuelle dédiée à travers le réseau d'un opérateur.

Le contrat porte sur un débit constant. Les paquets excédentaires sont lissés ou rejetés à l'entrée pour toujours rester conforme au contrat. L'opérateur s'engage à traiter ce trafic prioritairement. Pour que le service soit performant, il faut qu'il ne présente qu'une faible partie du trafic total pour qu'aucun paquet marqué EF ne soit rejeté dans le cœur du réseau.

Pour atteindre ces performances, les paquets d'un service EF ne devraient pas subir de file d'attente ou passer par des files de très petite taille et strictement prioritaires.

- **Assured Forwarding**

Le PHB AF fournit des niveaux de garantie d'acheminement des paquets. Il est constitué d'un ensemble de 4 classes de service ayant chacune 3 niveaux de rejet de paquets différents.

- (04) quatre classes de service (Il n'y a pas de priorité parmi ces classes)
- (03) priorités définissant l'ordre de rejet dans un routeur en cas de congestion.

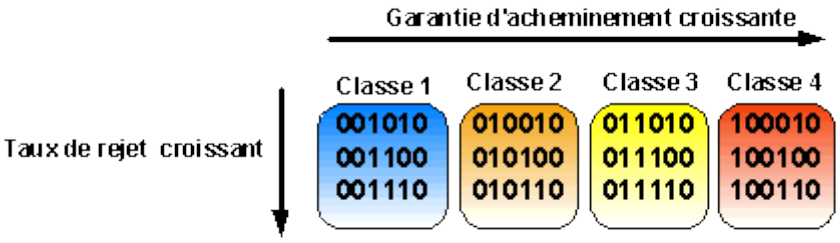

Figure III-15 : Ensemble des classes du PHB AF

Par exemple, en cas de congestion dans la classe de service 4, les paquets de valeur DSCP 100110 seront rejetés (drop) en premier lieu.

Les classes sont donc choisies par l'utilisateur et restent les mêmes tout au long du trajet dans le réseau. Tous les paquets d'un même flux appartiennent à la même classe.

A l'intérieur de chaque classe, un algorithme de rejet sélectif différencie entre 3 niveaux de priorité. En cas de congestion dans une des classes AF, les paquets de basse priorité sont rejetés en premier. La priorité peut être modifiée dans le réseau par les opérateurs en fonction du respect ou non des contrats.

AF offre différents niveaux de services :

- AF1 (AF11, AF12, AF13)
- AF2 (AF21, AF22, AF23)
- AF3 (AF31, AF32, AF33)
- AF4 (AF41, AF42, AF43)

III.6.3.2 Le Traffic Engineering (MPLS TE)

Cette application est en étroite relation avec la qualité de service, puisque son résultat immédiat est l'amélioration de paramètres tels que le délai ou la gigue dans le réseau. Elle est tout de même considérée comme une application à part entière par la plupart des industriels. Ceci vient du fait que MPLS TE n'est pas une simple technique de réservation de ressources pour les applications réseau. C'est un concept plus global qui se veut être une solution qui vise à augmenter les performances générales du réseau en jouant sur la répartition équilibrée des charges (trafics) dans le réseau pour ainsi avoir une utilisation plus optimale des liens [02].

III.7 EVOLUTIONS MPLS

III.7.1 GMPLS

Une première extension du MPLS est le Generalized MPLS. Le concept de cette dernière technologie est d'étendre la commutation aux réseaux optiques. Le label, en plus de pouvoir être une valeur numérique peut alors être mappé par une fibre, une longueur d'onde et bien d'autres paramètres. Le GMPLS met en place une hiérarchie dans les différents supports de réseaux optiques. GMPLS permet donc de transporter les données sur un ensemble de réseaux hétérogènes en encapsulant les paquets successivement à chaque entrée dans un nouveau type de réseau. Ainsi, il est possible d'avoir plusieurs niveaux d'encapsulations selon le nombre de réseaux traversés, le label correspond à ce réseau étant conservé jusqu'à la sortie du réseau. GMPLS reprend le plan de contrôle de MPLS en l'étendant pour prendre en compte les contraintes liées aux réseaux optiques. En effet, GMPLS va rajouter une brique de gestion des liens à l'architecture MPLS. Cette brique comprend un ensemble de procédures utilisées pour gérer les canaux et les erreurs rencontrées sur ceux-ci [04].

III.7.2 VPLS

VPLS qui veut dire Virtual Private LAN Services, définit un service de VPN au niveau de la couche 2 (service Ethernet) multipoint-à-multipoint qui peut être indifféremment délivré au niveau d'une infrastructure métropolitaine ou sur des réseaux longue distance.
Ce service apporte une connectivité entre plusieurs sites comme si ces sites étaient reliés par un même LAN Ethernet. [04]

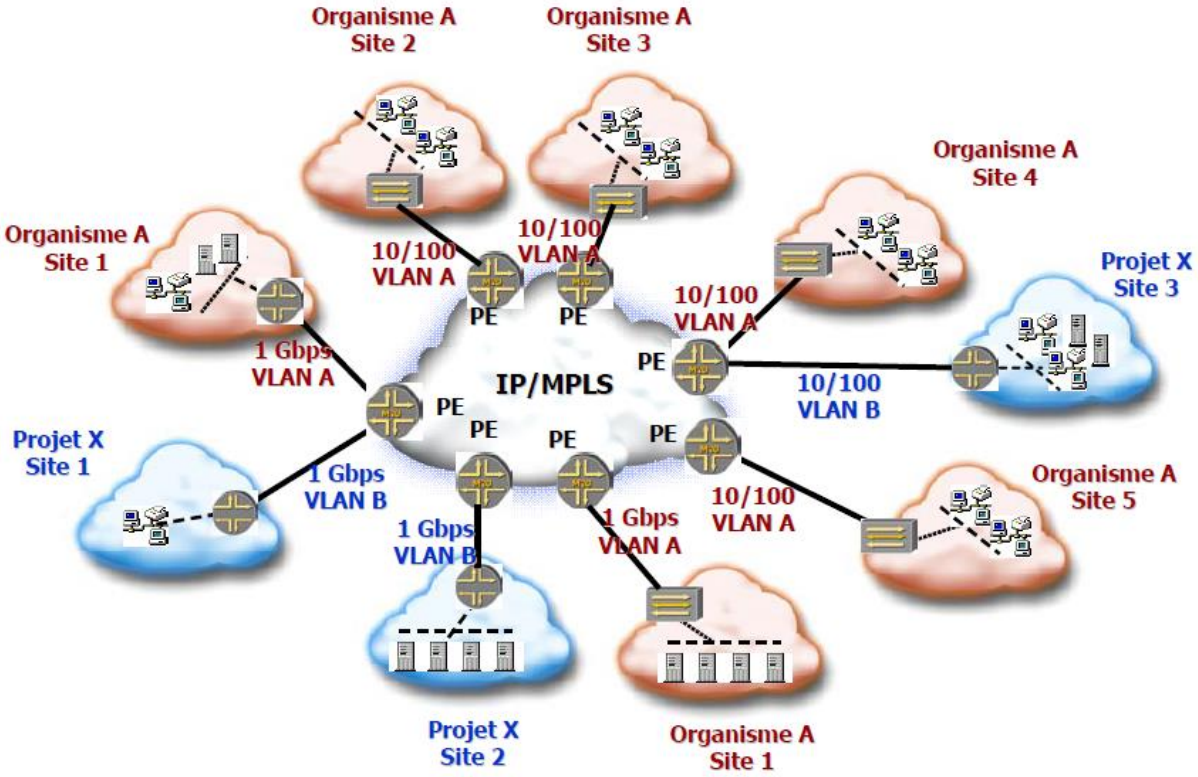

Figure III-16 : VPLS délivre un service Ethernet multipoint-à-multipoint [03]

Qui peut s'étendre à plus d'une zone métropolitaine Contrastant avec l'offre de service Ethernet multipoint-à-multipoint apportés par une infrastructure d'opérateur basée sur des commutateurs Ethernet, VPLS utilise une infrastructure IP/MPLS.
Du point de vue de l'opérateur, l'utilisation des protocoles de routage IP/MPLS au lieu d'une technologie Ethernet basée sur le Spanning Tree Protocol, ainsi que l'utilisation des labels (étiquettes) MPLS au lieu des identités VLAN, apportent à l'infrastructure de l'opérateur une souplesse et une capacité de déploiement de services Métro Ethernet à grande échelle.

Ce nouveau service permet aux réseaux de Recherche et Enseignement d'envisager une approche innovante pour rapprocher les chercheurs et enseignants souvent dispersés sur des sites distants, parfois à l'échelle nationale. Le réseau peut devenir un outil étendant les capacités du LAN traditionnel Ethernet, en s'affranchissant de la distance et du nombre de réseaux

intermédiaires (domaines IP). Ainsi il apporte une synergie supplémentaire favorisant le partage et l'échange des ressources et connaissances au niveau régional, national, et au-delà.

III.8 SECURISATION DES RESEAUX MPLS

L'utilisation d'IP-MPLS pour le transport de services temps réel impose une excellente disponibilité du réseau. De tels services imposent notamment de pouvoir garantir un rétablissement de la connectivité en moins de 50 ms, en cas de panne de lien ou de nœud IP-MPLS.

Les méthodes actuelles de protection SDH (AIS, MS-SPRING) permettent de garantir ces temps de sécurisation. En revanche, elles sont très coûteuses en ressources car elles nécessitent de dédier des liens à la protection, et ne permettent de protéger le trafic que contre les pannes de liens, et non contre les pannes de routeur. Il est donc préférable de réaliser la sécurisation des liens et des routeurs directement au niveau de la couche IP-MPLS [05].

Les pannes des éléments du réseau peuvent être d'origines diverses. Ainsi les pannes de liens peuvent être la cause d'erreurs sur des chantiers de travaux publiques (coups de pelleteuse sur une fibre optique) ou plus simplement d'un lien débranché. En ce qui concerne les routeurs cela peut provenir d'une panne de courant. A cela il faut ajouter les pannes logicielles dues à des erreurs humaines.
Tous les éléments d'un réseau sont susceptibles de tomber en panne. Pour garantir un haut niveau de disponibilité du réseau, il faut donc prévoir ces pannes et déterminer des méthodes automatiques pour les détecter et assurer la continuité du service le plus rapidement possible [06].

Parmi les mécanismes de protection, nous allons décrire :

- le modèle de réparation globale (Backup).
- le modèle de réparation locale ou restauration d'un segment d'un LSP (Fast Reroute),
- la protection à plusieurs niveaux (Multi-Layer).

Dans le premier modèle, un nœud d'entrée est responsable d'effectuer la restauration suite à la réception du signal d'indication de panne quel que soit le lieu où la faute est intervenue le long du chemin principal. Cette méthode nécessite un chemin de Backup disjoint pour chaque chemin principal.

Dans le cas d'une réparation locale, la protection a lieu sur une partie du chemin principal et la procédure de restauration commence tout simplement par le point de défaillance. Le dernier modèle de protection à différents niveaux est applicable dans le cas de scénario avec des pannes multiples.

III.8.1 La protection de Chemin (Backup)

Le protocole MPLS permet d'établir et de maintenir automatiquement les LSPs à travers le cœur de réseau en utilisant le protocole de réservation de ressource (RSVP). Le chemin employé par un LSP dépend étroitement des ressources disponibles dans le réseau.

Pour des services fondés sur des critères de qualité de service, on peut escompter obtenir le niveau de qualité garanti en sélectionnant des routes concordant avec ces critères. MPLS est aussi employé par les opérateurs pour améliorer la tolérance aux pannes du réseau lorsqu'un incident intervient sur un nœud de réseau ou un lien. La protection des liens repose sur l'établissement d'un chemin de secours entre le routeur d'entrée et le routeur de sortie pour chaque LSP primaire créé [05].

La panne du LSP principal provoque le basculement du trafic sur le LSP de secours, pré configuré ou établi dynamiquement. Le chemin du LSP est calculé à la source de celui-ci. En cas de pannes la source du LSP détermine un nouvel itinéraire pour le LSP. Le calcul de ce chemin de Backup prévoit une utilisation optimale des ressources.

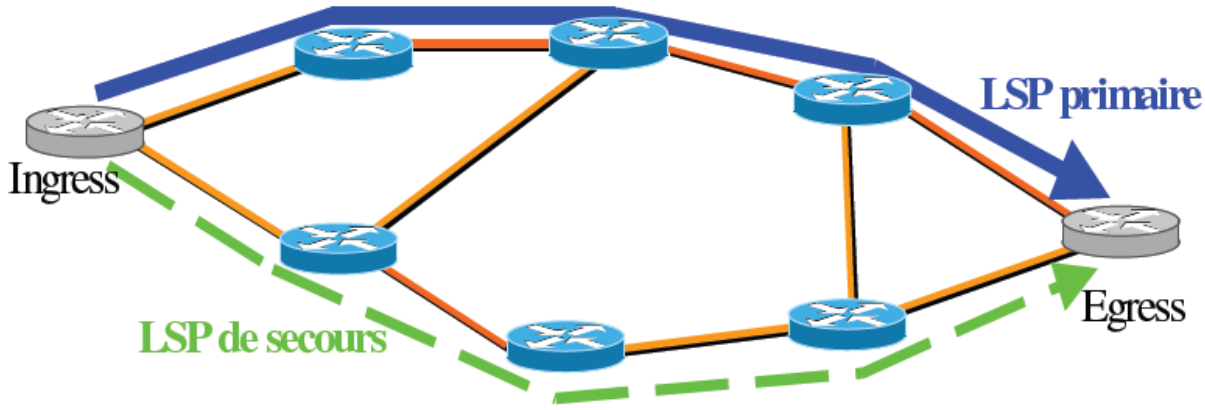

Figure III.17 : Protection du LSP par chemin de Backup

Le LSP de Backup est le mode de protection par défaut de MPLS-TE. Il faut distinguer deux sous modes pour ce type de protection :

- Le mode « Head-End Backup » ou le Backup n'est ni calculé ni signalé donc tout se fait après panne et durant ce laps de temps dû aux délais de transmission des messages, un nombre important de paquets vont être perdus.
- Le mode « Stand-by LSP » est une extension de RSVP-TE où le Backup est signalé et prêt à l'emploi l'inconvénient dans ce cas est la sur-réservation de bande passante

  .

Un LSP de secours pré-alloué peut être utilisé pour protéger plusieurs LSPs primaires, ce qui permet d'économiser des ressources. Dans ce cas, on considère que des pannes simultanées affectant plusieurs LSPs partageant un même LSP de secours sont très peu probables.

Il faut également bien voir que tous les LSPs n'ont pas besoin d'être protégés par ce type de technique qui nécessite la pré-allocation des ressources. Cela peut faire l'objet d'un contrat entre l'opérateur et ses clients : protection totale du LSP, protection partagée avec d'autres LSPs, ou bien pas de protection du tout [05].

III.8.2 La protection par reroutage local (Fast-Reroute)

MPLS peut aussi assurer la protection des liens et des routeurs localement en utilisant des techniques de reroutage rapide (Fast Reroute). Il devient ainsi possible d'approcher le délai de 50 ms qu'offre la reconfiguration de liens dans un réseau SDH classique.

C'est une méthode qui permet d'assurer la continuité du service en cas de panne d'un lien ou d'un nœud avec une interruption très faible du service. Le mode Fast Reroute qui est une extension de RSVP-TE assure la protection de liens (et de nœud) pour un LSP. Cela permet le reroutage local et rapide des trafics transportés par le LSP à travers un chemin contournant la panne.

La décision de reroutage est une décision locale complètement gérée par le routeur source du lien en panne. Ce dernier établit un LSP de contournement quand il reçoit une notification de panne par l'IGP ou par RSVP.

Le Fast Reroute permet de minimiser la perte de paquets due à la panne d'un lien (ou d'un nœud). Cela permet aussi de donner au routeur source du LSP le temps nécessaire à l'établissement du chemin de Backup optimal [05].

III.8.2.1 Etapes d'un Fast Reroute de lien

Nous allons décrire les différentes étapes d'un Fast Reroute de lien à travers l'exemple suivant : il s'agit d'un cœur de réseau où l'on va mettre le lien R2-R3 en panne. Le LSP entre R1 et R9 défini par les labels (37, 14, pop) utilise le lien R2-R3 et va donc être Fast Rerouté Afin de protéger le lien R2-R3 le routeur R2 va créer un LSP de Backup (dans ce cas ce LSP passera par R6 et R7 et sera définit par la suite de labels (17, 22, pop)) La décision de reroutage des paquets revient entièrement au routeur R2. Quand celui-ci reçoit la notification de la panne du lien R2-R3 il déroute les paquets sur le LSP de Fast Reroute. Cela est fait de façon très simple en insérant le label 17 aux paquets IP destiné au routeur R3 (ceci bien sur après l'opération de swap des deux labels 37 et 14).

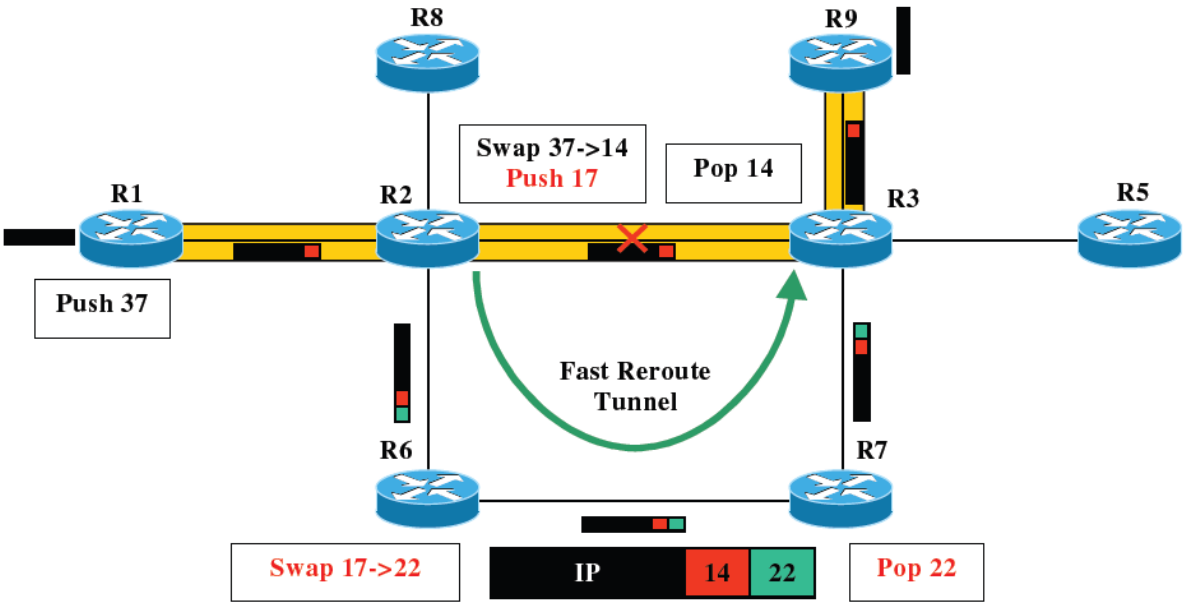

Figure III-18: Fast Reroute du lien R2--R3

III.8.2.2 Etapes d'un Fast Reroute de Nœud

Le Fast Reroute de nœuds est la généralisation du cas panne de liens. Il s'agit de créer des LSPs de détour pour tout couple de nœuds périphériques au nœud en panne et véhiculant des trafics MPLS.

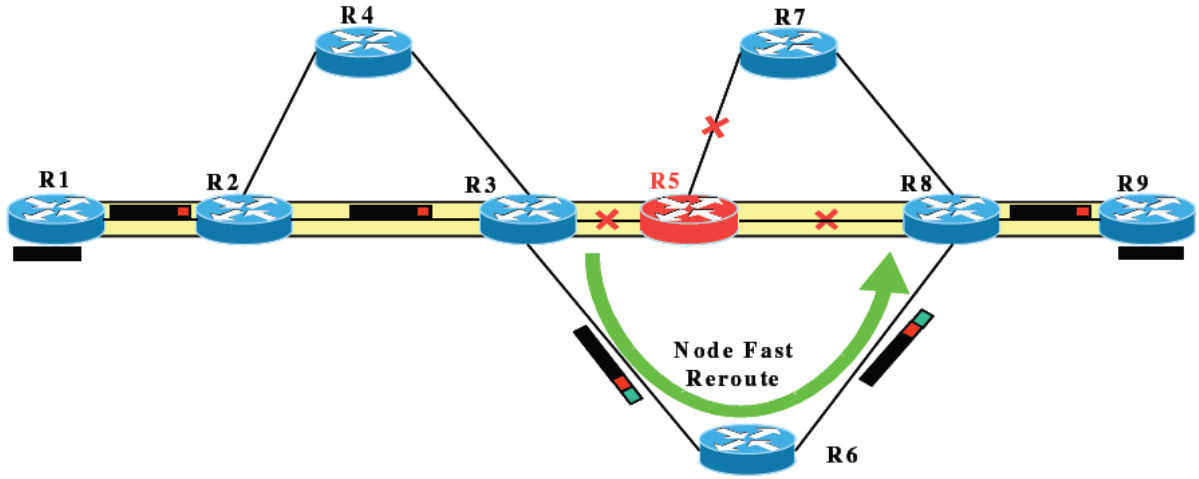

Figure III-19 : Fast Reroute du Nœud R5

La Figure III-19 illustre le cas de la panne du routeur R5 il faudra considérer les couples suivant : (R3, R8), (R3, R7), (R8, R3), (R7, R3), (R7, R8), (R8, R7).
Une fois les couples déterminés on ne garde que ceux qui véhiculent des LSPs. Dans le cas présent on ne garde que le couple (R3, R8).

Les étapes suivantes utilisent le même principe que le Fast Reroute de lien. Le routeur R3 va établir un LSP entre R3 et R8 (évitant le nœud R5). Le nœud R3 déroutera ainsi tous les paquets qui devaient transiter par le nœud R5 vers le LSP de détour en ajoutant un niveau de label [05].

Intérêts de l'approche Fast Reroute

La solution Fast Reroute apporte deux gains notables au réseau IP :

- Une fiabilité accrue pour les services IP : MPLS TE avec Fast Reroute utilisent la technologie « Fail Over Time » qui s'adapte très bien avec les techniques de restauration de lien SONET. Ce qui permet un haut degré de résilience pour les trafics IP circulant dans le cœur de réseau et des services plus robustes.
- Une scalabilité importante inhérente au design du réseau : Cela est dû au fait que le Fast Reroute utilise un mapping de tous les LSPs qui transitent par un lien Fast Rerouté vers un seul LSP de Fast Reroute. Cela permet donc de borner la croissance du nombre de LSP de Fast Reroute au nombre de liens du réseaux et non pas au nombre de LSPs.

III.8.2.3 La protection multi-niveaux (Multi-Layer)

Traditionnellement l'étude de la tolérance aux pannes se base sur l'hypothèse de la panne unique qui avec l'avènement des réseaux optiques n'est plus acceptable. En effet la pannes d'une fibre optique peut impacter plusieurs liens au niveau de la topologie IP-MPLS.

Le modèle à pannes multiples basé sur la notion de SRLG (Shared Risk Link Group) ou encore SRNG (Shared Risk Node Group) que l'on peut regrouper sous un même identifiant à savoir SRRG permet une gestion plus réaliste du problème de la résilience des réseaux actuels. Tenir compte des contraintes imposés par les SRRG dans le routage implique de trouver des chemins disjoints tel que les liens et nœuds des différents chemins n'appartiennent pas au même SRRG.

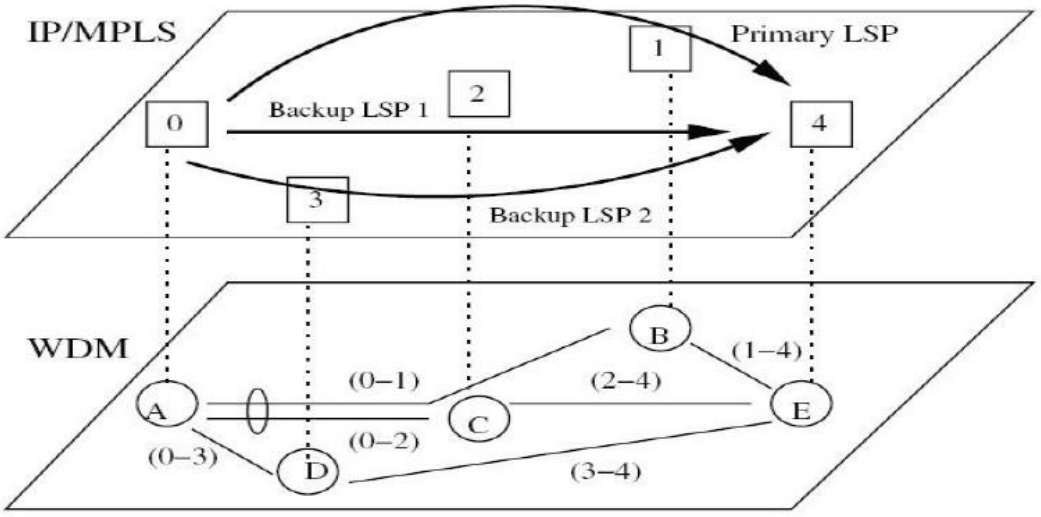

Figure III-20 : Sécurisation SRLG du LSP primaire

La Figure III-20 montre le cas d'un réseau IP/MPLS sur WDM. Le lien (0-1) est implanté au niveau WDM par le chemin (A – C – B). On peut voir que le LSP primaire emprunte le chemin (0 – 1 – 4) qui est nœud disjoint au niveau IP/MPLS avec le chemin de backup (0 – 2 – 4).
Ils partagent par contre, une ressource commune au niveau WDM qui est le lien (A – C). Le second chemin de Backup (0 – 3 – 4) est nœuds disjoints aux niveaux IP/MPLS et WDM car ils ne partagent aucune ressource commune au niveau de la topologie WDM [05].

III.9 Conclusion

Dans ce chapitre, nous avons présenté le mécanise de fonctionnement de l'architecture MPLS, ses éléments les plus importants (LSR, LSP, FEC,..), leurs déférents rôles, et les applications que MPLS permet de réaliser.

CHAPITRE IV

LES RÉSEAUX DE TRANSPORT OPTIQUES

IV.1 Introduction

Le réseau de transport est divisé en différentes couches, chacune dédiée à une fonction particulière pour assurer le transport d'un signal entre deux points différents du réseau.
Dans ce chapitre nous étudierons les différentes architectures liées à la conception de la couche physique d'un réseau de transport optique commuté. Cette couche transporte la lumière sur le lien physique (la fibre optique) en établissant une connexion entre deux points du réseau [06].

Au-dessus de cette couche se trouve une couche cliente qui peut être constituée aujourd'hui par la couche SDH (Synchronous Digital Hierarchy), suivie par les couches ATM (Asynchronous Transfer Mode) et IP (Internet Protocol), mais qui peut être aussi directement la couche IP, moyennant des adaptations de la couche physique, ces adaptations servent entre autres à envoyer des messages à la couche physique pour obtenir la connexion des requêtes provenant des couches supérieures. Les évolutions des architectures réseau permettent d'envisager une couche de transport convergente intégrant les fonctionnalités habituellement réalisées par les couches supérieures. Ainsi la recommandation (Optical Transport Network), OTN, utilisant comme couche de transport la fibre optique assure les fonctions de transport, multiplexage, brassage et supervision des signaux optiques présents dans le réseau [06].

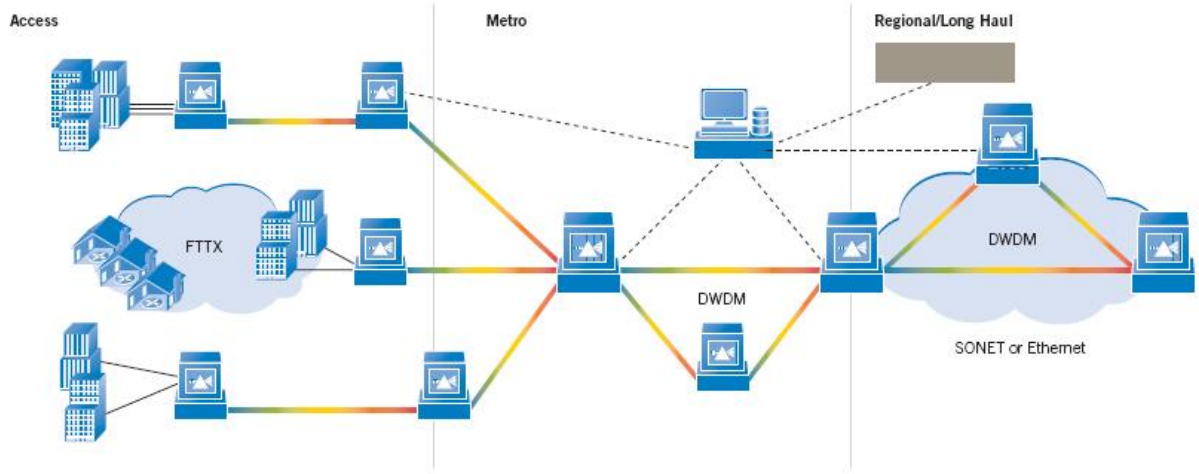

Figure IV-1 : Schématisation d'architecture d'un réseau transport optique (Cœur, métro et accès).

OTN intègre à la fois la couche physique fibre optique et aussi une sous couche d'adaptation (comme GFP, Generic Framing Procedure), La figure IV-1 représente les différentes couches d'un réseau de transport optique.

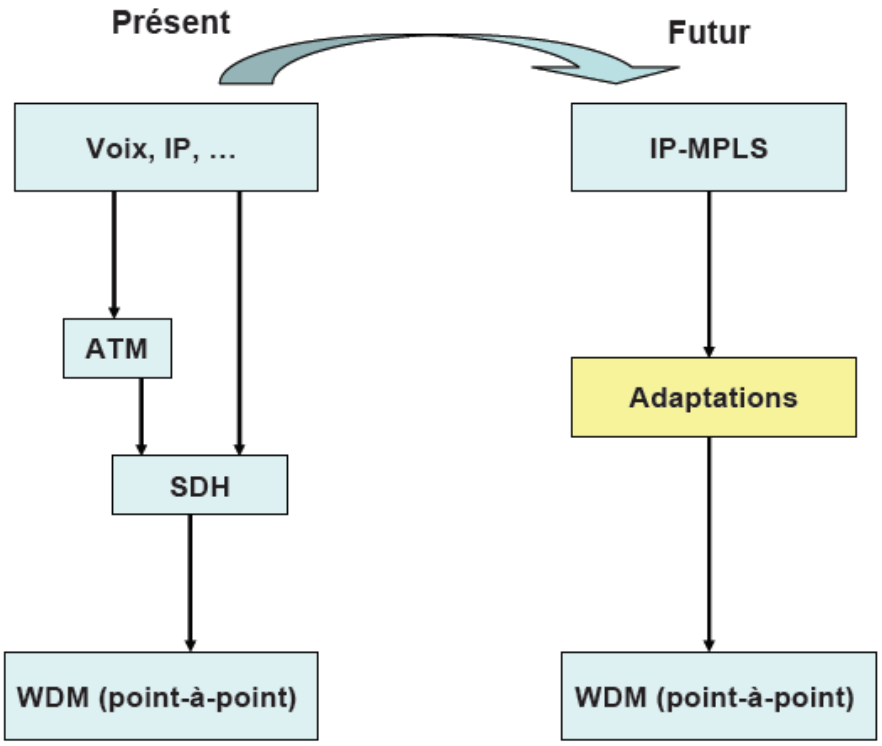

Figure IV-2 : Evolutions des couches d'un réseau de transport.

Aujourd'hui, les deux principales applications des réseaux de fibres optiques longues distances sont les applications SDH et les applications DWDM.

IV.2 Le support de transmission optique

La fibre optique est certainement l'une des plus remarquables technologies de communication du siècle dernier, et toute porte à croire qu'elle le sera encore au cours de ce siècle. Avec toujours plus d'applications large bande telles que les applications multimédia, les réseaux de télécommunication sont de plus en plus sollicités. Face à cette évolution, seules les solutions optiques permettront d'atteindre des capacités qui se mesurent en milliards de bits d'information par seconde (Gbit/s).

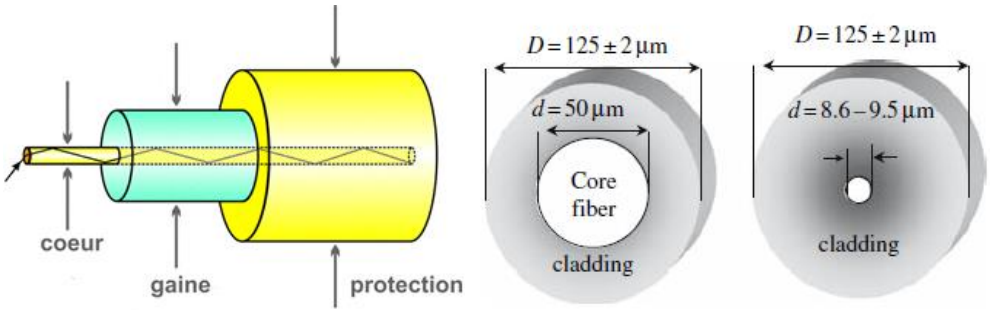

Figure IV-3 : Fibre optique (monomode/multimode)

Les **fibres optiques** peuvent être classées en deux catégories selon le diamètre de leur cœur et la longueur d'onde utilisée : les **fibres monomodes** et **multimodes.**

VI.2.1 Les fibres multimodes

Les fibres multimodes (dites MMF, pour Multi Mode Fiber), ont été les premières sur le marché. Elles ont pour caractéristiques de transporter plusieurs modes (trajets lumineux). Du fait de la dispersion modale, on constate un étalement temporel du signal proportionnel à la longueur de la fibre. En conséquence, elles sont utilisées uniquement pour des bas débits ou de courtes distances. La dispersion modale peut cependant être minimisée (à une longueur d'onde donnée) en réalisant un gradient d'indice dans le cœur de la fibre. Elles sont caractérisées par un diamètre de cœur de plusieurs dizaines à plusieurs centaines de micromètres (les cœurs en multimodes sont de 50 ou 62,5 µm pour le bas débit). Cependant les fibres les plus récentes, de type OM3, permettent d'atteindre le Gbit/s sur des distances de l'ordre du km. Les longues distances ne peuvent être couvertes que par des fibres optiques monomodes.

VI.2.2 Les fibres monomodes

Pour de plus longues distances et/ou de plus hauts débits, on préfère utiliser des fibres monomodes (dites SMF, pour Single Mode Fiber), qui sont technologiquement plus avancées car plus fines. Leur cœur très fin n'admet ainsi qu'un mode de propagation, le plus direct possible c'est-à-dire dans l'axe de la fibre. Les pertes sont donc minimes (moins de réflexion sur l'interface cœur/gaine) que cela soit pour de très hauts débits et de très longues distances. Les fibres monomodes sont de ce fait adaptées pour les lignes intercontinentales (câbles sous-marin). Ces fibres monomodes sont caractérisées par un diamètre de cœur de seulement quelques micromètres (le cœur monomode est de 9 µm pour le haut débit).

Les bandes de transmission sont classées aujourd'hui par l'UIT-T selon la terminologie suivante :

- Bande O : de 1260 à 1360 nm (original)
- Bande E : de 1360 à 1460 nm (extended) – position du « pic d'eau »
- Bande S: de 1460 à 1530 nm (short wavelength)
- Bande C : de 1530 à 1565 nm (conventional)
- Bande L : de 1565 à 1625 nm (long)
- Bande U : de 1625 à 1675 nm (ultra long wavelength)

Les fibres G.652 (fibres unimodales) sont classées à leur tour en trois catégories (A, B et C). La G.652A et la fibre classique qui permet le transport de débit à 2,5 Gbit/s dans les bandes O, C et S. La fibre G.652B permet des canaux en DWDM à 10Gbit/s dans les bandes O, C, L et S. Les autres fibres sont peu utilisées. La G.653 (fibre à dispersion décalée) est employée au Japon et en Italie pour les transmissions dans la bande C. La G.654, à cause de son faible affaiblissement linéique, est réservée aux liaisons sous-marines pour 1300 et 1550 nm. Les fibres G.655 (fibre à dispersion décalée non nulle-NZ DSF) sont dédiées au 40 Gbit/s ou N fois 40 Gbit/s en DWDM (la G.655A avec un espacement inter canal de 200 MHz – la G.655B avec un espacement inter canal de 100 MHz et avec une limitation de 400 km – et la G.655C, en 100 MHz mais pour les liaisons supérieures à 400 km). La fibre G.656 utilise le multiplexage en longueur d'onde dans les bandes S, C et L.

La fibre optique idéale devrait permettre le plus grand nombre de canaux possibles à haut débit sans dégradation, elle devrait permettre le maximum de portée. Enfin, elle devrait répondre, pour le prix minimum, aux exigences du réseau de transport, à celles du cœur de réseau et du réseau d'accès.

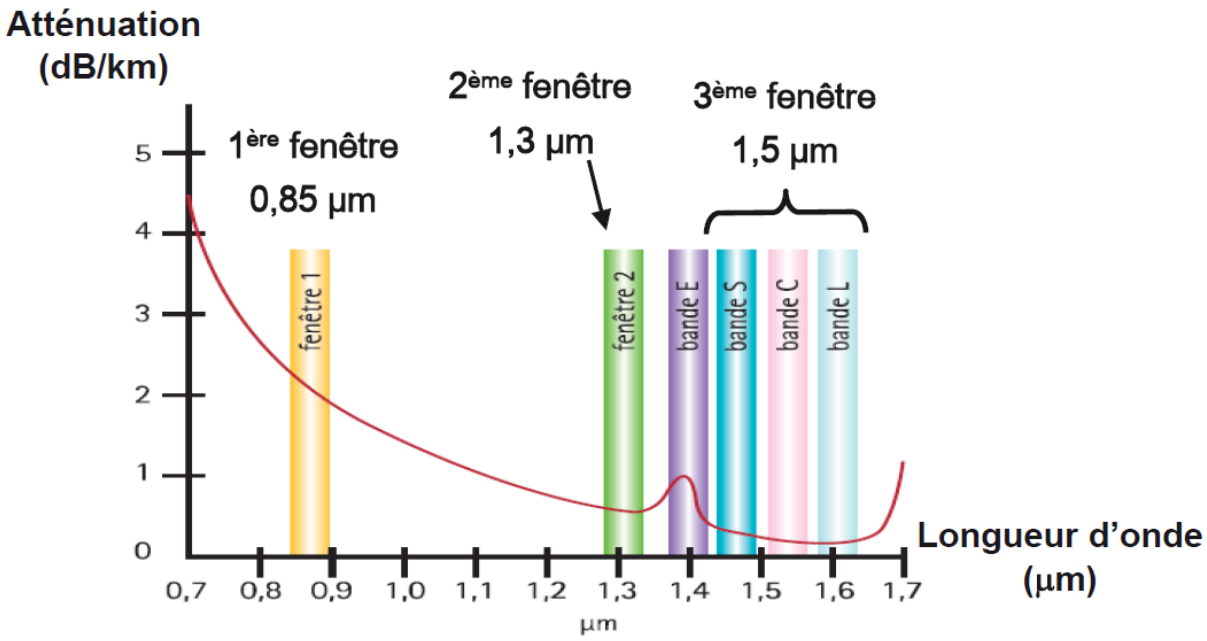

Figure IV-4 : Atténuation de la fibre en fonction de la longueur d'onde (db/nm)

Le dernier record en date, pour la capacité de transmissions de données sur fibre optique, a consisté à mettre sur la même fibre 140 canaux à 111 Gbit/s, soit 14 Tbit/s, multiplexés en longueur d'onde (WDM) sur une distance de 160 km. A titre d'exemple, NTT vise la mise en place d'une épine dorsale de réseau optique comprenant des canaux au débit de 100 Gbit/s, au lieu de 10 à 40 Gbit/s par longueur d'onde.

Les caractéristiques de la fibre optique

- L'atténuation est proportionnelle à la distance.
- Les effets de dispersion (se cumulent avec la distance).
  - ✓ dispersion intermodale (pour les fibres multimodes).
  - ✓ dispersion chromatique (ou intramodale).
  - ✓ dispersion modale de polarisation (PMD).

- Les effets non-linéaires (dépendent de la puissance en ligne).
  - ✓ effet Kerr (SPM, XPM, FWM).
  - ✓ effets de diffusion stimulée Brillouin et Raman.

IV.3 Evolution technologique

VI.3.1 Les systèmes SONET/SDH

SONET (Synchronous Optical Network) est un système de multiplexage temporel TDM (Time Division Multiplexing) classique sur fibre optique.

- SDH: Synchronous Digital Hierarchy (en Europe)
- SONET: Synchronous Optical Network (aux USA)

La SDH (Synchronous Digital Hierarchy) constitue la principale application des infrastructures fibres optiques longues distances.

Cette application constitue aujourd'hui le support de transmission de la grande majorité des applications de télécommunication. Elle fait suite, à ce titre, en en améliorant les caractéristiques, à la hiérarchie précédente PDH (Plesiochronous Digital Hierarchy).

VI.3.1.1 L'ARCHITECTURE DES RÉSEAUX SDH

La SDH réalise le transport d'un ensemble d'« affluents » (canaux numériques à bas débit) sur un canal « agrégat » à haut débit sur fibre optique. Les affluents sont insérés et extraits au niveau d'un multiplexeur qui réalise un multiplexage temporel TDM (Time Domain Multiplex) dans le canal agrégat.

Les multiplexeurs SDH sont généralement baptisés ADM (Add and Drop Multiplexer) Entre deux multiplexeurs ADM distants, le signal agrégat est remis en forme, périodiquement, par des répéteurs régénérateurs [07].

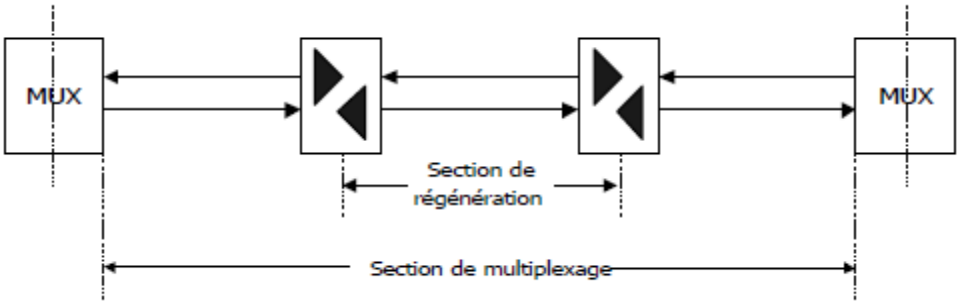

Figure IV-5 : Schématique d'une liaison SDH

Un réseau SDH est construit, en réalité, sur la base d'une architecture en « boucle », qui relie des Multiplexeurs ADM. L'architecture en boucle permet d'insérer ou d'extraire des « affluents » en tout point de la boucle. Elle permet par ailleurs de sécuriser le transport de l'agrégat. En cas de rupture d'une liaison entre deux multiplexeurs, la continuité de service est assurée par « reroutage automatique » du lien sur la boucle de secours [07].

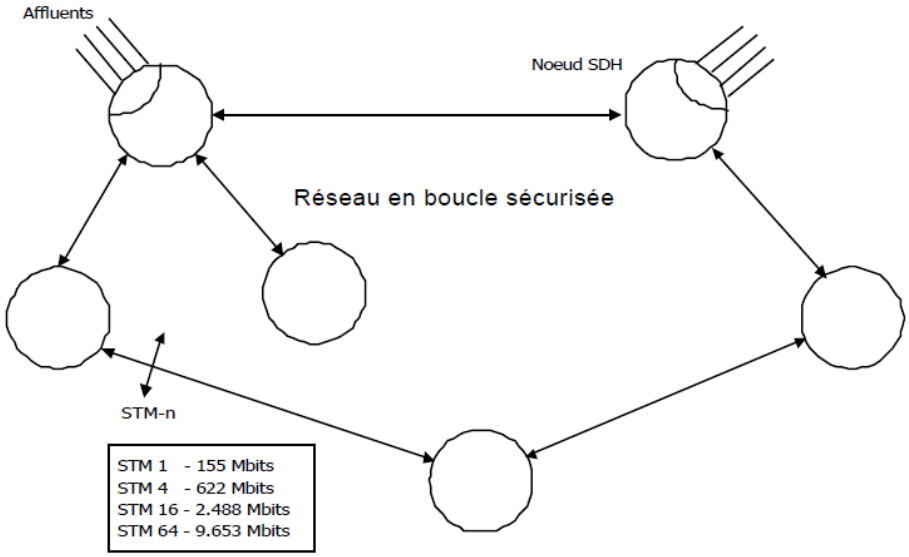

Figure IV-6 : Anneau SDH

VI.3.1.2 L'APPORT VIS À VIS DES ARCHITECTURES PDH

La hiérarchie plésiochrone PDH définie antérieurement à la SDH définit des classes de débit de 2 jusqu'à 140 Mbit/s. La hiérarchie SDH a donc pris le relais de cette hiérarchie vers les hauts débits, en prévoyant l'ensemble des mécanismes d'encapsulation des débits de l'ancienne hiérarchie dans la nouvelle.

Elle a permis par ailleurs d'accroître, outre la sécurisation, la flexibilité de configuration du réseau et des services en offrant un « adressage » des canaux affluents dans la trame d'agrégat multiplexée à haut débit. Cette fonction permet d'insérer et d'extraire un affluent en tout point du réseau, en laissant transiter dans la trame agrégat l'ensemble des autres informations. Cette fonction constitue un apport fonctionnel important de la SDH vis à vis de la hiérarchie précédente, qui nécessitait un démultiplexage complet de l'ensemble des canaux pour extraire un de ceux-ci :

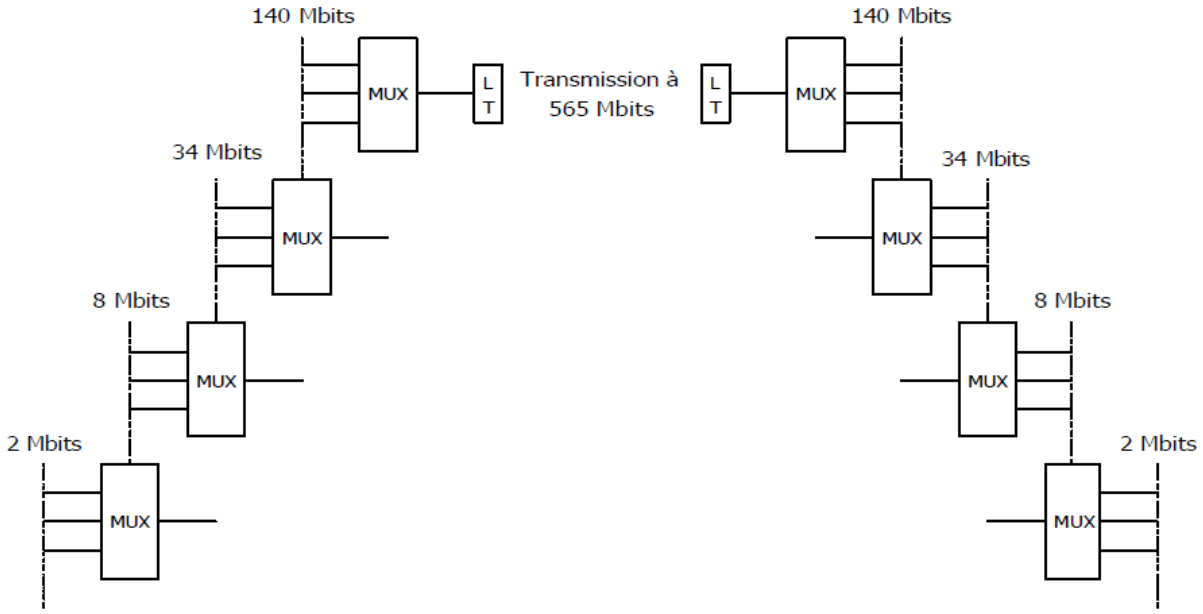

Figure IV-7 : Démultiplexage PDH

Dans un réseau SDH, la mise en relation entre un affluent entrant dans le réseau et un affluent sortant s'effectue par l'administration de réseau. Cette mise en relation permet de configurer un « circuit » (il s'agit d'un circuit virtuel permanent) qui relie les deux points, au travers du réseau. Le « routage » de ce circuit au travers du réseau s'effectue de manière plus ou moins automatique au travers de l'outil d'administration du réseau SDH.

VI.3.1.3 L'ÉTAT DES DÉBITS

Le tableau ci-après fournit l'état de l'Art des types d'interfaces et débits, chez les constructeurs d'équipements, et sur le terrain [07].

Classe de débit SDH	Débit en ligne
STM1	155 Mbit/s
STM4	622 Mbit/s
STM16	2,5 Gbit/s
STM64	10 Gbit/s
STM256	40 Gbit/s

Figure IV-8: Différentes types d'interface et débits SDH

VI.3.1.4 L'INTERFACE PHYSIQUE SDH

Les caractéristiques des interfaces SDH sont définies par la recommandation UIT G957. Celle-ci prévoit plusieurs types d'interfaces longue distance ou courte distance, fonctionnant soit dans la fenêtre 1310 nm soit dans la fenêtre 1550 nm.

λ	1310 nm	1550 nm
Gamme d'atténuation	0-12 dB ou 10-24 dB	
Distance couverte	15-40 km	15-80 km

Figure IV-9 : Deux types de fenêtre optique

VI.3.1.5 LES SUPPORTS DE TRANSMISSION

Les interfaces SDH ont été définies pour un support fibre optique monomode répondant à la recommandation G652. Cette fibre est la fibre la plus couramment utilisée, en Europe sur les réseaux fibres optiques. Les principales caractéristiques de cette fibre sont reprises dans ce document.

L'utilisation de fibre à dispersion décalée non nulle répondant au standard G655 permet d'accroître les portées, et les débits pour les interfaces à très haut débit (STM64 et STM256) par l'optimisation de la dispersion chromatique dans la fenêtre 1550 nm. Cette fibre permet, pour le support des longues distances, l'économie de modules de compensation de dispersion chromatique externes. Par contre, l'utilisation de la 2ème fenêtre de transmission (1310 nm), normalement utilisée pour les courtes distances par les équipements de transmission n'est pas optimisée avec ce type de fibre. Les exigences en matière de qualité de connectique et d'épissures (bilan d'insertion, réflectance) ont été définies dans la recommandation G671 [07].

VI.3.2 MULTIPLEXAGE EN LONGUEUR D'ONDE

VI.3.2.1 CWDM

Recommandation UIT-T G.695 traite de la technique de multiplexage par répartition approximative en longueur d'onde (CDWDM, coarse wavelength division multiplexing), dont les applications concernent les réseaux métropolitains en connexion point à point ou en boucle. Dans les équipements CWDM, des lasers non refroidis, et donc moins onéreux, sont utilisés. Ces lasers requièrent moins de précision dans le contrôle de la longueur d'onde. Les interfaces optiques relatifs aux recommandations UIT-T G.695. Les applications peuvent être de type unidirectionnel ou de type bidirectionnel, en général jusqu'au 1 Gbit/s.

VI.3.2.2 DWDM

Les systèmes DWDM (Dense Wavelength Digital Multiplexing) sont basés sur la capacité de transmettre plusieurs longueurs d'ondes simultanément sans interférence sur une seule fibre. Chaque longueur d'onde représente un canal optique. La technologie WDM s'est développée à un point que les espacements entre les longueurs d'ondes sont très petits - une fraction de nanomètre - ce qui a permis de transmettre une grande densité de longueurs d'ondes dans une fibre optique.

Ces applications sont déployées de plus en plus fréquemment car elles permettent d'optimiser l'usage d'une même fibre optique en multiplexant sur cette fibre plusieurs canaux, par exemple de type SDH. Ce multiplexage s'effectue en longueur d'onde, c'est à dire que chaque canal est modulé sur une « couleur » spécifique.

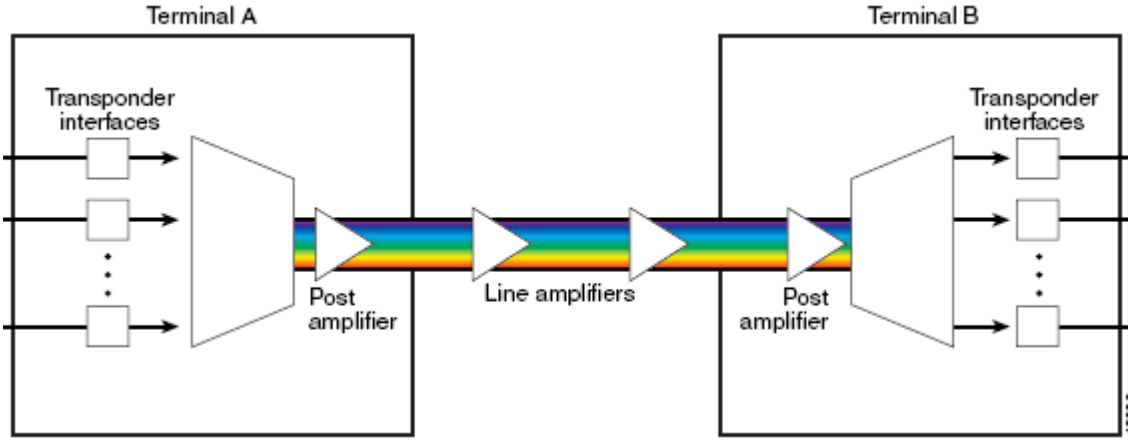

Figure IV-10 : Multiplexage DWDM

Le multiplexage en longueurs d'onde (Lambda - λ) repose sur un certain nombre de facteurs technologiques.

Le premier d'entre eux est la capacité de la fibre à transporter non pas une seule couleur mais tout un peigne de « couleurs ». C'est une caractéristique physique de ce support de transmission.

La technologie DWDM n'a connu d'applications industrielles qu'à partir du moment où il a été possible de générer des sources émettrices «accordées » et stables sur une longueur d'onde précise du spectre et de « filtrer » en réception la longueur d'onde désirée dans le spectre de couleurs.

La maîtrise de la tête optique laser et de sa précision d'émission (largeur de raie, stabilité en longueur d'onde et puissance) est une des clés technologiques des systèmes DWDM. Les éléments de filtrage utilisent quant à eux des réseaux à base d'optique intégrée ou des réseaux de Bragg.

L'essor de cette technologie a été possible, enfin, grâce aux progrès de l'amplification optique (EDFA). Ces composants, basés notamment sur des fibres dopées à l'erbium, permettent de réamplifier en ligne, l'ensemble du spectre optique, sans avoir à « démultiplexer» les canaux.

VI.3.2.3 ARCHITECTURE DES SYSTÈMES DWDM LONGUES DISTANCES

Les systèmes DWDM longues distances (dans les cœurs réseau) sont constitués principalement :

- de terminaux d'émission,
- de terminaux réception,
- d'amplificateurs optiques de ligne (OLA – Optical Line Amplifier),
- d'amplificateurs optiques à insertion extraction (OADM).

Les terminaux Réception :

Ceux-ci réalisent en premier lieu une ré-amplification du signal de ligne reçu, puis un filtrage des canaux, longueur d'onde par longueur d'onde, et enfin une re-transposition du canal vers la longueur d'onde « client ».

Les Amplificateurs optiques (OLA) :

Ceux-ci réalisent, en ligne, une ré-amplification de l'ensemble du spectre optique. Toutes les longueurs d'onde du spectre se trouvent ainsi ré-amplifiées sans besoin de démodulation individuelle. Les gains des amplificateurs optiques varient entre 20 et 35 dB, ce qui permet de compenser des pertes de la liaison sur des distances de l'ordre de 100 km [07].

Figure IV-11 : Amplificateurs optiques (OLA)

LES MULTIPLEXEURS A INSERTION EXTRACTION MIE (OADM) :

Un multiplexeur à insertion/extraction optique (OADM) autorise l'ajout ou l'extraction d'un ou de plusieurs signaux optiques du signal multiplexé WDM/DWDM à n'importe quel point de la fibre physique. À un nœud donné du réseau, un OADM joue le rôle d'un commutateur ou d'un aiguilleur optique. À partir du signal composite WDM, il redirige, vers les équipements d'accès uniquement les longueurs d'onde qui transportent des signaux clients qui ont pour destination le nœud courant. Ainsi, un Nœud d'accès n'a plus besoin de convertir la totalité du signal de transport optique à haute vitesse.

Pour sécuriser automatiquement un parcours deux équipements OADM placés aux extrémités d'une fibre optique peuvent être utilisés à condition de travailler en synchronisme sur les bons parcours lumineux demandés.

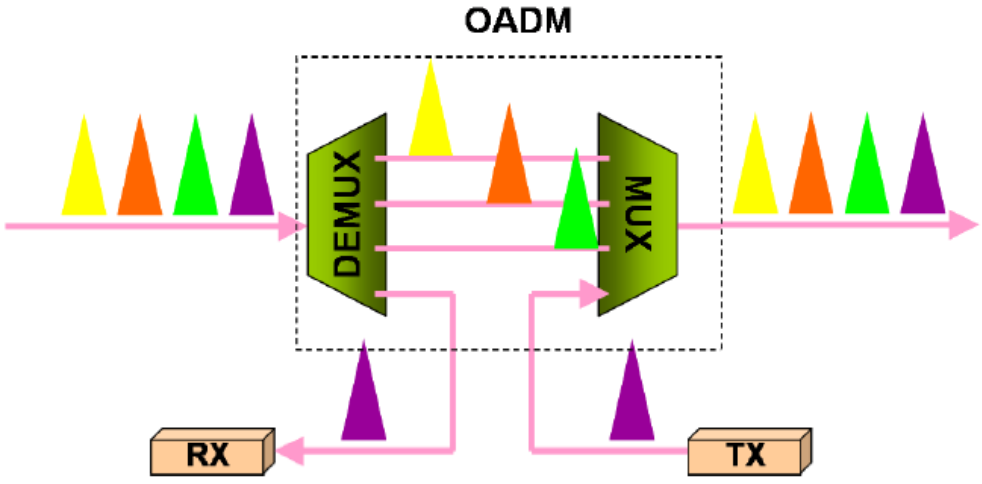

Figure IV-12 : schéma synoptique d'un OADM

Dans ce cas, on dispose de ROADM (R pour Reconfigurable), Un ROADM (Reconfigurable Optical Add/Drop Multiplexer) est un OADM reconfigurable qui offre en plus la possibilité de commuter des signaux de transport optiques à distance au niveau de la couche de longueurs d'onde du système WDM. Cela permet à une ou plusieurs longueurs d'onde.

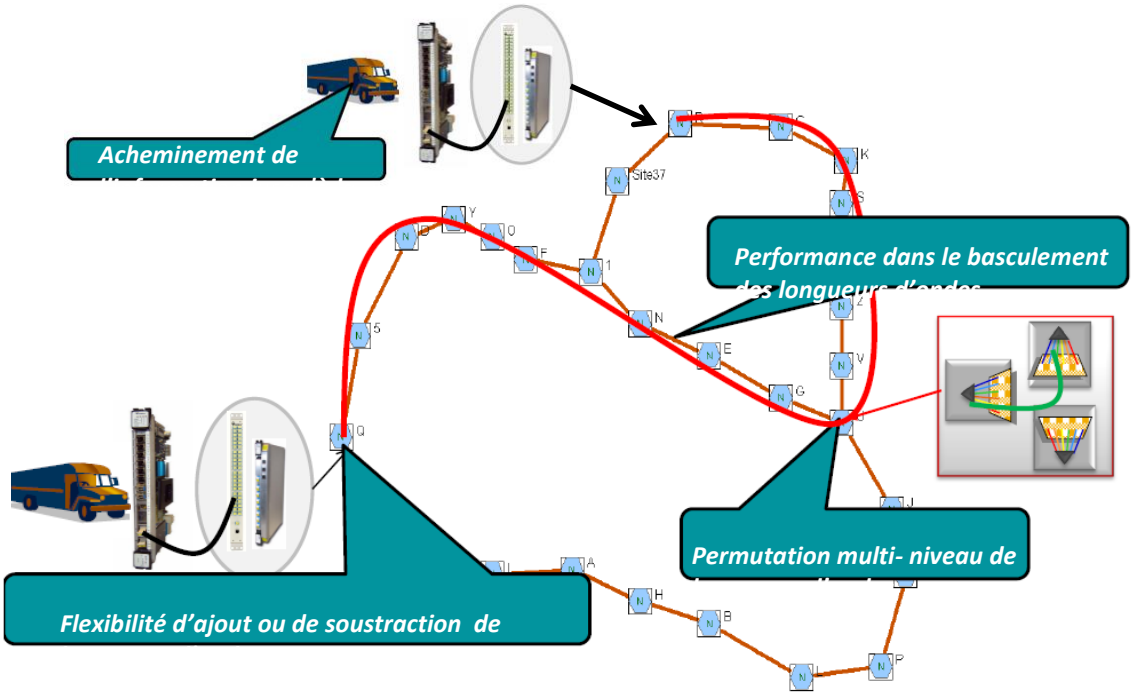

Figure IV-13 : Fonctionnement des ROADM dans un Cœur de Réseau

Figure IV-14 : modèle de carte ROADM

LES EQUIPEMENTS DE COMMUTATION OPTIQUES :

Les Cross Connect Optiques (OXC – Optical Cross Connect) sont des équipements de commutation susceptibles de mettre en relation des ports optiques d'entrée avec des ports optiques de sortie. Ils réalisent ainsi, une commutation de circuits optiques.

Associés aux équipements DWDM, ces commutateurs apportent souplesse et facilité dans la gestion du réseau. Disposant d'une « intelligence » associée à l'administration centralisée du réseau, ils permettent de gérer le « routage » des circuits optiques et la redondance des circuits au travers du réseau maillé [07].

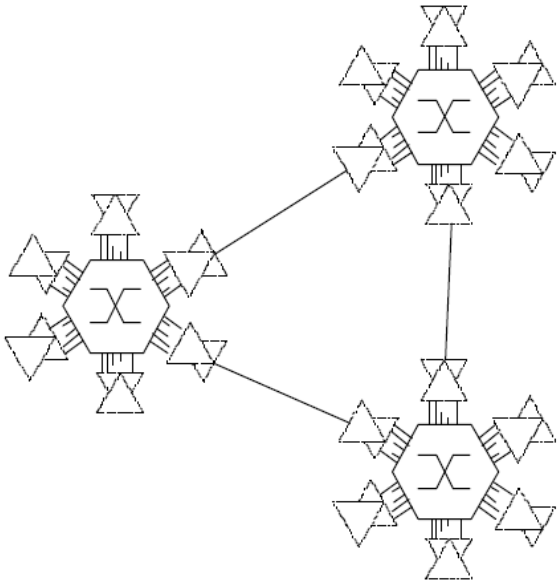

Figure IV-15 : schéma synoptique d'un OXC

VI.3.2.4 PERFORMANCE DES SYSTÈMES DWDM LONGUES DISTANCES

Les performances des systèmes DWDM s'apprécient par :

- le nombre des longueurs d'onde gérées (nombre de canaux),
- le débit maximal sur chaque longueur d'onde,
- la distance couverte.

Spectre optique et nombre de longueurs d'onde gérées :

Les longueurs d'onde des systèmes DWDM sont aujourd'hui comprises dans la fenêtre 1525-1565 nm.

L'UIT a défini un peigne de fréquences espacées au pas de 100 GHz. Cette grille définit des longueurs d'onde de transmission au pas de 0,8 nm. Les différents systèmes fonctionnent aujourd'hui au pas de :

- 200 GHz (longueurs d'onde espacées d'environ 1,6 nm).
- 100 GHz (longueurs d'onde espacées d'environ 0,8 nm).
- 50 GHz (longueurs d'onde espacées d'environ 0,4 nm).

Certains constructeurs travaillent aujourd'hui sur la maîtrise d'un peigne au pas de 25 GHz (longueurs d'onde espacées d'environ 0,2 nm).

Sur cette base, les systèmes existants permettent de véhiculer de 16 à environ 100 longueurs d'onde sur une même fibre.

L'analyse de l'évolution des systèmes DWDM démontre la volonté d'utiliser un nombre toujours plus important de longueurs d'onde sur une même fibre.

Cette amélioration s'effectue selon deux axes :

- une réduction du pas entre longueurs d'onde par une meilleure maîtrise des émetteurs, récepteurs et amplificateurs de ligne.
- une extension de la largeur de bande concernée.

Si la majorité des systèmes utilisent actuellement la bande C traditionnelle (1530 – 1563 nm), de nombreux constructeurs explorent aujourd'hui l'utilisation de la bande L (1570 – 1620 nm) L'utilisation de cette nouvelle bande sous-entend une qualification particulière des infrastructures de fibre en extrémité de bande. L'objectif lointain est par ailleurs le développement d'amplificateurs incluant la fenêtre 1310 nm permettant d'accroître considérablement le nombre de canaux transmis.

Débit maximal sur chaque longueur d'onde :

Aujourd'hui, le débit maximal supporté sur chaque longueur d'onde dépend des systèmes et constructeurs, mais également du type et de la qualité des fibres. Il est typiquement du niveau STM16 (2,5 Gbit/s), STM64 (10 Gbit/s) ou STM256 (40 Gbit/s), 100 Gbit/s et 400 Gbit/s au future.

Distance couverte :

La distance couverte s'exprime en fonction du nombre de « Spans » qui définit le système :

- entre terminal et amplificateur optique.
- entre amplificateurs optiques.

Ainsi que du budget optique sur un « span » élémentaire.
On parlera typiquement de systèmes 6 à 8 Spans de 20 dB. Avec une infrastructure fibre optique offrant un budget de 0,25 dB/km dans la fenêtre 1550 nm, le span sera d'environ 80 km, ce qui signifie que les amplificateurs optiques devront être implantés tous les 80 km environ.

La distance globale couverte sera de 640 km avec un système 8 Spans.

Le nombre de « Span » limite le nombre d'amplificateurs en ligne dans la liaison. Cette limitation est liée à la qualité de l'amplificateur.

Outre l'amplification du signal, l'amplificateur est générateur de bruit ; la mise en cascade d'amplificateurs augmente l'amplitude de bruit et il est nécessaire d'en limiter le nombre pour conserver un rapport signal à bruit correct en bout de liaison.

Au-delà du nombre maximum de « span » et donc de la distance maximale, il est possible d'étendre la distance de la liaison par adossement d'un terminal de réception et d'un terminal d'émission. On parle dans ce cas de « Back To Back ».

Certains systèmes distinguent dans les règles d'ingénierie le débit visé sur chaque longueur d'onde. Ainsi le nombre de spans et le budget sur chaque span pourra être plus élevé si on limite l'usage de la liaison à un débit de type STM16 (2,5 Gbit/s) ; ils devront être réduits si on envisage l'usage de cette liaison pour le support de longueurs d'onde en STM64 (10 Gbit/s).

VI.3.2.5 SERVICES OFFERTS PAR LES RÉSEAUX OPTIQUES DE NOUVELLE GÉNÉRATION

Pour appréhender ces services, il est pratique de voir le réseau optique comme constituant une couche optique qui offre des services aux couches supérieures du réseau. Trois types de services sont ainsi offerts par les réseaux optiques de seconde génération aux couches réseau supérieures [07].

- **service de chemin optique**

Un chemin optique est une connexion entre deux nœuds d'un réseau, qui est mise en place en assignant une longueur d'onde dédiée sur chacun des liens constituant le chemin. La totalité de la bande passante est ainsi mise à la disposition de la couche supérieure.

En fonction de l'implémentation du réseau, ce chemin optique peut être activé et désactivé à la demande de la couche supérieure, il peut donc être pensé comme un service de commutation de circuit similaire à celui fournit par le réseau téléphonique (le réseau établit ou supprime un appel à la demande de l'utilisateur). Il peut aussi être permanent, installé au moment du déploiement du réseau.
Si l'implémentation dispose de fonctions de conversion de longueur d'onde, la longueur d'onde dédiée utilisée pour établir le chemin optique est dynamiquement gérée par chacun des nœuds du réseau.

Le chemin optique sur la figure ci-dessous est établi entre les nœuds N1 et N7 en utilisant des longueurs d'onde différentes pour chacun des liens constituant le chemin optique.

Les nœuds sont dotés de capacité de conversion de longueur d'onde (transducer)

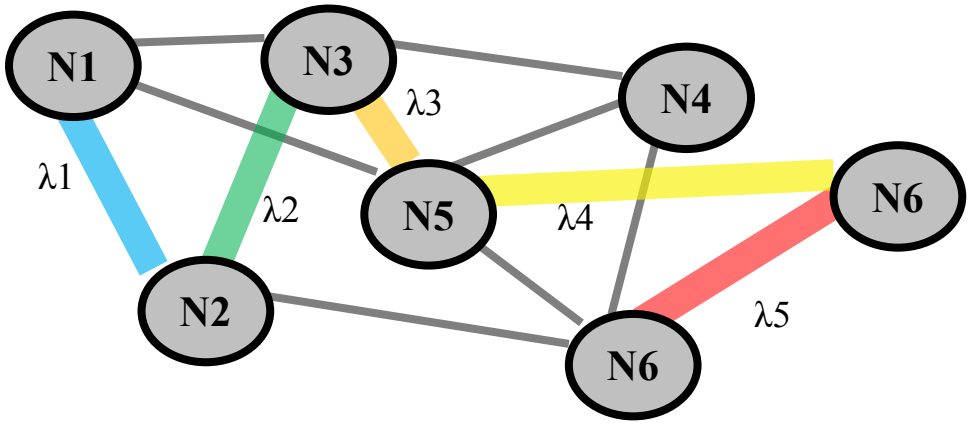

Figure IV-16 : Longueur d'onde dédiée sur chacun des liens

Sur la figure ci-dessous, pour ce chemin optique, c'est une longueur d'onde unique qui est utilisée pour établir la connexion entre le nœud N1 et le nœud N7 .Ce chemin peut être permanent ou établit dynamiquement.

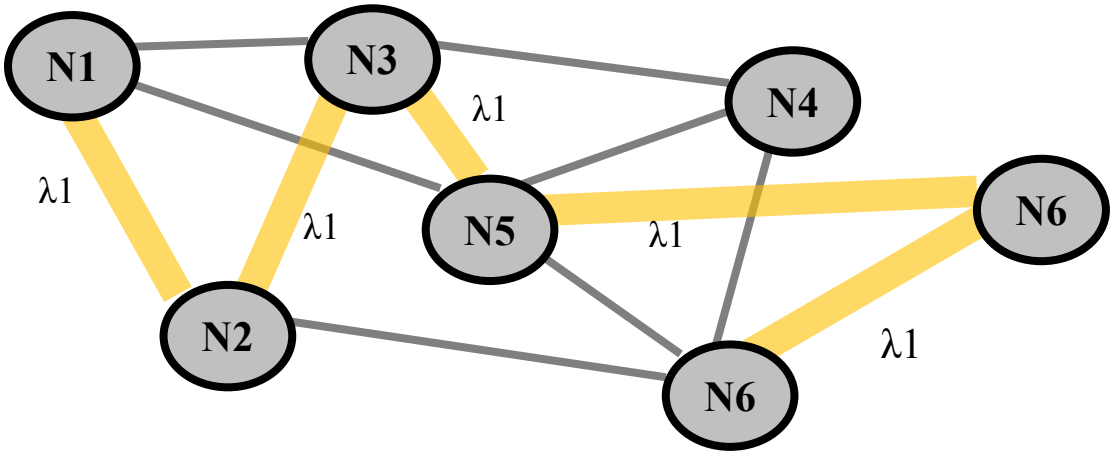

Figure IV-17 : Longueur d'onde unique pour la connexion entre le nœud N1 et le nœud N7

- **service de circuit virtuel**

Dans ce cas, le réseau offre une connexion du type commutation de circuit entre deux nœuds. Cependant, la bande passante offerte peut être plus faible que la bande passante complète disponible sur le lien. Le réseau doit alors disposer d'une forme quelconque de multiplexage temporel pour combiner plusieurs circuits virtuels sur une longueur d'onde du lien WDM. Ce multiplexage peut être fixe ou statistique.

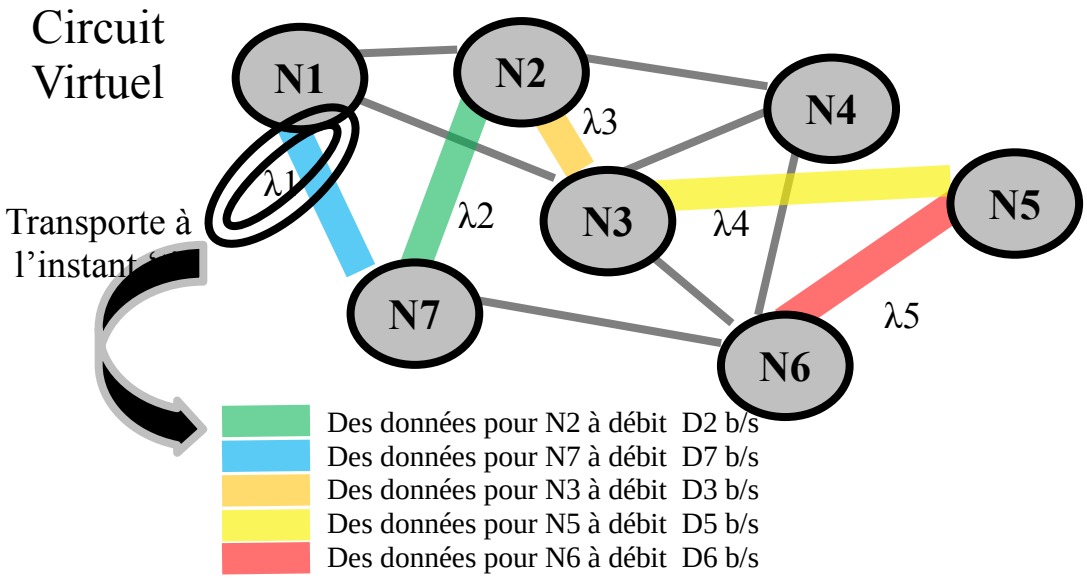

Figure IV-18 : connexion du type commutation de circuit entre deux nœuds

- **Service datagramme**

Ce service permet la transmission de paquets ou messages entre deux nœuds du réseau sans avoir installé de connexion explicite. Le protocole IP est un exemple de protocole fournissant uniquement des services de datagramme, les réseaux optiques sont capables de fournir ce type de service en point à point et en point à multipoint (*multicast ou broadcast*).

VI.3.3 LA PROTECTION DANS LES RESEAUX OPTIQUE

Les réseaux WDM il arrive qu'une interruption de service accidentelle ait lieu, coupant une ou plusieurs routes du réseau. La cause de ces pannes peut être de différentes natures : une coupure physique du câble optique, un incendie dans un local, ou simplement une erreur humaine. Une interruption de service n'est pas assez rare pour qu'elle puisse être considérée comme insignifiante. Par ailleurs, la quantité de données transportées dans une fibre est telle qu'une coupure provoque la perte d'une importante quantité de données. On cherche alors naturellement des mécanismes de protection qui rendent le réseau tolérant aux pannes ou assurant une continuité face aux pannes [08].
Il existe différents types de protections qui peuvent être mis en œuvre, nécessitant des routages différents

Restauration : La restauration consiste à re-router dynamiquement des connexions lorsqu'un cas de panne survient sur le réseau. On doit alors calculer, au moment de la panne, un nouveau routage à partir des ressources disponibles. On parle d'algorithme online (comme pour le routage) puisqu'ils ne répondent pas à un problème statique ou connu à l'avance. Dans la suite de cette thèse nous ne traitons pas le problème de la restauration, mais celui de la protection [08].

Protection par re-routage global : Le re-routage global consiste à prévoir un routage admissible pour chaque cas de panne possible. Pour chaque routage, une certaine capacité est nécessaire sur un câble du réseau. On choisit la capacité maximum, pour tous les cas de pannes possibles et l'on choisit d'allouer cette capacité maximale : on obtient l'assurance de pouvoir router, quelle que soit la panne, l'ensemble des requêtes sur le réseau. L'inconvénient direct d'une telle politique de protection vient du fait qu'entre l'état sans panne et un état de panne

donné, aucune garantie n'est donnée quant à l'emplacement des routes principales et des changements à opérer. Dans le pire des cas, toutes les routes principales sont à modifier, provoquant un impact d'ordre technique dans la configuration des nœuds [08].

Protection dédiée et partagée: La protection dédiée et partagée ne nécessite pas un reroutage total en cas de panne. Il s'agit au contraire de ne rerouter que les chemins principaux touchés par la panne par des chemins de secours. La protection dédiée nécessite d'allouer un chemin de secours qui ne peut être réutilisé dans un autre contexte. À l'inverse, la protection partagée permet d'utiliser une même ressource pour deux chemins de secours qui ne pourraient être activés en même temps. Notons enfin que le reroutage global fait partie de la protection partagée (tout le réseau est partagé).

On distingue alors la classification suivante pour la protection dédiée : la protection 1 + 1 qui consiste à envoyer la même information sur deux chemins disjoints (le chemin principal et de protection) en même temps. Au niveau du nœud de destination, le signal est reçu en double, garantissant la réception d'au moins un signal en cas de panne [08].

La protection 1 : 1 dédiée

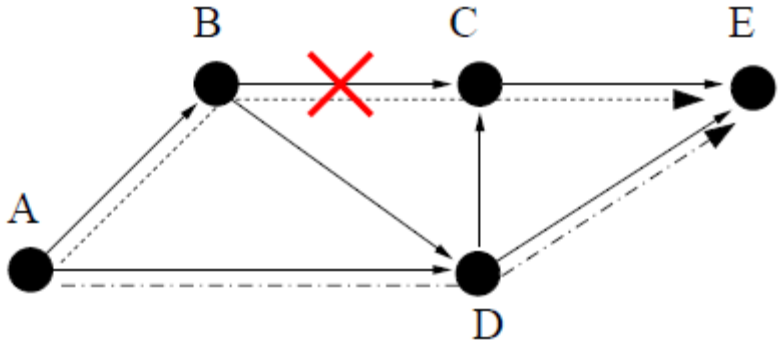

Figure IV-19: Protection 1 : 1 d'une requête *AE* pour la panne du câble AB.

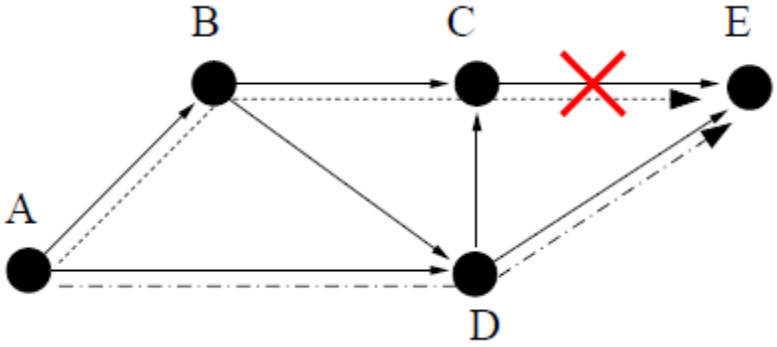

Figure IV-20: Protection 1 : 1 d'une requête AE pour la panne du câble CE.

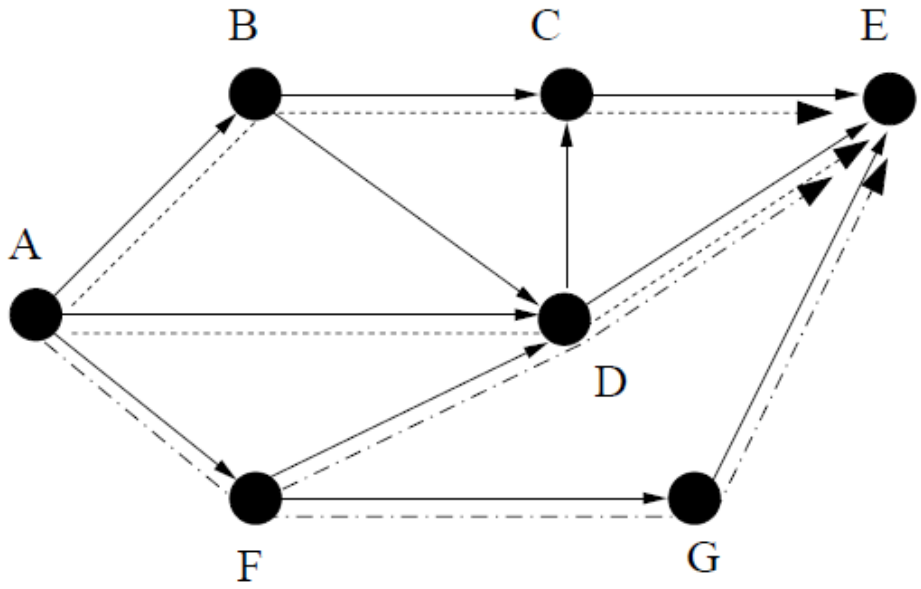

Figure IV-21 : Protection 2 : 2 d'une requête AE de taille 2

Réserve un chemin de secours pour chaque chemin principal. En cas de panne, le chemin de secours est activé. Dans le cas de la protection partagée, on parle aussi de protection 1 : 1. Dans ce cas, les chemins de secours peuvent partager des longueurs d'onde entre eux. Ce cas est montré en figures ci- dessus, où l'on protège le chemin (A,B,C,E) pour deux cas de pannes possibles. Pour ces pannes, on utilise le même chemin de secours, (A,D,E), qui est dit « partagé ». Plus généralement, pour plus de flexibilité, on utilise la protection M : N. Pour une même requête z Є Z,M chemins principaux sont protégés par N chemins de secours. Les N chemins de secours peuvent partager des longueurs d'onde avec d'autres chemins de secours (de la même requête ou d'une requête différente) qui ne peuvent s'activer pour la même panne. Figure IV-21 montre le cas d'une protection du type 2 : 2. Les chemins principaux, en pointillés, sont protégés par les chemins en pointillés discontinus. On note alors que sur le câble AF, on peut partager la capacité de protection puisque les chemins principaux ne peuvent tomber en panne en même temps [08].

Notons enfin que pour la protection 1 : 1 et M : N, les ressources réservées pour les chemins de protection ne sont pas utilisées. En pratique, les opérateurs font circuler sur ces canaux des flux non prioritaires. Ces flux peuvent être interrompus et remplacés par des flux de protection, le temps que la situation revienne à la normale.

VI.3.4 RESEAUX D'ACCES OU DE DESSERTE

Les réseaux d'accès, aussi appelés "réseaux de desserte" réalisent la connexion des usagers. Ils constituent le dernier lien ("the last mile") vers les utilisateurs du réseau. Ils représentent généralement le maillon crucial du réseau en termes économiques et de performance. A ce niveau, on dispose d'une panoplie importante de technologies filaires ou hertziennes qui ont chacune leurs avantages et inconvénients en fonction des applications.

Leur mise en œuvre répond à des critères très variés selon que l'on s'adresse à des usagers Résidentiels, des petits professionnels (SOHO - Small Office Home Office) ou à des entreprises.

Pour les infrastructures filaires, citons :

- ✓ La boucle locale cuivre qui est le champ d'action privilégié de l'opérateur historique et, à ce jour, des principaux opérateurs alternatifs qui accèdent à cette boucle via le dégroupage.
- ✓ L'introduction des technologies xDSL apporte un certain nombre de contraintes, notamment vis à vis de la portée. L'évolution des normes et l'apparition de différentes variantes (ADSL 2+, SDSL, VDSL) permettent d'augmenter les débits ou encore d'introduire de la symétrie dans ces débits, mais la contrainte de portée demeure importante. Certaines solutions mixtes alliant la fibre optique et le xDSL permettent de s'affranchir de ces limitations de portée.
- ✓ Les réseaux câblés de télédistribution, centrés sur les zones urbaines. Ces réseaux disposent d'une capacité multiservices ; ils mettent en œuvre une combinaison de technologies large bande sur fibre optique et sur câble coaxial.
- ✓ Les réseaux optiques passifs qui sont, entre autres, le support privilégié d'Ethernet à haut débit (Fast Ethernet ou Gigabit Ethernet). Ils peuvent être déployés sous la forme de liaisons spécialisées (point à point) ou à partir d'architectures partagées telles que les PON (Passive Optical Network = Réseau Optique Passif) dans des configurations comme le FTTB (Fiber To The Building) ou FTTH (Fiber To The Home).
- ✓ Les courants porteurs en ligne, qui sont adaptés aux réseaux locaux d'entreprise ou aux réseaux domestiques, mais dont la mise en œuvre pose encore de nombreux problèmes dans le domaine des réseaux d'accès.

Les réseaux d'accès radio, utilisent des technologies variées, citons :

- Les réseaux de téléphonie mobile (3G, 3G+ et 4G/LTE) : Les utilisateurs ne possédant qu'une ligne mobile sont de plus en plus nombreux, que ce soit pour téléphoner ou échanger et consulter des données via l'internet.
- Les réseaux wifi : des débits proposés vont de 6 à 10 Mbit/s pour les particuliers et jusqu'au 30 Mbit/s avec des antennes de réception alimentée par une fibre optique, la couverture pour les particuliers arrive jusqu'au 10 km.

Avantages des technologies mobiles de 3e et de 4 générations :

- Evolutions logicielles de la 3G proposant des performances accrues.
- Débit jusqu'à 100 Mbit/s avec la 4G permettant l'apparition de nouveaux services innovants encore inexistants.
- Coût des déploiements (prise en charge à 100% par les opérateurs)
- Diversité des terminaux (smartphones, tablettes, clé USB).
- Services de données en mobilité.
- Solutions de convergence fixe-mobile et possibilité de basculement automatique d'un réseau mobile à un hot spot Wi-Fi (technologie EAP SIM)
- Réseaux pouvant se substituer aux technologies fixes notamment en zones rurales (solutions de convergence fixe-mobile).

À ce stade du développement de la technologie et du marché, les technologies de réseaux mobiles ou sans fil (y compris LTE) ne paraissent capables de fournir des services (symétriques) à très haut débit, en particulier car ces technologies sont «partagées» et que, de ce fait, le débit dépendra du nombre d'utilisateurs connectés dans la zone couverte

VI.3.4.1 LA DESSERTE HAUT DEBIT PAR LES TECHNOLOGIES FTTX

L'introduction des technologies « fibre optique » dans le réseau d'accès découle d'un certain nombre d'éléments convergents :

- l'augmentation des besoins des utilisateurs :
  - les besoins des entreprises en communications symétriques sont en croissance régulière quelles que soient leur taille et leur activité, pour passer de 1 à 10 puis 100 Mbit/s, voire 1 Gbit/s à terme.
  - les besoins des usagers résidentiels combinent l'accès à plusieurs programmes de télévision (en haute définition), la navigation Internet, le téléchargement et le transfert de fichiers et les communications téléphoniques et visiophoniques.

- la convergence des applications et des terminaux, favorisée par l'utilisation du protocole IP, conduit à utiliser un média large bande et transparent.

- les technologies traditionnelles (cuivre) atteignent leurs limites liées aux lois de la physique, alors que les technologies alternatives (radio, satellite, CPL) ne sont que des solutions d'attente sur des applications ciblées.

Même si tout le monde s'accorde à penser que le réseau cible, satisfaisant tous les critères de pérennité, est fondé sur la fibre optique jusqu'à l'abonné, les aspects économiques ralentissent son déploiement immédiat. Pour sa part, le coût des équipements optoélectroniques est déjà en forte réduction et bénéficiera encore des effets de volume, la vraie question est liée au coût du génie civil, bien plus important que celui des composants optiques (câble, connectique, équipements actifs). Dans le réseau d'accès, les fibres optiques peuvent être déployées selon diverses topologies FTTx où la variable « x » décline le niveau plus ou moins profond de déploiement de la fibre vers l'usager final :

- ✓ FTTC (C = Curb),
- ✓ FTTB (B = Building),
- ✓ FTTH (H = Home) ou même FTTD (D = Desk).

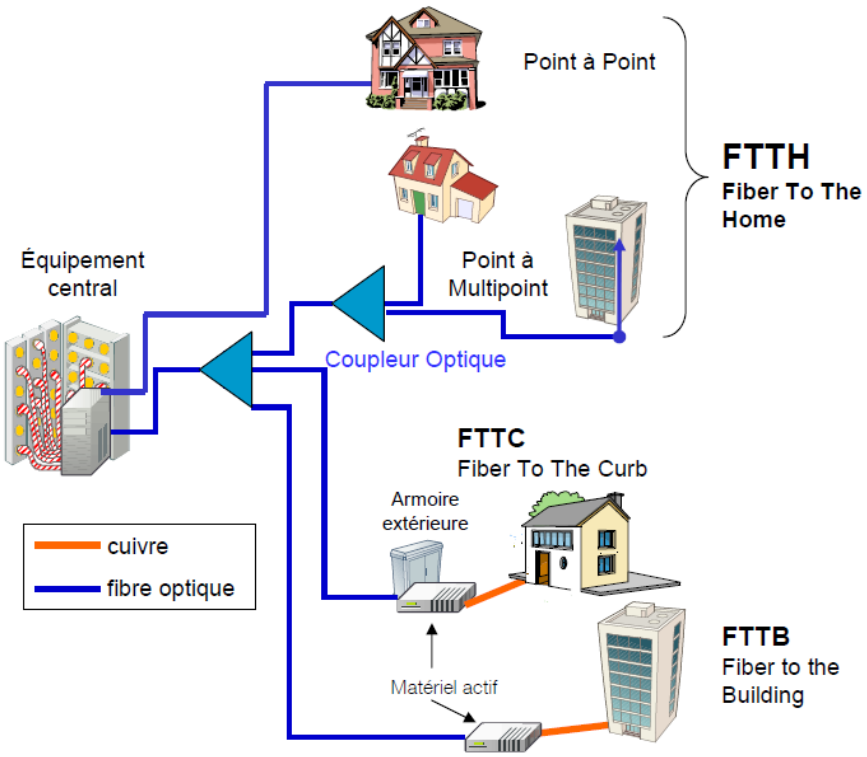

Figure IV-22 : Les différentes architectures FTTx

VI.3.4.2 LA DESSERTE HAUT DEBIT PAR LES TECHNOLOGIES XDSL

Un réseau **NGN** utilise un ensemble d'équipements qui jouent le même rôle qu'un commutateur traditionnel, mais qui sont désormais séparés en composants distincts :

- Le « Softswitch » est la solution qui gère dans un réseau **NGN** l'intelligence du service de commutation (gestion de tables d'appels, gestion des plans de numérotation). Toutefois, ce Softswitch n'est plus associé à un point physique du réseau, et ne gère plus les liens physiques du réseau, comme c'était le cas dans un réseau **TDM**.
- Le « Media Gateway », dont le rôle est d'assurer la gestion (disponibilité, détection de fautes) de la couche physique du réseau. Cette couche physique peut être le réseau de transmission, ou le réseau d'accès.

Dans le cas où il s'agit du réseau d'accès, la fonction de Media Gateway peut être embarquée dans l'équipement d'accès lui-même, comme c'est le cas pour un **MSAN**.

Dans la plupart des réseaux **NGN** déployés, la coexistence d'offres d'accès data et l'offres d'accès voix dans le portefeuille des opérateurs amène le déploiement de solutions « tout en un », permettant le contrôle d'accès pour les services voix et les services data. Ces solutions tout en un sont des **MSAN**.

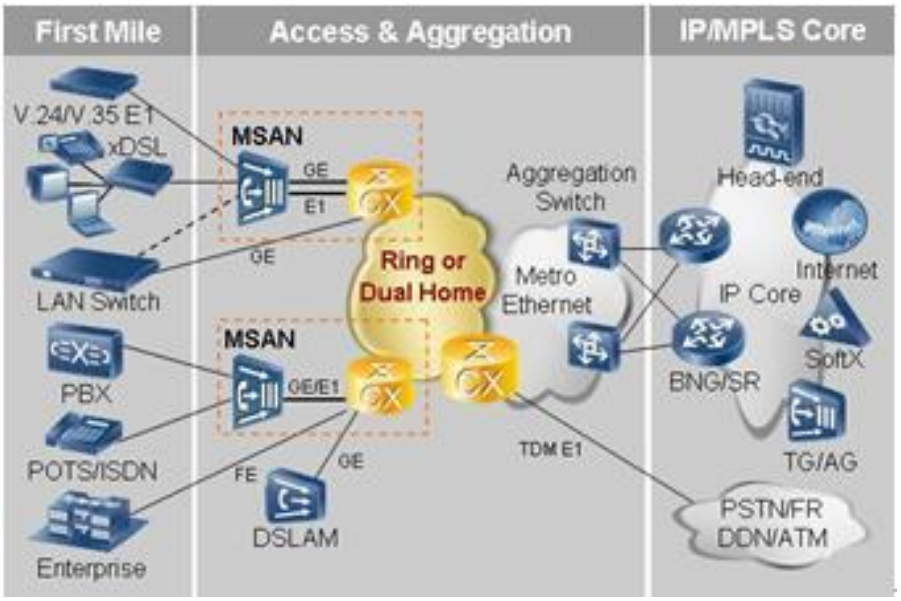

Figure IV-23 : Topologies réseaux d'accès MSAN

Les **MSAN** constituent une évolution naturelle des DSLAMs. Un MSAN est un équipement qui constitue, dans la plupart des architectures de type NGN, un point d'entrée unique vers les réseaux d'accès des opérateurs. A la différence d'un DSLAM, dont le châssis ne peut supporter que des cartes permettant de proposer des services de type xDSL, un MSAN peut supporter des cartes RNIS, Ethernet, FTTx, ou encore X25.

De ce fait, au sein d'un seul et même châssis, l'opérateur peut déployer toutes les technologies d'accès envisageables sur son réseau.

VI.4 Conclusion

Le but d'avoir une architecture de type NGN (Next Generation Network), consiste à bâtir une infrastructure unique basée sur l'IP au niveau du cœur du réseau de transport qui permet d'acheminé tout type de flux, voix ou données, et supporté toute les technologies d'accès (DSL, FTTH, RTC, WiFi, etc.).

CHAPITRE V

Les Différentes Phases Pour Un Déploiement d'un Réseaux De Télécommunication

V.1 Introduction

Les réseaux de télécommunications sont devenus des ressources stratégiques et leur importance économique ne cesse d'augmenter. Ainsi pour faire face à la croissance et à l'augmentation de la charge des réseaux, la première idée est d'utiliser des routeurs puissants avec beaucoup de mémoire, des processeurs rapides et des lignes à hauts débits. Il va de soit que le coût de telles infrastructures peut être exorbitant.

Partant de cet état de fait, l'élaboration d'une topologie optimale nous est apparue, dans ce contexte, un point important à étudier. Les principales difficultés rencontrées vont être de minimiser le coût total du système de communication tout en garantissant une QoS globale du réseau (résilience).

Dans cette partie, l'accent sera porté sur les différentes phases importantes de conception de réseaux modernes de communications.
La conception des réseaux de télécommunications représente une tâche très complexe et en règle générale, fort coûteuse. L'équipe de conception doit passer en revue sur les besoins déjà existants ou anticiper les besoins futurs, les coûts des différentes composantes des systèmes, les contraintes imposées aux performances, la fiabilité, la capacité d'adaptation aux évolutions, le service de contrôle de la qualité, etc.

Ainsi la conception d'un WAN (Wide Area Network) est un processus dans lequel des dizaines de sites aux caractéristiques différentes sont connectés afin de satisfaire à certains standards de fiabilité et de performance, et ce, à des coûts minimes.

L'une des questions clés de la conception d'un WAN est la grande complexité de la problématique. Ainsi même en décomposant le problème global, les sous problèmes auxquels on aboutit ne sont pas triviaux. Etant donné l'importance des investissements, si l'on réussit à réduire légèrement les coûts de quelques points de pourcentage, tout en assurant la même qualité des services, il sera possible de dégager des bénéfices économiques considérables.

V.2 Problèmes de conception des réseaux

Les évolutions de l'Internet, conduisent à une multiplication des services offerts par les réseaux et à une croissance du nombre d'utilisateurs et des volumes de trafics qu'ils génèrent. Dans une société où l'information et la communication ont pris une telle importance, l'interruption des services offerts par le réseau, ou même une dégradation significative de la QoS sont de moins en moins acceptables. Ceci pose aux opérateurs de télécommunication (FAI) de nouveaux problèmes.

Initialement, pour faire face à ces problèmes, les opérateurs se sont tournés vers un surdimensionnement des équipements. Les principales sources de dégradation de QoS étant les zones de congestion du réseau, limiter les risques de congestion par une augmentation conséquente des ressources permet d'écouler les volumes de trafic tout en garantissant la QoS requise.

Cependant, cette démarche n'est plus viable économiquement. Le contexte concurrentiel qui induit des marges bénéficiaires réduites ne permet plus d'améliorer les performances d'un réseau IP par un surdimensionnement excessif des équipements. D'un point de vue technique, cette démarche doit être modifiée si l'on veut vraiment maîtriser l'évolution du réseau. La garantie de performances, ne peut s'obtenir sans une nouvelle approche de conception de Réseaux, qui consistent à adapter le réseau (existant ou non encore installé) aux volumes de trafic et exigences de QoS qu'il doit supporter. Elles intègrent également les notions de résilience pour garantir non seulement une utilisation adéquate des ressources dans le réseau nominal, mais aussi des performances "acceptables" si le réseau est dans un état de panne. Planifier son réseau revient également à anticiper l'évolution globale du trafic, par exemple l'évolution des services dans le réseau et le nombre de clients par service.

On peut classifier le cycle de vie d'un projet de conception en six différentes étapes : Préparation – Planification – Conception – Implémentation – Exploitation – Optimisation

Le processus « préparer, planifier, concevoir, implémenter, exploiter et optimiser » reflète les phases du cycle de vie d'un réseau standard comme l'illustre la ci-dessous, les phases du cycle de vie sont distinctes, mais étroitement liées [09].

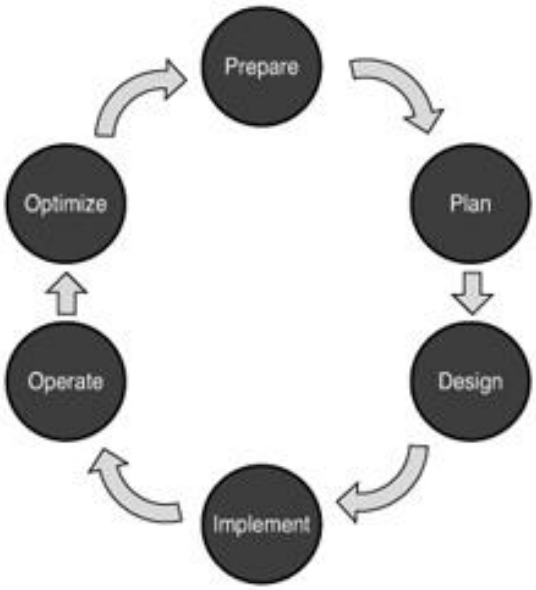

Figure V-1 : le Processus de conception de réseaux

1- la phase de préparation : Cette phase consiste à définir les besoins de l'organisation (entreprise), de développer une stratégie de réseau, en proposant conception d'architecture de haut niveau, et d'identifier les technologies qui peuvent soutenir au mieux l'architecture. La justification financière de la stratégie de réseau est établie en évaluant la rentabilité pour l'architecture proposée [09].

2- la phase de planification : La phase du Planification consiste à effectuer une analyse des problèmes et des besoins du réseau, afin de déterminer si l'infrastructure du système existant, et de l'environnement opérationnel, peut soutenir le système proposé. Un plan de projet permet de gérer les tâches, les responsabilités, les étapes critiques, et les ressources nécessaires pour appliquer les modifications du réseau. La sortie de cette phase est un ensemble de prérequis du réseau [09].

3- Phase de conception : Les spécialistes de conception du réseau utilisent les besoins initiaux identifiés lors de la phase de planification,

En intégrant toutes les données supplémentaires recueillies au cours de l'audit de réseau (lors d'une mise à jours d'un réseau existant) et par la discussion avec les clients finaux (les gestionnaires, et les utilisateurs du réseau), afin d'aboutir aux spécifications détaillée et complète qui répond aux exigences, en matière commerciale et technique pour soutenir la disponibilité, la fiabilité, la sécurité, l'évolutivité et la performance.

Cette spécification de conception fournit la base pour les activités de mise en œuvre [09].

4- la Phase d'implémentation : c'est l'opération de mise en œuvre et de vérification qui commencent après l'approbation de la phase conception. Le réseau et les composants supplémentaires seront installés selon les spécifications de la phase Conception, avec l'objectif d'intégrer des dispositifs sans perturber le réseau existant ou en créant des points de vulnérabilité [09].

5- la phase d'Exploitation : l'exploitation, c'est le test final de la phase Conception. Cette dernière consiste au maintien de l'état opérationnel du réseau, grâce à des opérations de suivi quotidiennes, afin d'assurer une haute disponibilité et une réduction de dépense. La détection et correction de faute ainsi que la surveillance quotidienne de performances, optimisent le cycle de vie du réseau [09].

6- la phase d'optimisation : Cette phase est basée sur une gestion proactive du réseau, dont l'objectif est d'identifier et de résoudre les problèmes avant qu'ils ne se compliquent et que le réseau soit touché. L'opération de détection de défauts et le dépannage (troubleshooting) sont nécessaires lorsque la gestion proactive ne peut pas prévoir et corriger les anomalies [09].

V.3 Avantages de l'approche du cycle de vie

L'approche du cycle de vie du réseau réduit le coût totaux CAPEX et OPEX de la conception du réseau suivant les éléments énumérés ci-dessous :

- Identifier et valider les besoins en technologie
- la planification des changements de l'infrastructure et les ressources nécessaires
- Préparer les sites pour soutenir le système à mettre en œuvre et accélérer sa mise en œuvre
- Améliorer l'efficacité du réseau et les compétences du personnel
- Évaluer l'état de la sécurité du réseau et sa capacité à soutenir la conception proposée
- Spécification correcte de l'ensemble du matériel et des versions logicielles.
- Mise en service et test du système proposé avant le déploiement
- surveillé pro-activement les failles du système et les alertes, évaluer les tendances de disponibilité et définir des plans d'assainissement
- Améliorer la disponibilité, la fiabilité et la stabilité du réseau, et les applications tournant sur ce dernier

CHAPITRE VI

Etude comparatif de performance réseau MPLS et MPLS_diffserv sous OPNET MODELER

VI.1 Introduction

C'est quoi Opnet ?

OPNET est une famille des logiciels de modélisation et de simulation de réseaux s'adressant à différent public tel que les entreprises, les opérateurs et la recherche, OPNET Modeler est la version académique de cette famille il offre la possibilité de modéliser et d'étudier des réseaux de communications, des équipements, des protocoles et des applications avec facilité et évolutivité. OPNET est utilisé par les entreprises technologiques les plus performantes pour accélérer leurs procédés de recherches et développements.

L'approche orientée objet associée à des éditeurs graphiques intégrés d'OPNET simplifie la composition des réseaux et des équipements. Ceci permet de réaliser facilement une correspondance entre un système d'informations et le modèle correspondant.

OPNET est basé sur une série d'éditeurs hiérarchisés qui parallélisent la structure du réseau réel, des équipements et des protocoles [10].

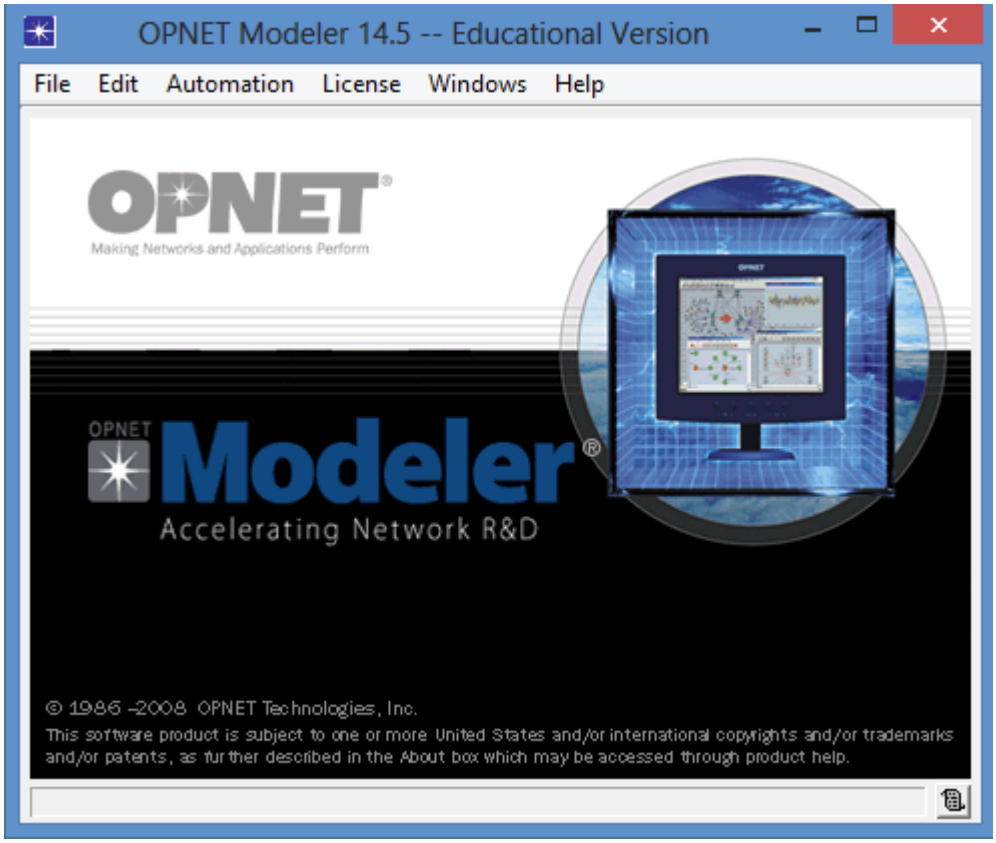

Figure VI-1 : Le logiciel Opnet Modeler (version 14.5)

Pourquoi Opnet ?

Notre choix d'OPNET Modeler se base sur le fait qu'OPNET est l'un des meilleurs logiciel de simulation de réseaux présent sur le marché, le seul problème d'OPNET c'est qu'il est payant mais ce problème est résolu avec la version académique, celle qu'on a choisi, puisqu'elle intègre tous les paramètres et protocoles qu'on en a besoin dans notre simulation, ainsi que son interface claire et conviviale présente un bon avantage pour utiliser ce simulateur [10].

VI.2 Mise en œuvre

Dans cette modélisation nous avons utilisé OPNET Modeler 14.5 pour comparer les performances de la technologie MPLS_Diffserv par rapport à MPLS traditionnelle, deux scénarios de cœurs de réseaux, en configurant (03) types d'application (Ftp, voice, video conférence),

VI.2.1 Modélisation d'un réseau MPLS

La première étape dans la modélisation d'un réseau est sa schématisation. Pour ce faire, nous avons implémenter une architecture du Backbone basé sur 9 routeur de cœurs (P) de réseau rattachés avec des liens E3 de capacité de 34 Mo, et deux routeurs Edge (PE) et rattachés au routeur core avec des liens E1 de 2 Mo, cette architecture et déployer avec le MPLS_Diffserv et MPLS afin de faire une étude comparatif entre les 2 scénarios et la qualité de service assuré par chaque technologie.

La figure IV-2 ci-dessous montre la topologie physique du réseau de cette simulation

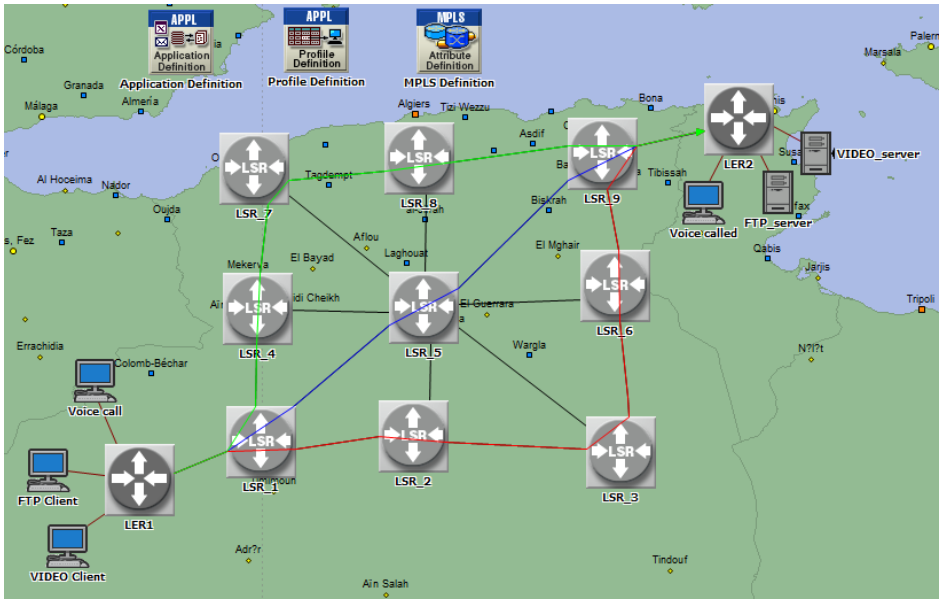

Figure VI-2 : Scénario1_Backbone MPLS

La figure VI-3 ci-dessous montre le réseau MPLS_diffserv, qui est le même que le réseau MPLS pour cette recherche en ajoutant l'objet QOS.

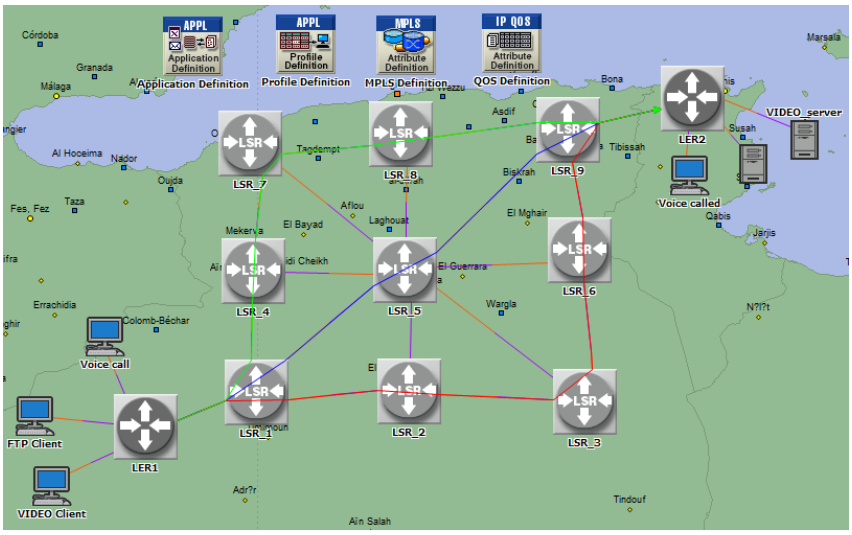

Figure VI-3: Scénario2_Backbone MPLS_diffserv

Le cœur du réseau MPLS est constitué de 09 P-Routeur qui sont représentés par les routeur LSR (Label Switch Routeur) sur opnet modeler.

Le réseau MPLS de distribution (MPLS Edge Network) est constitué de 02 PE-Routeur qui sont représentés par les routeur LER (Label Edge Routeur) sur opnet modeler. Les routeurs

VI.2.2 Configuration d'un réseau MPLS

- ✓ **Source de trafic :**

Les sources de trafic sont générées par les postes clients des objets (node) à partir de laquelle nous associons le profil d'application qui présente la configuration des applications multiples. Nous avons utilisé Ftp, voix et vidéo au sein de notre simulation.
Les figures ci-dessous montrent les valeurs choisies et les paramètres de notre modèle de trafic.

Trafic Ftp :

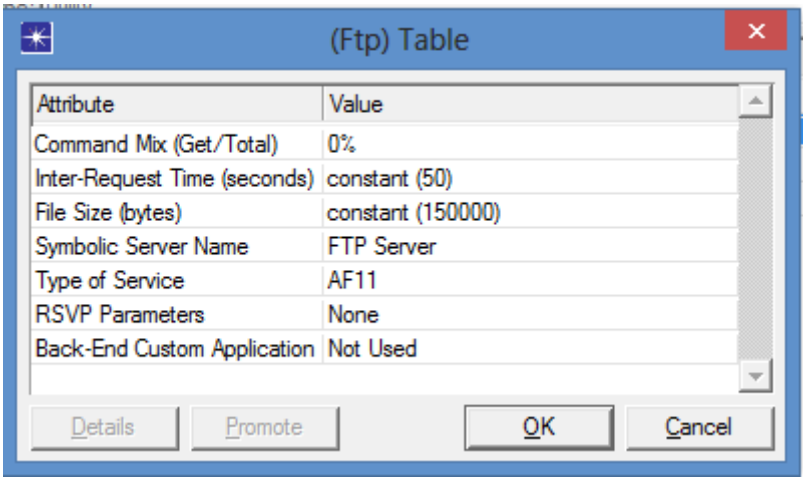

Figure VI-4 : Définition trafic FTP

Trafic Voice :

Pour le trafic voix, le codeur est de type GSM FR, le type de service AF31

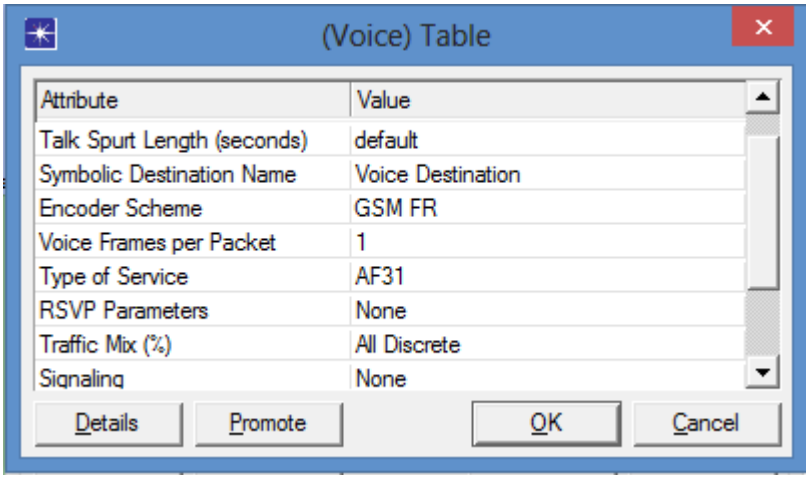

Figure VI-5 : Définition trafic voix

Trafic Video Conferencing :

Pour le trafic video , nous utilisons une résolution moyenne à 15 image/s (frame/sec) de 128x240 pixels, le paramétrage du champ DSCP à AF41.

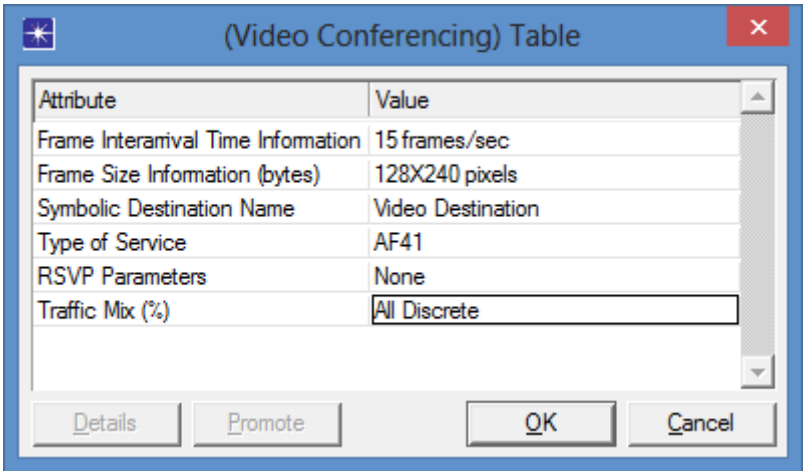

Figure VI-6 : Définition trafic video

- ✓ **DSCP to EXP Mapping :**

Le réseau que nous avons mis en place nous permet de réaliser une continuité de service entre les réseaux IP (représentant les réseaux locaux) et le réseau MPLS (représentant le réseau Opérateur).

Pour assurer cette continuité, nous utilisons le tableau de mapage DSCP à EXP

Ce principe consiste à copier la valeur du champ ToS d'IP dans le label EXP de MPLS. Il est utilisé par les routeurs LER (en entrée du réseau MPLS). Il assure la « translation » des valeurs de classe entre IP et MPLS.

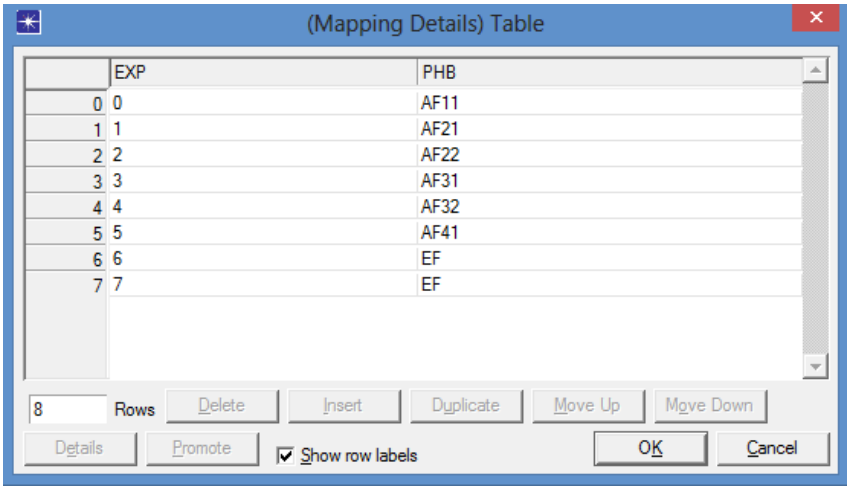

Figure VI-7: Translation DSCP à EXP

Une fois le réseau MPLS schématisé, il faut le configurer de telle sorte qu'il soit opérationnel selon des critères sélectionnés. Les étapes de configuration d'un réseau MPLS sont :

- la définition des FEC
- la définition des Trunks
- la définition des LSP
- configuration des commutateurs MPLS

✓ Définition des FEC

Une FEC se compose d'une ou plusieurs entrées permettant de spécifier un trafic. Pour chaque entrée, les adresses IP source et destination, les ports de transport source et destination, le type de protocole transporté ainsi que la valeur du champ ToS peuvent être utilisés pour cette spécification. Un LER recevant un paquet correspondant à la définition d'une des entrées d'une FEC acheminera ce paquet sur le LSP correspondant à cette FEC. Pour configurer les FEC qui seront utilisées dans notre simulation, il faut éditer l'attribut FEC Specification de l'objet MPLS Configuration

La figure suivante présente un exemple des différentes options permettant de caractériser le trafic recherché par la FEC

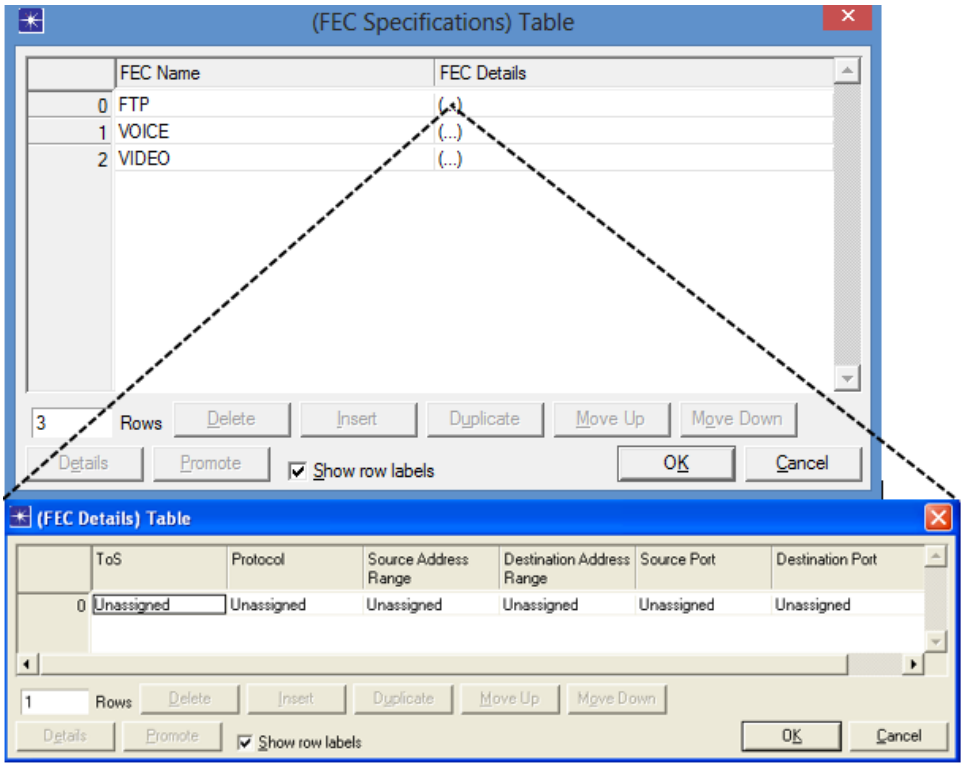

Figure VI-8 : Définition FEC

La valeur du champ ToS

Le champ ToS d'un paquet IP est constitué de 8 bits. La valeur de ce champ peut être configurée selon l'approche, telle que définie dans la spécification IP d'origine en utilisant quatre paramètres [RFC 791]. Ces paramètres sont Delay, Throughput, Reliability et Precedence. Le paramètre Precedence, définissant l'importance du datagramme, peut prendre les 8 valeurs suivantes : (0) Best Effort, (1) Background, (2) Standard, (3) Excellent Effort, (4) Streaming Multimedia, (5) Interactive Multimedia, (6) Interactive Voice et (7) Reserved.

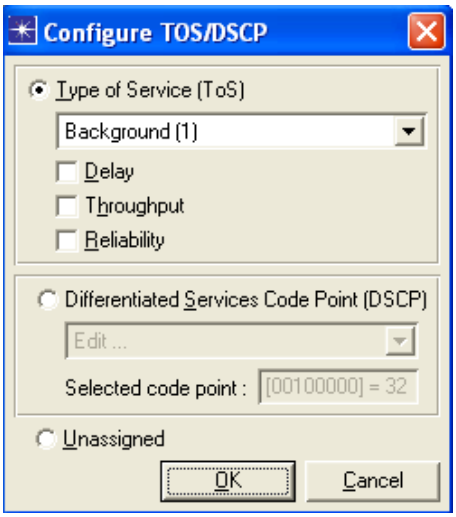

Figure VI-9: Configuration du champ ToS

Le champ ToS des paquets IP peut également être configuré avec l'approche DSCP (Differenciated Services Code Point) [RFC 2474] utilisée avec les réseaux IP supportant l'architecture de qualité de service Diffserv. Dans ce cas, le champ ToS prend une des valeurs définies pour les différentes classes de service de cette architecture. La valeur de ce champ peut alors être: Expedited Forwarding (EF), Assured Forwarding (AFl, AF2,AF3, AF4). Si la classe de service du paquet est AFl à AF4, il s'ajoute une valeur définissant la priorité d'être supprimé en cas de besoin: AFxl pour les paquets ayant priorité de ne pas être supprimés, AFx2 pour les paquets pouvant être supprimés au besoin, AFx3 pour les paquets de la classe x devant être supprimés en premier.

La valeur du champ Protocole

Il est possible de définir la valeur de champ protocole que doit avoir un paquet pour faire partie de la caractérisation de trafic de la FEC. La valeur de ce champ peut être : TCP, UDP, OSPF, IGRP, EIGRP, ICMP ou toute valeur numérique représentant le type de donnée transporté dans le paquet IP.

Les adresses IP source et destination

Cette contrainte permet de définir l'adresse d'origine et/ou de destination des paquets caractérisés par la FEC. Il est possible d'utiliser une adresse IP unique ou une adresse de réseau assortie d'un masque.

Les ports de transport source et destination :

Cette contrainte permet de définir 1' application ayant généré le trafic et celle à qui est destiné le trafic à 1' aide des ports de transports. La valeur de ce champ peut être :

Custom, Database, Email, Http, Ftp, Remote Login, X Windows, Video Conferencing, Print, Voice ou toute valeur numérique représentant un port de source ou de destination

✓ Définition des Trafic Trunk

Un *Traffic trunk* ne fait pas partie des fondements de la technologie MPLS. Dans un réseau MPLS sans ingénierie de trafic, les paquets caractérisés par une FEC suivent le LSP correspondant. Le *Trafic Trunk* est un concept relié à l'ingénierie de trafic. Pour déplacer le trafic là où il y a de la bande passante, la FEC n'associe par le trafic à un autre LSP, c'est le *Trafic Trunk* qui est associé à un autre LSP. Lorsque l'ingénierie de trafic est utilisée, la FEC associe un trafic à un *Trafic Trunk* qui est lui-même associé à un ou plusieurs LSP. OPNET impose l'utilisation des *Trafic Trunk.* Pour configurer ceux qui seront utilisés dans notre simulation, il faut éditer 1' attribut *Traffic Trunk Profiles* de 1' objet *MPLS Configuration.*

Dans la fenêtre de configuration des profils de *Trunk* (Figure 20) il faut choisir le nombre de profils que l'on désire configurer

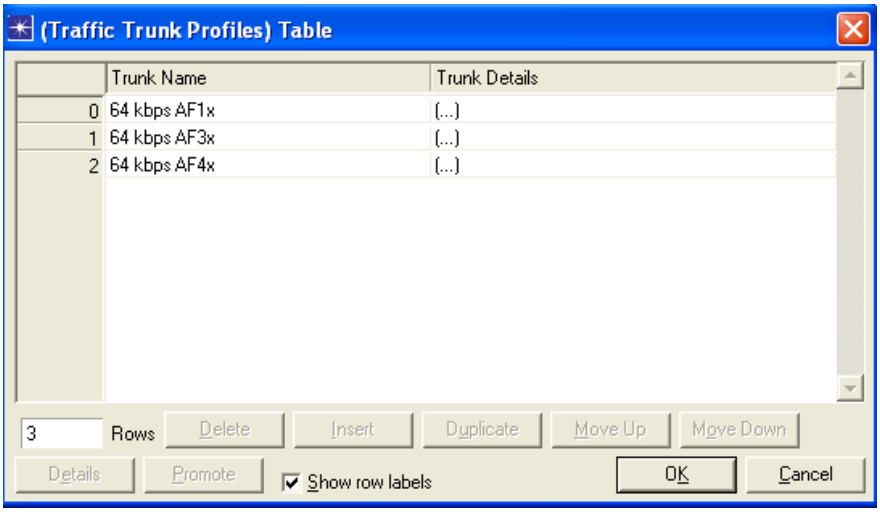

Figure VI-10: Table des profils de *Trunks*

Pour notre simulation, nous avons configuré un profil de *Trunk* pour le trafic voix et un autre pour video et autre pour FTP. Le profil de *Trunk* associé à la voix est caractérisé par un débit maximum et moyen quelconque. En effet sa capacité devra varier en fonction des besoins déterminés par la prédiction des besoins en bande passante déterminée par la fonction de contrôle d'admission. Le trafic excédentaire ne sera pas supprimé et la classe de service du *Trunk* est ***Expedited Forwarding*** afin d'assurer la bande passante désirée et de minimiser le délai et la gigue des paquets de voix.

Pour la video, un *Trunk* différent sera utilisé afin de marquer ce trafic avec une classe de service différente. Ce *Trunk* aura un débit maximum et moyen de 64000 bps. Le trafic excédentaire ne sera pas supprimé et la classe de service sera *Assured Forwarding* 41.

- ✓ **Association des FECs au LSP**

Chaque type de trafic doit être associé avec le chemin de commutation d'étiquettes spécifiques (LSP) correspondant, et qui transporte de trafic jusqu'au routeur PE de destination. L'association de trafic vers le LSP est effectuée sur le routeur de périphérique LER_1 (Traffic Mapping Configuration) (voir la figure ci-dessous)

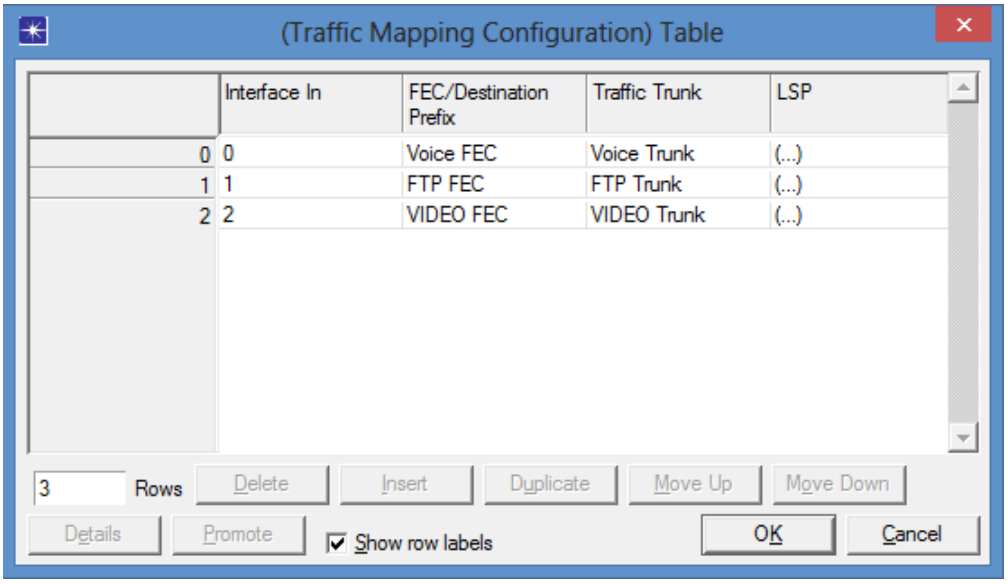

Figure VI-11: Association des FEC au LSP

Association des FECs au LSP pour le service FTP

Le trafic FTP sera acheminé à travers le LSP (en Vert) (LER1 → LSR_1 →LSR_4→LSR_7→LSR_8→LSR_9→LER2)

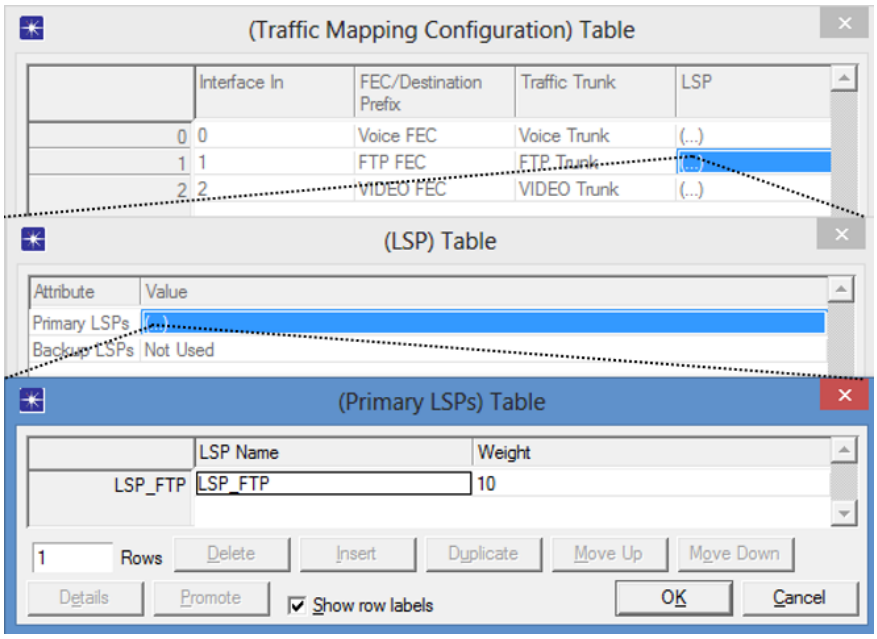

Figure VI-12: Association des FECs au LSP pour le service FTP

Association des FECs au LSP pour le service voix

Le trafic voix sera acheminé à travers le LSP (en Rouge) (LER1 → LSR_1 →LSR_2→LSR_3→LSR_6→LSR_9→LER2)

Le service voix n'a pas de LSP de Backup (en cas de coupure)

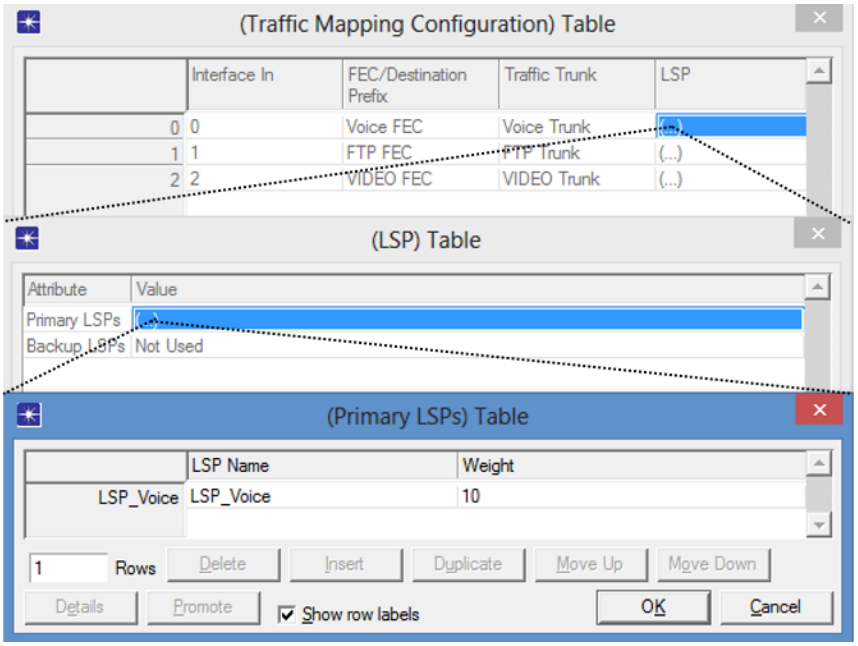

Figure VI-13: Association des FECs au LSP pour le service voix

Association des FECs au LSP pour le service video

Le trafic video sera acheminé à travers le LSP (en Bleu) (LER1 → LSR_1 →LSR_5→LSR_9→LER2)

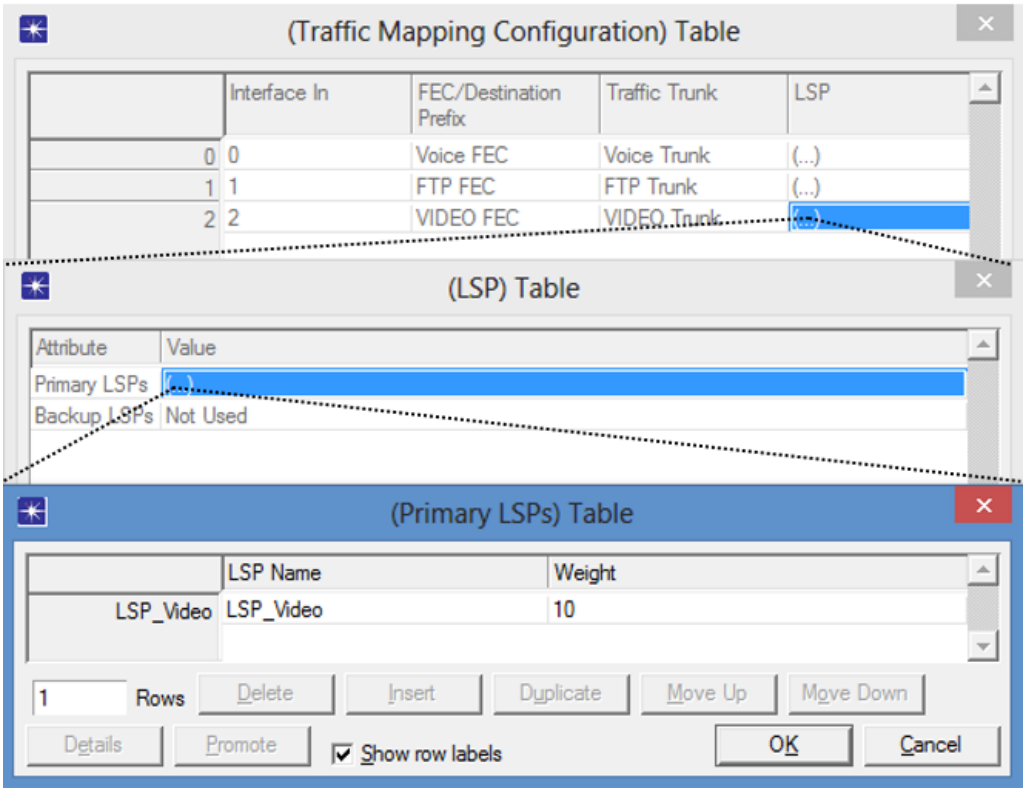

Figure VI-14 : Association des FECs au LSP pour le service video

- ✓ **Configuration des commutateurs MPLS**

L'activation de MPLS diffère suivant l'emplacement du routeur dans le backbone, dans les 9 routeurs P nous avons activé MPLS sur toutes les interfaces tandis que dans les 2 routeurs PE, MPLS est activé seulement sur les interfaces liant ces routeur aux routeurs P. Nous avons choisi le protocole LDP pour distribuer les labels MPLS.

VI.3 Analyse des résultats de simulation :

✓ Analyse du trafic FTP :

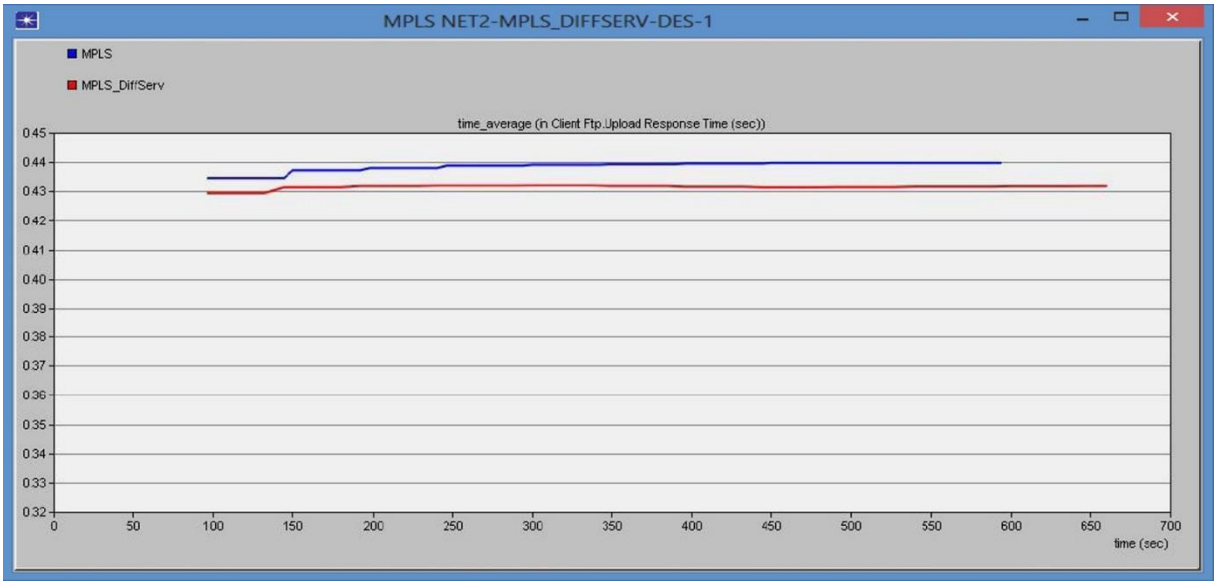

Figure VI-15 : Temps de réponse FTP avec light load (Blue – MPLS, Red – MPLS/DiffServ)

Le temps de réponse de MPLS est plus élevé que le réseau MPLS / DiffServ. Nous remarquons que le réseau MPLS avec DiffServ fournit une meilleure performance dans les temps de réponse pour le trafic basé sur FTP.

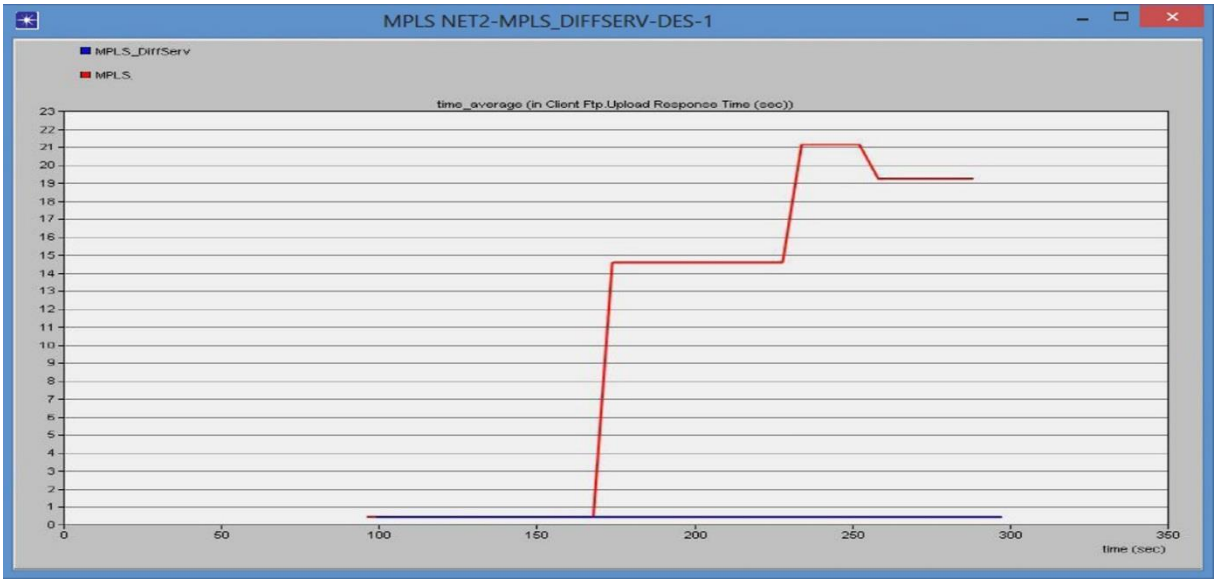

Figure VI-16 : Temps de réponse du trafic FTP avec heavy Load

(Blue – MPLS/DiffServ; Red–MPLS)

Après augmentation de la charge sur le réseau (heavy load), le temps de réponse pour MPLS passe à une valeur très élevée, mais DiffServ reste à peu près le même que celui indiqué dans la Figure VI-16 :

- ✓ **Analyse du trafic Voice :**

Ensuite, nous nous pencherons sur l'étude des performances du réseau lorsque le trafic est la voix. Nous allons comparer entre les deux scenarios MPLS et MPLS_ DiffServ. Figure VI-19 et Figure VI-20 illustrent les paramètres du retard de bout-en-bout pour le trafic light load et heavy load.

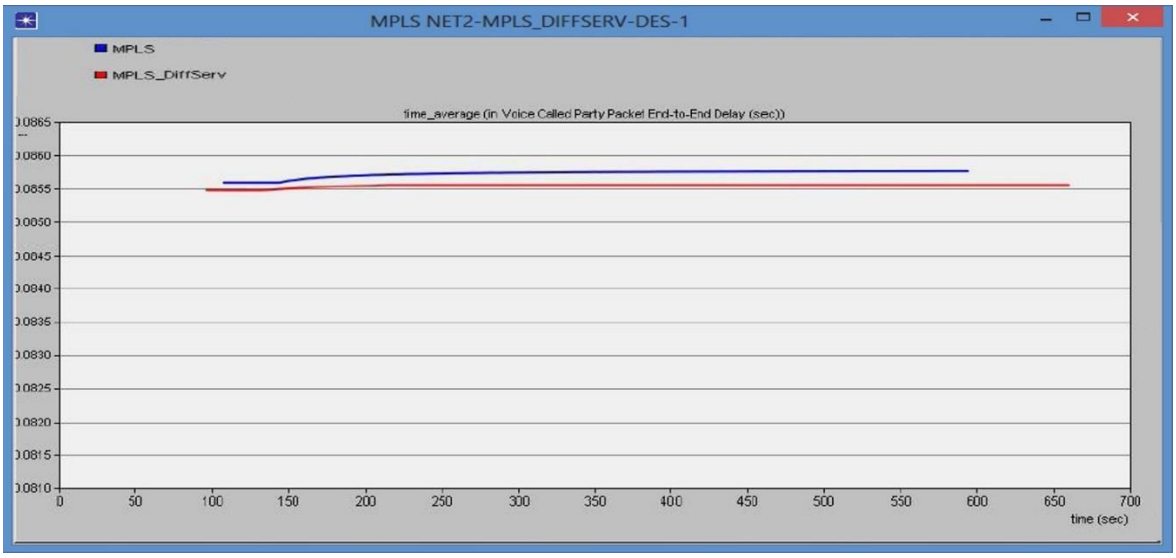

Figure VI-17 : Retard de bout en bout du trafic Voix avec light load

(Blue – MPLS; Red – MPLS/DiffServ)

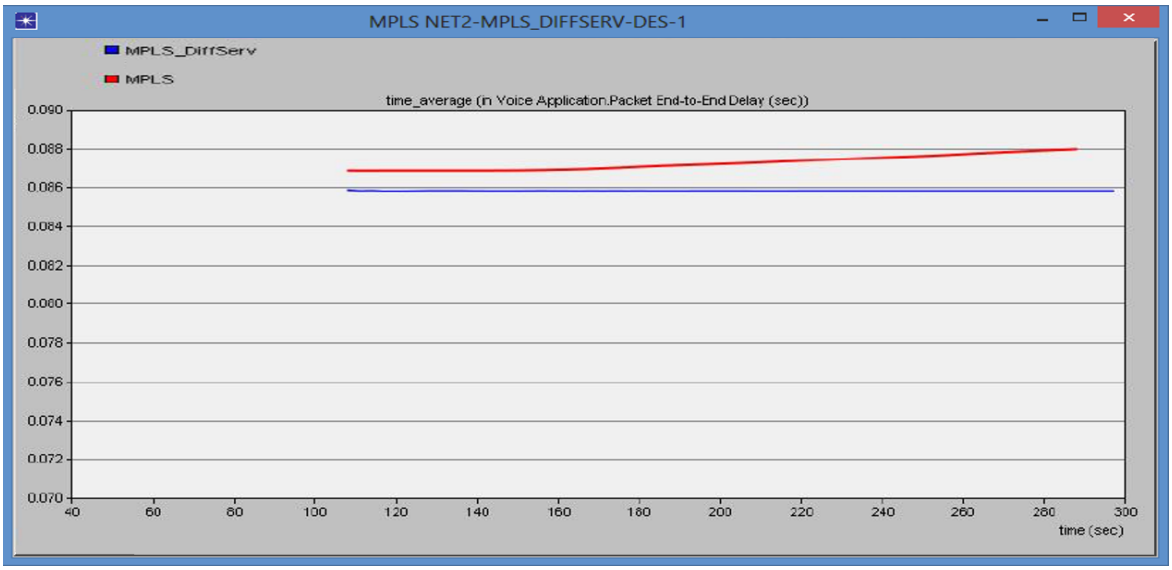

Figure VI-18 : Retard de bout en bout du trafic Voix avec heavy load

(Blue – MPLS/DiffServ; Red–MPLS)

Les figures VI-19 et VI-20 montrent les variations de retard (gigue) du trafic voix pour le trafic light load et heavy load.

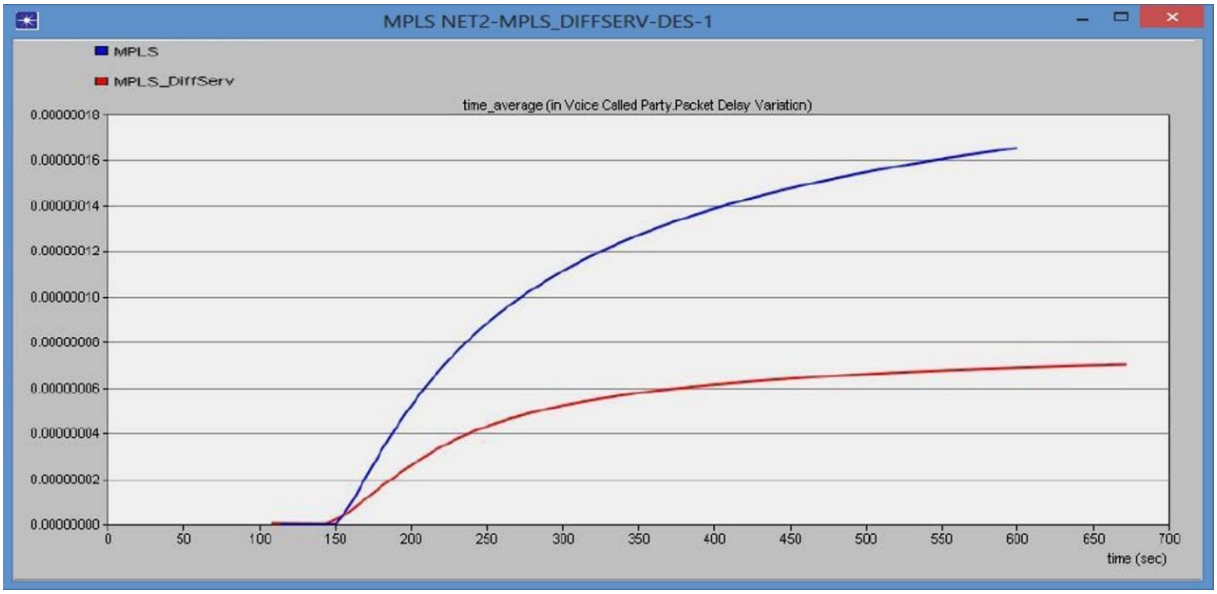

Figure VI-19: Variation du délai de retard (gigue) du trafic Voix avec light load

(Blue – MPLS; Red – MPLS/DiffServ)

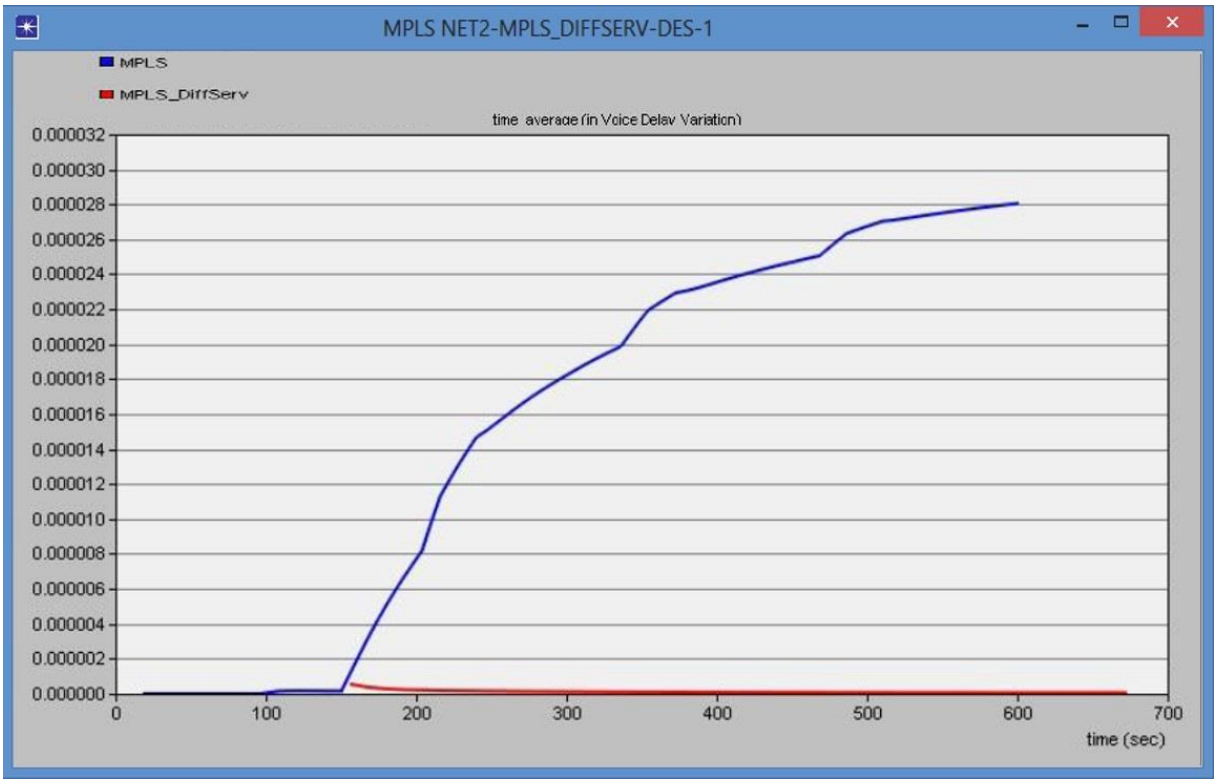

Figure VI-20: Variation du délai de retard (gigue) du trafic Voix heavy load

(Blue – MPLS; Red–MPLS/DiffServ)

✓ **Analyse du trafic Video :**

Par la suite nous étudions les performances du réseau lorsque le trafic est la Video. Nous allons comparer entre les deux scenarios MPLS et MPLS_ DiffServ. Ci-dessous, illustrent les paramètres du retard de bout-en-bout pour le trafic light load et heavy load.

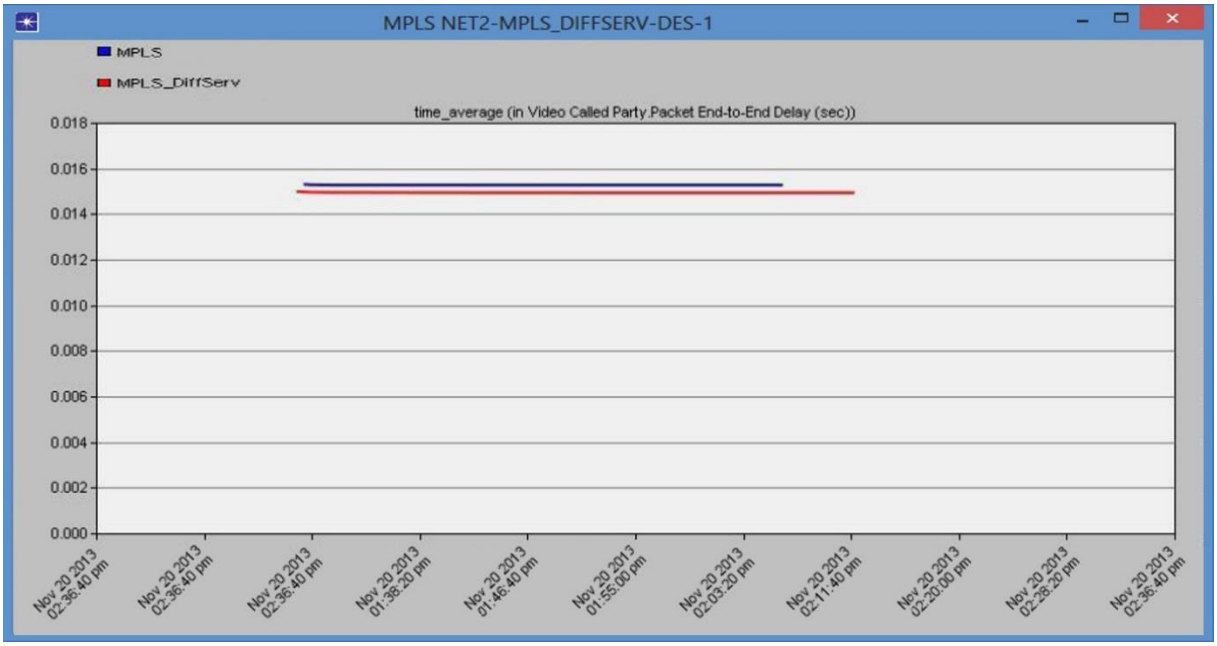

Figure VI-21 : Délai de bout en bout du trafic Video avec light load

(Blue – MPLS; Red – MPLS/DiffServ)

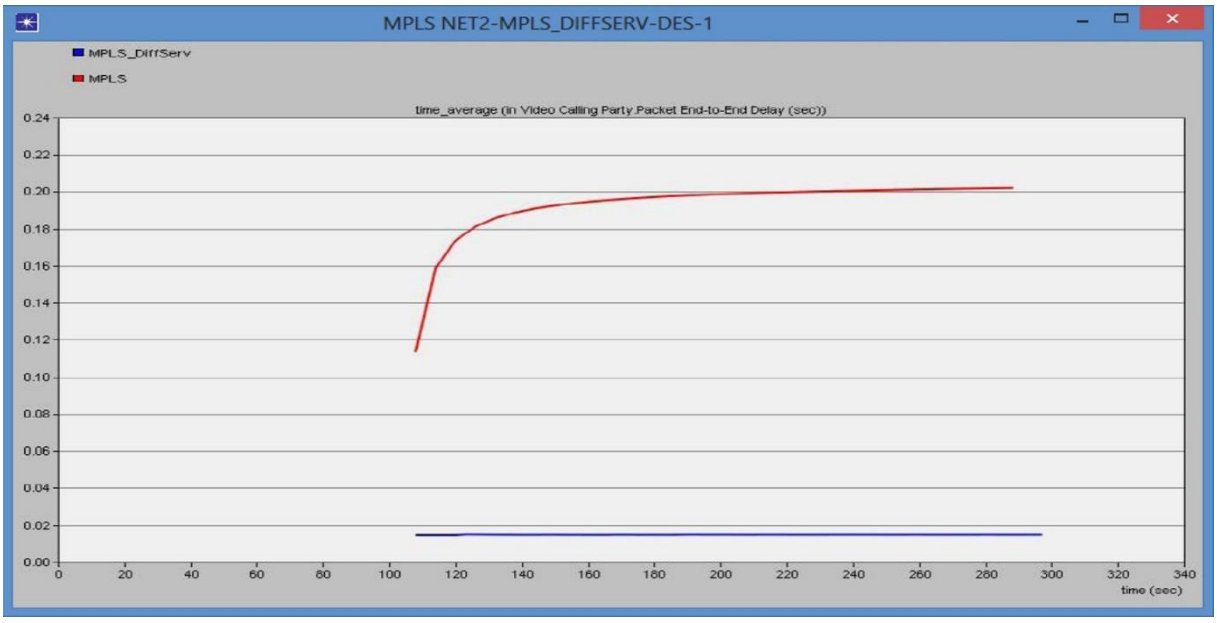

Figure VI-22 : Délai de bout en bout du trafic Video avec heavy Load

(Blue – MPLS/DiffServ; Red–MPLS)

Le délai de bout en bout pour le flux de données vidéo est plus élevé pour MPLS par rapport au MPLS / DiffServ. Après l'augmentation de la charge, le délai de bout en bout pour MPLS devient très élevé et ne cesse d'augmenter. Pendant que le retard MPLS / DiffServ reste à un niveau bas. Cela montre m2que MPLS / DiffServ offre une meilleure qualité de service même en réseau encombré avec des charges plus élevées, tandis que dans MPLS, le retard augmente à une valeur très élevée.

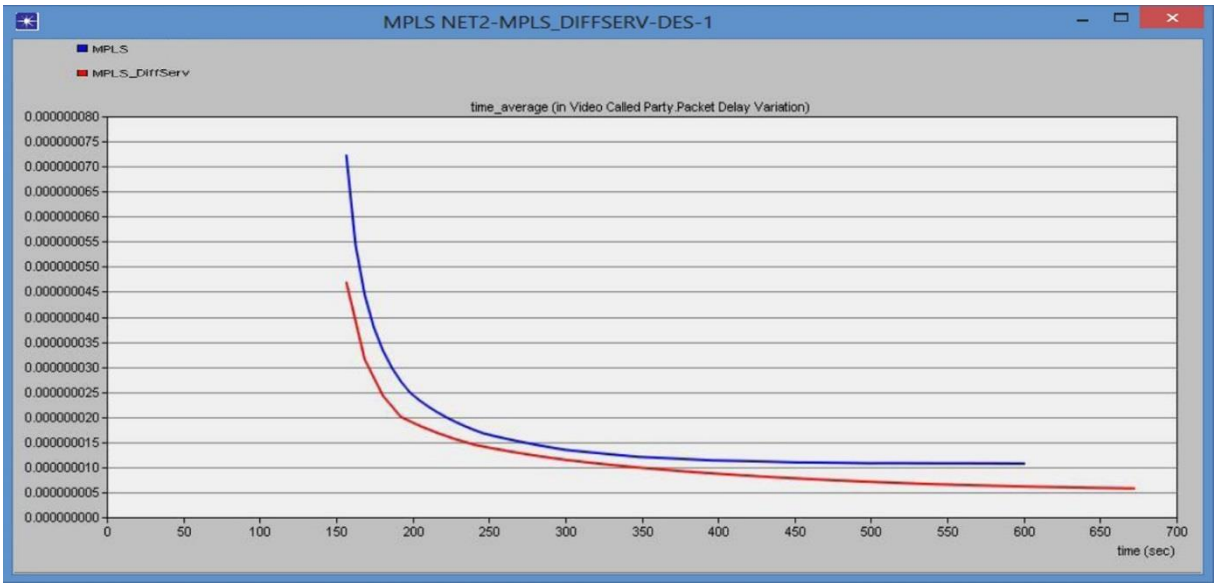

Figure VI-23 : Variation du délai de retard (gigue) du trafic video avec light load

(Blue – MPLS; Red – MPLS/DiffServ)

La variation du retard dans la figure VI-25 démontre la meilleure qualité du service MPLS / DiffServ.

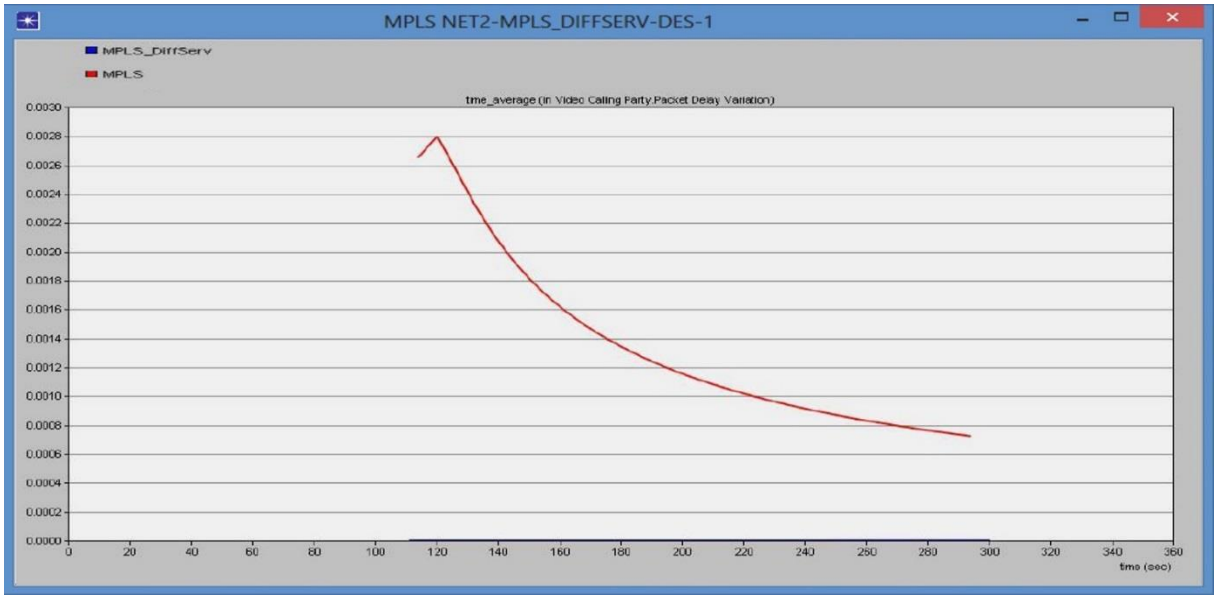

Figure VI-24 : Variation du délai de retard (gigue) du trafic video avec heavy Load

(Blue – MPLS/DiffServ; Red - MPLS)

Après l'augmentation de la charge du trafic, les résultats de la figure VI-26 : sont évidents que la variation de retard a augmenté à une très grande valeur pour MPLS, tandis que la variation du délai MPLS_ DiffServ est restée à une valeur très faible, en gardant la performance de qualité de service au niveau requis.

Les paramètres comparés étaient :

- Temps de réponse du trafic FTP (light / Heavy Load)
- End-to-End Delay du trafic video (light / Heavy Load)
- variation du retard avec le trafic vidéo (light / Heavy Load)
- End-to-End Delay du trafic voix (light / Heavy Load)
- variation du retarmd du trafic video (light / Heavy Load)

Pour tous les paramètres étudier ci-dessus, MPLS avec DiffServ démontre une meilleur performance autant sur le Heavy load que sur le light par rapport au MPLS.

Le temps de réponse du trafic FTP sur MPLS_ DiffServ avec un trafic (Heavy Load) était inférieur à celui du MPLS comme dans VI-15 et VI-16

Le retard des trafics voix et vidéo qui sont indiquées aux figures VI-17 à VI-24 démontre que MPLS / DiffServ à une valeur de retard inférieur à celle du MPLS ; la valeur du retard sur le modèle du (Heavy Load) devient beaucoup plus importante.

Les valeurs du retard dans le cas de la voix et de la vidéo est inférieur à 150 ms, selon la norme de l'UIT-T.

VI.4 Conclusion

Considérons dans nos simulations, que la combinaison entre DiffServ et MPLS présente une stratégie très attrayante pour les fournisseurs de service réseau puisqu'elle permet d'assurer le partage de charge et la qualité de service demandée par les clients. Toutefois, la gestion de ce type de réseau n'est pas une fonction simple et ne peut pas être réalisée manuellement.

Conclusion générale

Actuellement les opérateurs de télécommunication misent beaucoup d'investissements sur les réseaux de télécommunication modernes, vue leurs utilités, leur facilité d'utilisation et d'intégration de nouveau gammes de services et leur exploitation à faible coût.

Dans ce mémoire de magister, on s'est intéressé à l'ingénierie des réseaux de nouvelle génération – NGN, et à la mise en œuvre d'une simulation sous OPNET afin d'effectuer une étude comparative de performance entre les réseaux MPLS et les réseaux MPLS_diffserv avec intégration des services FTP, Voix et vidéo qui sont très répandues actuellement.

Ainsi, on a commencé au premier chapitre de situer notre sujet dans l'introduction aux réseaux NGN, puis au second chapitre, nous avons abordé les évolutions technologiques des cœurs de réseaux Ensuite, nous nous sommes attaqués en chapitre III au mécanisme de fonctionnement de l'architecture MPLS dans les réseaux étendu, ce qui nous a conduits au chapitre IV de présenté les réseaux de transport optiques. Dans le chapitre V nous avons vu intéressant de présenter une méthodologie de conception avec ces différentes phases pour un déploiement d'un réseau de télécommunication. Enfin, au sixième chapitre, nous avons fait une simulation sous logicielle opnet modeler 14.5 afin de faire une étude comparative de performance entre une architecture MPLS et MPLS avec diffserv.

Ce travail préliminaire nous a permis de nous initier sur le logicielle OPNET MODELER 14.5, ce nouveau Outil de recherche très réputé. Et de bien comprendre le principe du protocole MPLS et MPLS Diffserv.

Le MPLS offre aux opérateurs télécom des services adéquats à leurs attentes, au niveau de la garantie de transfert et la disponibilité de la bande passante. La gestion des flux de trafic, l'optimisation de la détermination de l'acheminement des paquets, la garantie de la bande passante constituent des améliorations conséquentes par rapport aux technologies utilisées pour les trafics traditionnels

Perspectives

Nous pensons que, pour approfondir les tests de déploiement de la technologie MPLS, il faudrait, en plus de tout ce dont nous avons fait jusqu'ici, se tourner vers la solution de tests avec les équipements matériels réels. Ce travail, loin d'être complet, pourra être amélioré dans tous les sens du terme, par qui conque qui s'y intéresserait.

Bibliographies & Références

[01] Ismail « Mise en œuvre d'un cœur de réseau IP-MPLS » par à l'institut national des télécommunications et des technologies de l'information et de la communication- Oran 2009.

[02] Oussama Foudhaili « Analyse des performances de MPLS en terme de "Traffic Engineering" dans un réseau multiservice », école supérieur des communications de tunis 2004/2005.

[03] Jean-Marc Uzé « VPLS : Virtual Private LAN Service » Juniper Networks

[04] Timothee Amega « Etude et Implémentation des Réseaux IP VPN MPLS », Cnam 2011.

[05] Mohamed Anouar Rachdi « Optimisation des ressources de réseaux hétérogènes avec cœur de réseau MPLS », l'Institut National des Sciences Appliquées de Toulouse, 2007.

[06] Annalisa Morea « Contribution à l'étude des réseaux optiques translucides : évaluation de leur faisabilité technique et de leur intérêt économique ». L'école nationale supérieure des télécommunications paris, 2006.

[07] Guide Réseau Fibre Optique étendu MAN – WAN – Réf 12/00-006 FR CREDO

[08] Jean-François Lalande « Conception de réseaux de télécommunications : optimisation et expérimentations », l'Université de Nice-Sophia Antipolis, 2004.

[09] Network Design Methodology, cisco Internetwork solution v2.1

[10] Ben Hassine Elyes et Morjen Fedia « Evaluation des performances VOIP sur le backbone de tunisie telecom », Univesité de Sousse 2009.

Liste des Abréviations

A

ACL Access Control Lists

ADSL Asymmetric Digital Subscriber Line

AF Assured Forwarding

ASCII American Standard Code for Information Interchange

ATM Asynchronous Transfer Mode

B

BA Behavior Agrégate

BBRR Bit by Bit Round Robin

BE Best-Effort

C

CBQ Class Based Queuing

CBR Constraint Based Routes

CB-WFQ Class Based Weighted Fair Queueing

CL Controlled-Load

CoS Class of Service

CR-LDP Constrained Routing-Label Distribution Protocol

D

DiffServ Differentiated services

DLCI Data Link Channel Identifier

DS Differentiated Services

DSCP Differentiated Services code point

DWDM Dense Wavelength Division Multiplexing

$\mathcal{E}$

ECN Explicit Congestion Notification

EF Expedited Forwarding

Exp Expérimental

E-LSP EXP-Inferred LSP

$\mathcal{F}$

FEC Forwarding Equivalent Class

FIFO First In First Out

FQ Fair Queueing

FRED Flow RED

$\mathcal{G}$

GPRS General Packet Radio Service

GS Guaranteed Service

GSM Globale System Mobile

$\mathcal{H}$

HTTP HyperText Transfer Protocol

$\mathcal{I}$

IETF Internet Engineering Task Force

IGP Interior Gateway Protocol

IntServ Integrated Services

IOS Internetwork Operating System

IP Internet Protocol

ISP Internet Service Providers

ITU International Telecommunication Union

$\mathcal{L}$

LDP Label Distribution Protocol

LER Label Edge Router

LLQ Low Latency Queueing

LSP Label Switch Path

LSR Label Switch Router

L-LSP Label-Only-Inferred LSP

$\mathcal{M}$

MF MultiField

MPLS Multi Protocol Label Switching

$\mathcal{N}$

NGN Next Generation Network

$\mathcal{P}$

PC Personal Computer

PHB Per Hop Behavior

PPP Point-to-Point Protocol

PPRR Packet by Packet Round Robin

PQ Priority queuing

$\mathcal{Q}$

QoS Quality of Service

$\mathcal{R}$

RED Random Early Detection

RESV RESerVation

RFC Request For Comments

RIO RED In and Out

RSVP Resource ReSerVation Protocol

RTC Réseau Téléphonique Commuté

RTCP Real-Time Transport Control Protocol

RTP Real-time Transport Protocol

$\mathcal{S}$

SDP Session Description Protocol

SIP Session Initiation Protocol

SLA Service Level Agreements

SLS Service Level Specification

SPT Shortest Path Tree

$\mathcal{T}$

TCA Traffic Conditionning Agreement

TCB Traffic Conditionning Bloc

TCP Transmission Control Protocol

TE Traffic Engineering

TOS Type Of Service

TTL Time To Live

$\mathcal{U}$

UDP User Datagram Protocol

UMTS Universal Mobile Telecommunications System

$\mathcal{V}$

VCI Virtual Channel Identifier

VPI Virtual Path Identifier

VPN Virtual Private Network

$\mathcal{W}$

WFQ Weighted Fair Queing

WiFi Wireless Fidelity

WRED Weighted Random Early Detection

Résumé

Durant ces dernières années, l'architecture de l'internet s'est développée, par l'introduction des nouvelles technologies, et ce afin d'assurer une adaptation aux nouveaux besoins.

L'introduction du protocole MPLS (Multi-Protocol Label Switching) a contribué au routage internet, à l'ingénierie du trafic et à la qualité de service requise pour l'introduction des nouveaux services.

Il serait intéressant de comparer les performances QoS des réseaux MPLS et MPLS / DiffServ, en prenant en compte leurs contraintes particulières.

Dans cette thèse, nous avons évalué les mesures de performance QoS tels que la variation de retard, le retard, temps de réponse, le débit pour différents types de trafics (voix, données et vidéo) pour les deux plateformes MPLS et MPLS / DiffServ.

L'objectif de cette thèse est de comparer les performances des réseaux MPLS et MPLS / DiffServ à l'aide d'une application de simulation de réseau bien connu «OPNET Modeler v14.5 », qui permettra de reproduire un véritable scénario de réseau réel, en utilisant les dernières techniques de simulation, où les différents paramètres de QoS peuvent être mesurés pour comparer les performances des réseaux.

Notre approche dans cette thèse, s'est de concevoir et de construire un cœur de réseau de type opérateur pour simuler un scénario réel qui véhicule les différents types de trafics (voix, données et vidéo).

Les résultats de la thèse sont présentés suivant le temps de simulation et la charge du réseau. Les résultats de la comparaison démontrent l'avantage sur la performance des réseaux MPLS avec diffserv par rapport aux réseaux MPLS traditionnelles.

Mots clés : OPNET, MPLS, réseau de nouvelle génération NGN

Abstract

In the recent years, the Internet architecture has evolved, incorporating new technologies and adapting to the changing needs of its use. The introduction of Multi-Protocol Label Switching (MPLS) as a part of the Internet forwarding architecture has immediate applications in traffic engineering (TE) and Quality of Service (QoS). It would be interesting to compare QoS performance of MPLS networks and MPLS/DiffServ networks, given their particular constraints. In this thesis, we evaluated the QoS performance measures such as delay variation, delay, page response time, throughput, for different types of traffics (data, voice, and video) for both MPLS and MPLS/DiffServ platforms. The aim of this thesis is to compare the performance of MPLS and MPLS/DiffServ networks using the well known network simulator application "OPNET Modeler". OPNET Modeler, v14.5, provides a platform to replicate a real world network scenario using latest simulation techniques, where different QoS parameters can be measured to compare networks performance. Our approach in this thesis is that, we have designed and built a National Carrier based core and edge network to simulate a real live scenario that spans in the Algeria , Some of the results in the thesis are presented against simulation time and some against network load. The results of comparing and evaluating these two core networks (MPLS and MPLS/DiffServ) through well know QoS parameters show that complimenting MPLS by Diffserv give better results than MPLS alone.

keys word: OPNET, MPLS, NGN,

ملخص الرسالة

في السنوات الأخيرة، تطورت الانترنت من ناحية تكوين البنية التحتية وذلك عن طريق دمج بعض التقنيات الجديدة وتكييفها لاستيعاب حاجة التقنية وتوافقها مع التغيرات المستمرة المتسارعة في العالم.

تقوم هذه الأطروحة بمقارنة شبكات MPLS مع شبكات MPLS with DiffServ من حيث الأداء باستخدام بعض المعايير المشهورة من معايير أداء الخدمة QoSوتشمل هذه المعايير الاختلاف في التأخير في الرزم المرسلة، التأخير في الرزم المرسلة، زمن استجابة الصفحة، الانتاجية، باستخدام رزم من عدة انواع (بيانات عادية، فيديو، و صوت.)وللقيام بهذه المقارنة ، جاءت الحاجة للبحث عن برنامج محاكاة يتيح لنا دراسة هذه الشبكات،حيث تم اختيار و استخدام برنامج المحاكاة المشهور. OPNET MODELER Release 14.5 :

تُقدم الأطروحة مُقدمة إلى تقنيات OPNET ، MPLS و MPLS/DiffServ ، وتصف منهجية المحاكاة ومقاييس الأداء.

في هذه الاطروحة تم بناء شبكة مشابة لشبكات ناقلي البيانات في الجزائر، ليتم عمل مقارنة للأداء بين كُلٍ من شبكات MPLS و MPLS/DiffServ عن طريق مقاييس الاداء QoS ، و تبين لنا ان اداء شبكات MPLS/DiffServ افضل من اداء شبكاتMPLS

الكلمات المفتاحية : OPNET, MPLS, NGN