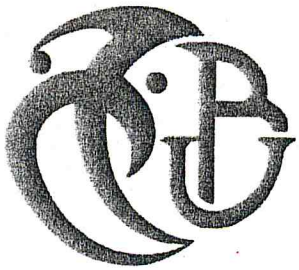
RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ SAAD DAHLEB-BLIDA



Faculté des sciences

Département informatique

Mémoire présenté par :

RIAHI FARAH

KIAS BESMA

En vue de l'obtention du diplôme de Master LMD

En informatique

Option :Génie des systèmes informatique

THÈME

MIGRATION D'UN RÉSEAU WAN/OSPF VERS UN RÉSEAU WAN/MPLS ET DÉVELOPPEMENT D'UN OUTIL DE SUPERVISION BASÉ SUR SNMP

ENCADREUR :

Mr AMMAR KHOUDJA SAMIR

PROMOTRICE :

Mme REZZOUG

PROMOTION 2012-2013

MA-004-164-1

Remerciement

En premier lieu, nous tenons a remercier le bon dieu de nous avoir munies du courage de la force, de la santé et de la patience pour surmonter toutes les épreuves rencontrées tout au long de nos études et de notre stage pratique .

Comme nous tenons a exprimer notre sincère gratitude et nos vifs remerciements a ***ZAHIDA****, malgré que ces mots ne suffisent pas pour une personne qui a fait l'impossible pour nous dés le début de notre stage pratique jusqu'au la fin ,sans elle ce travail ne verra pas ce jour .*

Nous adressons aussi nos remerciements a nos parents pour leur soutien matériel, financier, moral et psychologique. Mais particulièrement pour l'amour qu'ils nous portent .

Nous tenons a exprimer nos remerciements avec un grand plaisir et un grand respect au chef de département de réseaux et télécommunications ***Mr Messi*** *pour l'aide, es conseils précieux ainsi que le suivi pendant notre période de stage a* ***SONATRACH*** *.*

Nous tenons a exprimer aussi nos remerciements a notre encadreur ***Mr AMMAR KHOUDJA*** *pour l'encadrement dont nous avons bénéficie ,pour l'attention , la disponibilité dont il a fait preuve .*

Ainsi un très grand merci pour notre promotrice ***Mme REZZOUG*** *pour l'assistance qu'elle nous a témoignée, pour sa disponibilité pour ses orientations et conseils .*

Nos vifs remerciements a l'ensemble du personnel de la ***SONATRACH*** *et les employés de la Division Production le directeur* ***Mr BACHI*** *ainsi* ***Tata Souad,Tata sihem*** *et* ***hadjer .***

Nous tenons a nous remercier finalement toute personne qui a de prés ou de loin contribué d'une manière ou d'une autre au succès de ce travail

Dédicace

Je dédie ce mémoire a tous ceux qui m'ont très chers

A mes très chers parents

Je vous dois ce que je suis aujourd'hui grâce a votre amour ,a votre patience et vos innombrables sacrifices

Que ce modeste travail, soit pour vous une petite compensation et reconnaissance envers ce que vous avez fait d'incroyable pour moi

Que dieu le tout puissant, vous préserve et vous procure santé et longue vie afin que je puisse a mon tour vous combler

Je ferai de mon mieux pour rester un sujet de fierté a vos yeux avec l'espoir de ne jamais vous décevoir

A ma très chère grande mère yema

Que dieu vous garde et vous alloue bonne santé, bonheur, prospérité et longue vie

A mon très cher frère CHAWKI que je l'aime très fort .

En souvenir de nos éclat de rire des bons moments et de tout ce qu'on a vécu ensemble

A ZAHIDA

Aucune dédicace ne serait exprimer assez profondément de que je ressens envers vous

Je vous dirais tous simplement un grand MERCI

A mon très cher oncle et sa femme el Alia

A toute mes tantes maternelles et paternelles

A tout mes cousins et toute mes cousines

En souvenir de toute les joies et forces qui unissent notre chère famille a Meryem, Iméne ,Houda

farah

Dédicace

Je tiens a dédié ce mémoire a mes très chers parents

Pour tout l'amour dont vous m'avez entouré, pour tout ce que vous avez fait pour mi

Que ce modeste travail, soit l'exaucement de vos veux tant formulés et de vos prières quotidiennes

A mes très chères sœurs

Nesrine, Mouna ,manel et Aida

A mon cher frère

Bachir

A mes tantes maternels et paternelles

A ma très chère grande mère

Que dieu vous garde et vous alloue bonne santé, bonheur, prospérité et longue vie

Besma

1.Introduction générale :

A l'origine, un réseau était un rassemblement de personnes ou d'objets. De nos jours on entend par réseau, les réseaux d'entreprises, qui connectent différentes machines afin de pouvoir les faire communiquer entre elles. Que ce soit pour le partage de fichiers ou l'envoi de messages, la plupart des entreprises sont aujourd'hui dotées d'un réseau afin d'être plus efficientes .ces réseaux sont classés selon leur portée et selon leur échelle au niveau de l'entreprise en réseau LAN qui présente le réseau interne d'une entreprise , et le réseau WAN qui relie plusieurs LAN sur des grandes distances .

De nos jours, bon nombre d'entreprises disposent des réseaux de transmission de données basé sur des protocoles routés et des protocoles de routages , ils sont ces jargons spécialisés qui sont utilisés par les divers équipements d'un réseau pour accomplir leurs tâches.

Le protocole qui s'est imposé comme le langage universel est le protocole IP (Internet Protocol) , ainsi que le TCP qu'est souvent associé a IP afin d'assurer la transmission fiable des données, ces protocoles routés sont acheminer grâces au protocoles de routages statiques ou dynamiques tel que le *RIP, IGRP, OSPF, BGP et EIGRP*..Ces protocoles permet d'établir une route de plus court chemin en terme de distance ou de délai entre deux nœuds source et destination .

Dans le cadre d'une qualité de service, le but du protocole de routage est de trouver la meilleure route selon les critères précis de la qualité de service souhaitée (délai, taux de perte, quantité de bande passante, ...), et reposant sur des liens fiables.

Avec le développement des usages d'Internet - téléphonie haute définition, e-mails et Internet ou centralisation des applications, la qualité de service ou QoS est devenue primordiale pour le bon fonctionnement des entreprises .

Les réseaux IP établissent l'architecture *best-effort .cette dernière* ne permet pas de garantir une quelconque qualité de service et il a été nécessaire de définir de nouvelles architectures de réseaux pour répondre à ces nouveaux besoins. De cette nécessité sont nées les architectures à intégration de service tel que les réseaux ATM (Asynchronous Transfer Mode), et le modèle IntServ (*integrated services*) pour les réseaux IP qui s'appuient sur une réservation, et plus récemment le modèle DiffServ (Differentiated Services) qui effectue un traitement

différencié des trafics, regroupés en quelques classes de services, pour garantir la qualité de service.

Toutefois, les technologies utilisées jusqu'à maintenant n'étaient pas optimales concernant la gestion des réseaux, et ne répond pas aux exigences des entreprises ,Cela conduit a un choix d'une technologie hautement performante induisant le moins des taches administratives possible.

2.Contexte et motivation :

Pour mettre en valeur plus sur les problèmes rencontrés par les entreprises et de sensibiliser la technologie qui répondent a leur exigences, nos études ont inclus les travaux sur la qualité de service ainsi les différents protocoles existés jusqu'à maintenant nous avons arrivé a proposer une solution logicielle ainsi d'orienter notre choix vers le protocole MPLS comme la meilleure solution qui répond besoins des entreprises .

La société SONATRACH qui occupe une place incontournable dans l'économie de notre pays avec son réseaux vaste, qui nécessité une interconnexion entre les différents sites situé dans des zone géographiquement éloigné présente un parfait endroit ou nous pouvons prouver notre proposition on appliquant sur son réseau le protocole MPLS et notre approche développé .

3.Problématique :

Les réseaux d'entreprises actuels reposent pour la plupart sur le plus connu des protocoles, à savoir Internet Protocol (IP). Avec le temps, ceux-ci ont révélé leurs atouts mais surtout leurs faiblesses, liées au format même du protocole et à sa spécification. Nous présentons ci dessus quelques lacunes qu'on pourra rencontré dans un réseau d'entreprise :

- **Problème lors de l'expansion** : lors de l'ajout d'un nouveau site dans le réseau on doit réaménagé les tables d'adressage pour qu'ils prennent en charge ce site.
- **La redondance** :avec l'accroissance du nombre de sites connecté a l'entreprise, cette dernière rencontre le problème que deux sites distants ont le même champs d'adresses .

- Besoin de l'extension de certaines technologies, comme la VoIP nécessitant d'avoir un faible délai .La majorité des entreprises possèdent un réseau incapable de supporter ce genre de trafic sans mécanisme de la Quality of Service(QoS) .
- Le besoin de plus grandes performances ou d'un meilleur rapport qualité/prix au niveau des routeurs.
- **Besoin d'augmenter la bande passante** pour les applications déployées au entreprise .
- **Le besoin d'un système de sécurité réseau** qui permet cette dernière de connecter en toute sécurité des bureaux et des utilisateurs distants par le biais d'un accès Internet tiers et peu coûteux .

4.Objectif de mémoire :

L'objectif de notre travail est de palier aux lacunes des réseaux ,on proposant une solution destinée a palier certaines faiblesses du protocole IP en assurant une interconnexion flexible et évolutive entre les différents sites, une sécurité améliorée avec une gestion du trafic efficace ,mais aussi, l'introduction nécessaire d'une bonne politique de Qualité de Service (QoS) .

5.Contenu de mémoire :

Notre mémoire sera organisé comme suit :

- ***Chapitre 1*** : Nous étudierons dans ce chapitre les différents protocoles de la couche 2 et 3 du modèle OSI ,afin de justifier le choix du protocole MPLS .
- ***Chapitre 2*** :Ce chapitre décrit en détail un des principaux application du protocole MPLS qui est la qualité de service Nous définissons dans un premier temps la notion de qualité de service ces caractéristiques , ces classes de services ainsi la gestion de la QOS dans les réseaux IP nous présenterons aussi les travaux ayant déjà été effectués dans le domaine de la qualité de service dans les réseaux IP .

- ***Chapitre 3*** :la première partie de ce chapitre contient une présentation de l'organisme d'accueil qui est la SONATRACH, en particulier le réseau WAN de cette dernière, dans la deuxième nous préciserons le besoin d'amélioration de ce réseaux, et la solution qu'on proposera coté protocole appliqué et approche développé qui permet d'améliorer la QOS dans les réseaux MPLS.
- ***Chapitre 4***:ce derniers chapitre contient des tests et des résultats .
- ***Conclusion générale :*** Nous terminerons avec une conclusion générale qui est une synthèse de tous les aspects abordés lors des différentes étapes de cette étude,

Introduction :

Dans le cadre des Réseaux à large distance (WAN-Wide Area Networks), il existe plusieurs protocoles destinés à transporter des données informatiques. Les nouveaux challenges des grandes entreprises qui sont dotées de ce type de réseaux consistent à améliorer leur sécurité et leur qualité de service en s'adaptant aux différents types de médias utilisés ainsi qu'aux impératifs grandissants en matière de trafic, d'optimisation de la bande passante, de contrôle du temps de latence et des délais d'acheminement ainsi que de réduction des pertes de données...

Nous allons décrire dans ce chapitre quelques protocoles de liaison, leurs limites et développements ainsi que leurs principaux avantages et inconvénients afin de justifier le choix de la technologie MPLS.

I-1 -Asynchronous Transfer Mode "ATM ":

I-1-1.Présentation :

ATM est né du besoin des opérateurs téléphoniques de disposer une technologie leur permettant de véhiculer la voix, les données et l'image sur un même réseau. Avec la panoplie des réseaux, ATM étant la technologie permettant le transport simultané de la voix, des données et la vidéo quelque soit le types de réseaux. Cette technologie est utilisable à la fois sur les réseaux locaux et distants[1] .

ATM se positionne comme une technologie universelle des réseaux de communication avec des débits allant de quelque Méga à plusieurs Giga bits par seconde "dispose d'un débit a 2,4 Gbits en 1998 ": d'où la possibilité de négociation de Qualité de Services. Ce concept a été mis en avant pour être le protocole de la couche réseaux [2] .

C'est un mode de communication dit « asynchrone » car il transmet les données par paquets, en fonction de leur arrivée en provenance des applications, sans imposer de synchronisation entre le débit de la source et le train de paquets circulant sur la liaison d'accès au réseau [3].

ATM n'étant pas basé sur un type spécifique de transport, il est compatible avec tous les réseaux physiques déployés actuellement. ATM peut utiliser des supports de type coaxial, fibre optique ou cuivre (paire torsadée) [3].

I-1-2.Fonctionnement :

ATM fonctionne en mode connecté, contrairement à Ethernet. Avec Ethernet, lorsqu'un utilisateur envoie des données à une autre personne à travers le réseau, ces données sont répétées par un concentrateur (hub), autant de fois qu'il y a de postes connectés à ce concentrateur. Ces données sont constituées en fait de paquets de 1516 octets au maximum, chacun contenant l'adresse du destinataire (adresse MAC). Lorsque les données arrivent sur un poste, l'adresse MAC contenue dans le paquet est comparée avec celle de la carte réseau du poste. S'il y a concordance, les données sont alors réceptionnées par le système [4] .

Le problème avec Ethernet est qu'un tel système basé sur la duplication des données peut provoquer des collisions qui engorgent inutilement le réseau. La technique ATM, en revanche, réduit considérablement ce danger grâce au mode connecté. Cela signifie qu'ATM met en œuvre des connexions point à point d'un ordinateur à un autre, qu'on appelle « circuits virtuels », les données ne sont pas dupliquées au niveau des concentrateurs du réseau, qui sont en fait des commutateurs. Le mode connecté établit une liaison unique et directe entre celui qui envoie les données et le destinataire .Les données prennent la forme de paquets qu'on appelle cellules de 53 octets (taille fixe) contenant l'adresse du destinataire. Dans ces 52 octets, 48 octets de la cellule sont utilisés pour les données elles-même, et 5 octets sont utilisés pour le contrôle de la transmission. Le principal intérêt d'ATM réside dans cette structure de données, l'utilisation de blocs de longueurs fixe permet de prévoir les délais nécessaires pour des applications en temps réel. Les très petits blocs conviennent pour les transmissions de la voix et de la vidéo, les grands blocs pour la transmission des données. Le format ATM qui s'inscrit entre ces deux tailles convient pour toutes ces tâches. ATM fournit donc un support unique pour la transmission des données et les applications multimédias dans des environnements LAN et WAN [4] .

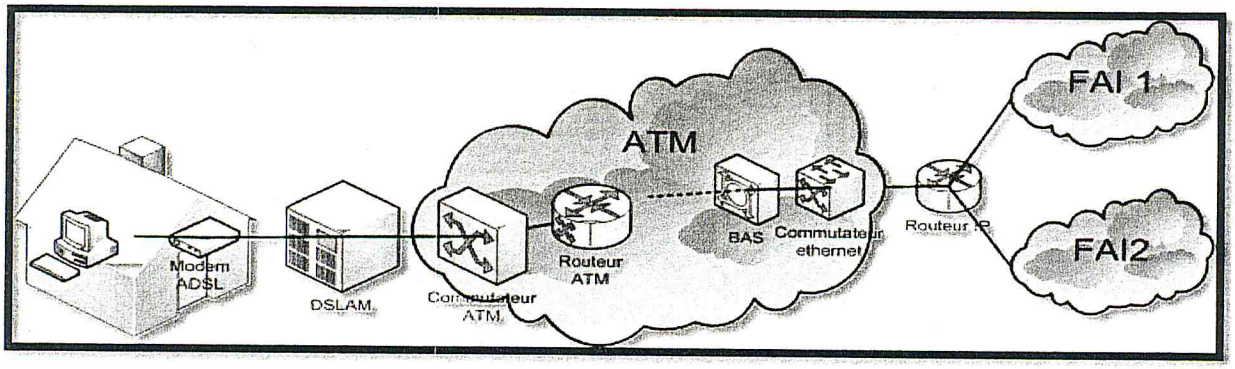


Figure I-1:Le protocole ATM [5]

I-1-3.Les avantages d'ATM :

- Qualité de service garantie pour les connexions (bande passante, délai, fluctuation de délai) [|6].
- Supporter tout types de commutations (voix, donnée et la vidéo) sur un même réseau [7].
- Distributeur de billets est aussi orienté connexion et fournit des données sur *des circuits virtuels* qui livrent des cellules dans l'ordre, une condition importante pour l'audio en temps réel et de la vidéo [1].
- Offrir le même service de bout en bout quelque soit le type des réseaux [1].
- Fonctionner à très haut débit de quelque Mbits/s à quelque Gbits/s [1].

I-1-4.Les inconvénients d'ATM :

- Inefficace pour le trafic de datagrammes .
- Un circuit virtuel par paire source/destination n'est pas *scalable*, $O(n^2)$ connexions nécessaires pour un réseau de n hôtes .
- L'établissement des circuits introduit une latence, ce qui peut être préjudiciable pour des connexions de courte durée [6].

L'ATM permet de garantir une relative qualité de service mais la longueur des cellules ATM étant fixe, les paquets doivent être segmentés, transportés et remontés sur un réseau ATM en utilisant une couche d'adaptation. Ce qui ajoute à la complexité et les coûts indirects importants dans le flux de données.

Les protocoles utilisés Afin de garantir la qualité de service au niveau 3 sont les suivants :

I-2-Le protocole RSVP :

I-2-1.Présentation :

Le RSVP (Resource ReSerVation Protocol) avait été conçu par L'IETF [AN01] en 1995 pour la réservation de ressource au sein d'un réseau Internet. Il peut être utilisé pour assurer la qualité de service et gérer les ressources de transport du réseau pour les sessions point à point (unicast) et point à multipoint (multicast). RSVP est un système de contrôle et de signalisation qui donne la possibilité de réserver la bande passante nécessaire au bon fonctionnement d'une application. C'est un besoin qui touche principalement les flux multimédias, plus sensibles aux aléas de l'acheminement que les flux de données pures du fait de leurs contraintes temporelles [8] .

RSVP a été présenté en 1995 à Interop [AN02], une démonstration mettant en scène des ordinateurs recevant du son et des images. Il a été prouvé qu'à travers un réseau Internet, même chargé, la qualité de la transmission de la vidéo et du son était bonne lorsque les données étaient acheminées via des sessions RSVP. Sans les mécanismes de réservation fournis par RSVP, les présentations devenaient inintelligibles [8].

I-2-2.Fonctionnement :

RSVP rend obligatoire la demande de QoS par le récepteur (l'application participante) plutôt que par l'émetteur (l'application source). Le récepteur apprend les spécifications du flux multimédia par un mécanisme hors-bande. Le récepteur peut ainsi faire les réservations qui lui sont appropriées. Cela est très utile dans le cas d'une transmission multicast. En effet, dans le cas où on aurait prévu que la demande de ressources soit faite par l'émetteur, une QoS identique à tous les émetteurs aurait été mise en œuvre et n'aurait pas été adaptée aux besoins

du récepteur. D'autre part, certains émetteurs auraient eu tendance à toujours demander la réservation la plus importante qui aurait nui au système dans sa globalité. Le fait que le récepteur décide des ressources dont il a besoin permet une facturation différenciée par récepteur [9].

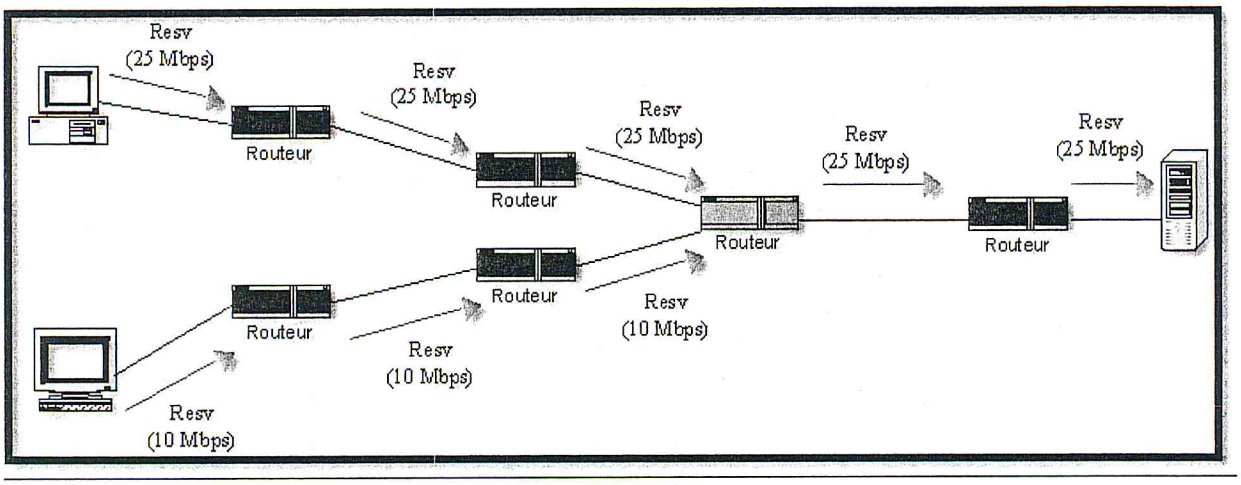


Figure I-2:Le protocole RSVP[9]

Les équipements d'interconnexions (routeurs), sur le chemin du flot des données, répondent aux requêtes RSVP , établissent et maintiennent les connexions. Les routeurs communiquent via RSVP pour initialiser et gérer la QoS réservée aux sessions [9] .

I-3-Le modèle Intersev/RSVP :

I-3-1.Présentation :

Le modèle IntServ (*integrated services*) définit une architecture capable de prendre en charge la Qualité de service (QoS) en définissant des mécanismes de contrôle complémentaires sans toucher au fonctionnement IP. C'est un modèle basé sur un protocole de signalisation RSVP. qui induit alors une couche de contrôle d'admission supplémentaire pour s'assurer que la bande passante requise est bien disponible à un instant T[10] .

IntServ avait pour objectif de migrer vers des échanges temps réel de bout en bout. Ainsi, il fallait apporter des solutions pour les réseau local et les réseaux d'accès ainsi le cœur de l'Internet [10] .

IntServ suppose que pour chaque flux demandant de la QoS, les ressources nécessaires sont réservées à chaque bond entre l'émetteur et le récepteur. IntServ requiert une signalisation de bout en bout, assurée par RSVP, et doit maintenir l'état de chaque flux. IntServ permet donc une forte granularité de QoS par flux et pour cette raison, est plutôt destiné à être implémenté à l'accès [11] .

I-3-2.Fonctionnement :

Services intégrés (IntServ). La méthode de la QoS IntServ fournit une garantie de service avec un délai de quantifier et de gigue normes. Le protocole IntServ utilise de bout en bout de signalisation et de réservation de ressources avec trois niveaux de services:

1. Service garanti en charge les applications temps réel et offre une connexion garantis par des normes pour la perte de paquets, les retards et la gigue qui ne peuvent pas être dépassées.

2. Contrôlée charge de service est le deuxième niveau supérieur de IntServ et est destiné à des applications qui peuvent tolérer un certain retard.

3. Best Effort Service fournit aucune garantie de service [12] .

Dans un réseau utilisant le protocole IntServ, tous les routeurs du réseau doivent mettre en œuvre IntServ, et toute demande qui nécessite un niveau de qualité de service doit réserver des ressources pour le service. Le protocole RSVP effectue la fin de signalisation à la fin et entre les routeurs. Il ya des problèmes avec IntServ telles que l'évolutivité pauvres. IntServ fonctionne bien dans de petits réseaux, mais dans les grands réseaux comme Internet, il est difficile de garder trace de nombreuses réserves. Il pourrait y avoir des milliers de réservations pour certains routeurs. Par conséquent IntServ est souvent recommandé pour les utiliser que dans les réseaux de pointe à l'intérieur du noyau du réseau, d'autres protocoles se réserve ressources en agrégats. Un autre problème est que IntServ doublons certaines des fonctions de RTP comme le contrôle de la gigue[12] .

I-3-3.Les avantage du modèle IntServ :

- Services proches des différentes types d'application .
- Conçu pour fournir des garanties absolues .
- Le flot peut être contrôlé par le routeur .

- QoS pour unicast ou multicast .
- Styles de réservation tendent à augmenter le taux d'utilisation des ressources réservées [13] .
- Adaptation « automatique » au changement de routes [13] .

I-3-4.Les inconvénients du modèle IntServ :

- Pas plus de 300/400 postes (pas "scalable") [14].
- Nécessite la prise en charge du protocole RSVP par les routeurs [14].
- Service de bout en bout garanti si tous les routeurs sont Intserv [13].
- Impraticable pour les flots à durée de vie courte [13] .
- Facturation du service complexe [13].

Intserv est très complexe à mettre en œuvre, il convient plutôt aux réseaux de petite taille, mais n'est pas vraiment adapté à Internet dans son ensemble. De ce fait, il a été peu déployé. Pour pallier à ces carences, l'IETF a adopté un second modèle DiffServ .

I-4-Le modèle DiffServ :

I-4-1.Présentation :

DiffServ ou Differentiated Services est une architecture réseau qui spécifie un mécanisme pour classer et contrôler le trafic tout en fournissant de la qualité de service (QoS)[15] .

Au contraire du modèle Intserv qui traite indépendamment chaque flot, le modèle diffserv propose de séparer le trafic par classes grâce à un code présent dans le paquet IP. Nous avons donc affaire à une granularité moins fine mais qui devient en revanche plus scalable. En effet, la granularité du flot implique la réaction en chaine suivante : plus il y a d'utilisateurs dans le réseau, plus il y a de flots, plus il y a de variables de classifications et d'ordonnancements dans les routeurs à maintenir, ce qui a pour conséquence une charge importante au niveau des routeurs qui deviennent alors de moins en moins performants [16] .

I-4-2.Fonctionnement :

Le service différencié de l'architecture Diffserv permet de diminuer les informations d'état que chaque nœud du réseau doit mémoriser. Il n'est plus nécessaire de maintenir des états dans les routeurs pour chacun des flux. Ceci permet son utilisation à grande échelle.

L'idée consiste à diviser le réseau en domaines. On distingue ainsi les routeurs à l'intérieur d'un domaine (*Core router*) des routeurs d'accès et de bordure (*Edge router*).

Les routeurs d'accès sont connectés aux clients, tandis qu'un routeur de bordure est connecté à un autre routeur de bordure appartenant à un domaine différent. Les routeurs de bordure jouent un rôle différent de ceux qui sont au cœur du domaine. Ils sont chargés de conditionner le trafic entrant en indiquant explicitement sur le paquet le service qu'il doit subir. Ainsi, la complexité des routeurs ne dépend plus du nombre de flux qui passent mais du nombre de classes de service. Chaque classe est identifiée par une valeur codée dans l'en-tête IP [16] .

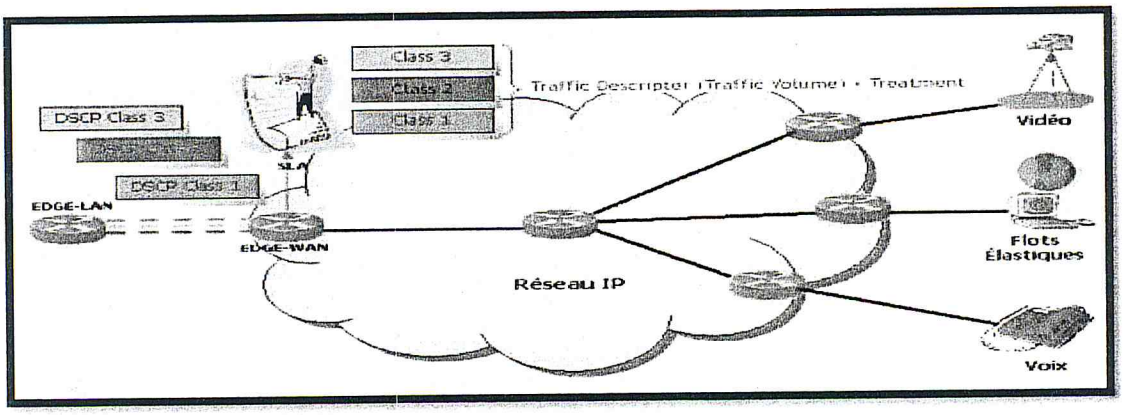


Figure I-3:Le modèle DIffServ [16]

I-4-3.Les avantages du modèle DiffServ :

- Adapté aux réseaux étendus comme ISP car pas d'information d'état à maintenir au niveau des routeurs [14].
- Pas de protocole lourd de signalisation à implémenter comme RSVP [14] .
- Discrimination pour un réseau commercial "Meilleur service pour ceux qui paient plus" [13] .
- Efficace pour les flots à durée de vie courte [13] .

I-4-4.Les inconvénients du modèle DiffServ :

- Complexité dans le provisionnement du réseau et la configuration [13] .
- Echelle de temps différente Charge de trafic et le provisionnement [13] .

- Il nécessite en effet d'établir préalablement un contrat dans tous les équipements de son domaine. Ceci implique une connaissance approfondie des applicatifs pouvant transiter sur le réseau et peut se révéler parfois difficile à appliquer [17] .

En terme de sécurité, il existe plusieurs protocoles dit de tunnelisation qui permettent la création des réseaux VPN(Virtual Private Network) [AN03],dont on va les définir ci-dessous .

On commence par une présentation du protocole PPP, à fin que PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions VPN (Virtual Private Network) sécurisées.

I-5-Le protocole PPP :

I-5-1.Présentation :

Par la ligne téléphonique classique, deux ordinateurs maximum peuvent communiquer par modem ensemble, au même titre qu'il n'est pas possible d'appeler simultanément deux personnes par la même ligne téléphonique. On dit alors que l'on a une **liaison point à point**, c'est-à-dire une liaison entre deux machines réduite à sa plus simple expression: il n'y a pas nécessité de partager la ligne entre plusieurs machines, chacune parle et répond à son tour [18] .

Ainsi, de nombreux protocoles de modem ont été mis au point. Les premiers d'entre eux permettaient une simple transmission de données entre deux machines, puis certains furent dotés d'un contrôle d'erreur, et avec la montée d'Internet, ils furent dotés de la capacité d'adresser des machines. De cette façon, il existe le grand protocole de modem :PPP [18] .

Le protocole point à point (PPP) est un protocole de réseau WAN le plus répandu, de liaison de données assurant l'échange de données de manière fiable sur une liaison point à point . Sa principale caractéristique est, une fois la liaison établie et configurée, de permettre à plusieurs protocoles de transférer des données simultanément [19].
parallèlement, PPP permet l'encapsulation de trames asynchrone et synchrone orienté bit, de configurer la liaison série, de connecter entre routeurs ou entre un hôte et un routeurs ,de

tester la qualité de la liaison, de multiplexer les différentes couches réseau, la Possibilité d'attribution dynamique des adresses de couche 3,détecter les erreurs[20] .

I-5-2.Fonctionnement :

- **I-5-2-1 Les composants de PPP et leurs rôles respectifs:**

Le protocole PPP est composé de trois éléments :

- Un protocole de contrôle de liaison LCP(Link Control Protocol)[AN04] qui a pour rôle d'établir, de configurer, de tester et de fermer la liaison de données.
- Une famille de protocoles de contrôle NCPs (Network Control Protocols)[AN05] pour lancer et configurer différents protocoles de la couche réseau (*Network Protocols, NPs*).
- Une méthode d'encapsulation permettant de transporter sur la même ligne les données en provenance de plusieurs protocoles de la couche réseau en même temps [21] .

- **I-5-2-2 Etablissement d'une session:**

Les quatre phases d'une session PPP, pour l'établissement des communications sur une liaison point à point, sont :

Phase 1 - Etablissement de la liaison : Le nœud d'origine envoie des trames LCP pour configurer et établir la liaison. Négociation des paramètres de configuration grâce au champ d'option des trames LCP (compression, authentification, etc.). Fin de cette phase par l'émission et la réception d'une trame LCP d'accusé de réception de la configuration [22].

Phase 2 - Détermination de la qualité de la liaison : Vérification de la qualité suffisante pour activer les protocoles de couche 3 [22].

Phase 3 - Configuration des protocoles de couche réseau : Émission de paquets NCP pour configurer les protocoles de couche 3 choisis [22].

Phase 4 - Fermeture de la liaison : Fermeture par le biais de trames LCP ou de paquets NCP spécifiques [22].

I-5-2-3 Authentification :

Le protocole PPP peut prendre en charge plusieurs modes d'authentification :

- Utilisation du protocole PAP.
- Utilisation du protocole CHAP.

Le protocole PAP n'est pas un protocole d'authentification très efficace. En effet, les mots de passe sont transmis en clair sur la liaison et il n'offre aucune protection contre la lecture répétée des informations ou les attaques répétées par essais et erreurs [2].

Le protocole CHAP protège contre les attaques de lecture répétée des informations passant par le modem en utilisant une valeur de confirmation variable, unique et imprévisible. Comme la demande de confirmation est unique et aléatoire, la valeur hachée obtenue est également unique et aléatoire. Les demandes de confirmation répétées visent à limiter la durée d'exposition à toute attaque[2] .

I-6-Le protocole PPTP :

I-6-1.Présentation :

PPTP (Point-to-point tunneling protocol), protocole de tunnel point-à-point, est un protocole d'encapsulation PPP sur IP conçu par Microsoft et soumise a l'IETF en juin 1996 . Il permet de mettre en place des réseaux privés virtuels (VPN) au-dessus d'un réseau public sans l'ajout de logiciel supplémentaire [23] .

Toute connexion PPTP met en œuvre un client et un serveur PPTP.et Windows n'est pas le seul système d'exploitation a avoir implanté PPTP, en effet, Linux supporte lui aussi ce protocole comme Apple, et la famille des systèmes BSD[AN06] [24] .

PPTP est un bon et léger protocole VPN offrant une sécurité en ligne de base avec des vitesses rapides. PPTP est intégré à un vaste éventail d'appareils de bureau et portables et présente un cryptage à 128 bits [25].

I-6-2.Fonctionnement :

Le principe du protocole PPTP est de créer des trames avec le protocole PPP et de les crypter puis de les encapsuler dans un paquet IP. Cela permet de relier les deux réseaux par une connexion point-à-point virtuelle acheminée par une connexion IP sur Internet. Cela fait croire aux deux réseaux qu'ils sont reliés par une ligne directe [26].

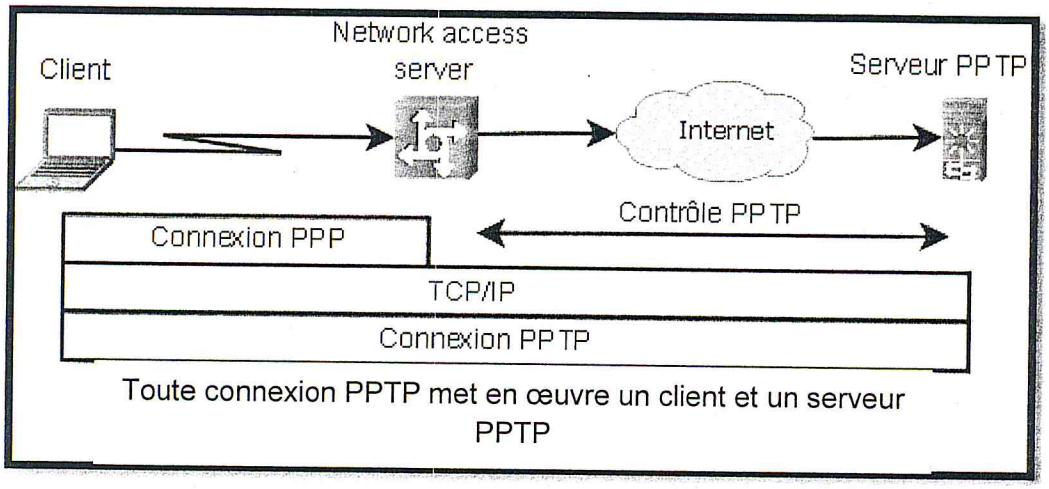


Figure I-4:Le protocole PPTP [28].

Pptp crée ainsi un tunnel de niveau 3 défini par le protocole Gre (Generic Routing Encapsulation) [AN07]. Le tunnel Pptp se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type Ppp et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets Ppp dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel Pptp. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de Pptp[28] .

I-6-3.Les avantages du protocole PPTP:

- L'intérêt de PPTP est de ne nécessiter aucun matériel supplémentaire car les deux logiciels d'extrémité (client et serveur) sont intégrés dans les systèmes d'exploitations [29].
- Son installation est assez facile. Le PPTP est compatible avec de nombreux supports. Par exemple : tablettes, portables, ordinateurs fonctionnant sous Windows, iOS, Mac OS X, Androïd, Linux ...[30].
- PPTP offre une très bonne stabilité, surtout concernant les hotspots wifi [25].
- Son fonctionnement simple qui permet de se doter d'une bonne vitesse vpn [30].

I-6-4.Les inconvénients du protocole PPTP:

- Son inconvénient premier réside dans le wifi et le routeur ADSL qui doivent être compatibles avec le PPTP. Outre le matériel réseau, il y a aussi le transport GRE qui est assez lourd [30].
- la sécurité : mauvaise gestion des mots de passe.et faiblesses dans la génération des clés de session [28].

Le protocole PPTP est caractérisé par sa facilité de mise en place car il est implanté sur toute les plates formes mais il reste non sécurisé dû à l'authentification par mot de passe ce qui conduit au protocole L2TP .

I-7-Le protocole L2TP :

I-7-1.Présentation :

L2TP (Layer Two Tunnel Protocol) est une norme préliminaire de l'IETF (Engineering Task Force). a été conçu pour encapsuler des paquets PPP sur les couches 2 ou 3 du modèle OSI.il est utilisé pour créer des réseaux privés virtuels (VPN), le plus souvent entre un opérateur de collecte de trafic (dégroupeur ADSL ou opérateur de téléphonie pour les accès RTC) et les fournisseurs d'accès à Internet[31] .

Ce protocole combine des fonctionnalités de deux protocoles tunnel : Layer 2 Forwarding (L2F) de Cisco et Point-to-point tunneling protocol (PPTP) de Microsoft. Ce protocole n'assure que le transport des données et leur intégrité, pas leur confidentialité. Ainsi les données qui transitent par l'intermédiaire de ce protocole ne sont pas cryptées et donc potentiellement lisible par quelqu'un [31].

I-7-2.Fonctionnement :

La mise en place d'un VPN L2TP nécessite deux serveurs d'accès [32]:

- LAC (L2TP Access Concentrateur) [AN08].
- LNS (L2tp Network Server) [AN09].

Les concentrateurs d'accès L2TP (LAC),peuvent être intégrés a la structure d'un réseau commuté comme le RTC (le réseau téléphonique commuté) ou encore associé a un système

d'extrémité PPP prenant en charge le protocole L2TP. Son principale rôle se limite à fournir un support physique qui sera utilisé par L2TP pour transférer le trafic vers un ou plusieurs serveurs réseau L2TP (LNS). Il assure le fractionnement en canaux pour tout protocole basé sur PPP. Le LAC joue le rôle de serveur d'accès ,il est a l'origine du tunnel est responsable de l'identification du VPN [32].

Les serveurs réseau LNS, peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP et gèrent le protocole L2TP côté serveur. Les serveurs LNS sont les émetteurs des appels sortants et les destinataires des appels entrants. Ils sont responsables de l'authentification du tunnel[32] .

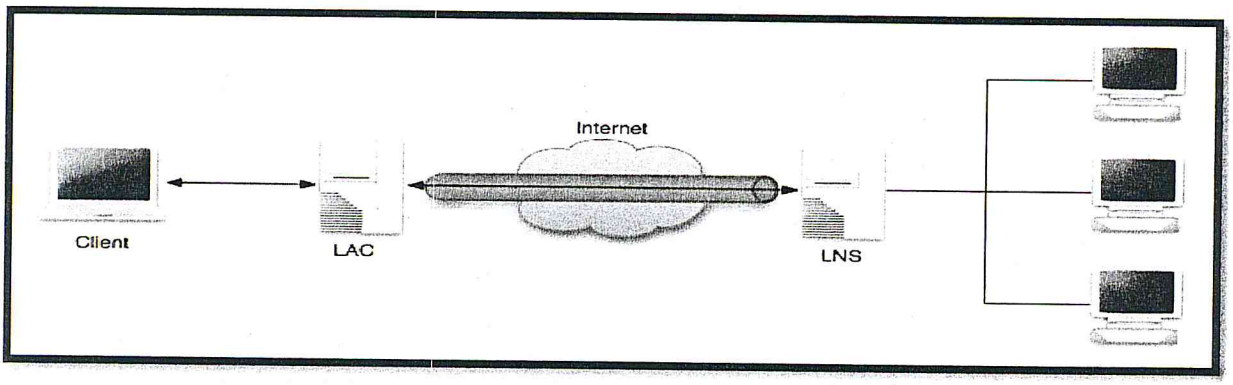


Figure I-5 :Le protocole L2TP [32]

I-7-3.Les avantages du protocole L2TP :

- Sécurité : Le protocole de fractionnement de canaux L2TP prend en charge l'authentification des canaux et des utilisateurs .
- Fiabilité : L2TP donne accès à des fonctions de sauvegarde permettant de configurer plusieurs pairs LNS et de les renforcer par des LNS de secours. Si une connexion vers le serveur LNS principal est indisponible pour une raison quelconque, le serveur d'accès réseau NAS (concentrateur d'accès LAC) établit une connexion vers le serveur LNS de secours [23].
- Modularité : L2TP supporte un nombre illimité de connexions sur chaque LAC et peut assurer plus de 2 000 sessions par LNS sur une plate-forme de routage Cisco [23].
- Mobilité (salarié peut se connecter à un VPN de son entreprise en conservant ses droits et ses restrictions)[23] .

I-7-4.Les inconvénients du protocole L2TP :

- L2TP repose sur UDP (User Datagram Protocol)[AN10] qui lui même repose sur IP. Au total, l'empilement total des couches protocolaires est le suivant (en partant du backbone) : IP/PPP/L2TP/UDP/IP/Couche2. A cela se rajoutent TCP/HTTP si l'utilisateur surfe sur le web. L'ensemble n'est donc pas très léger, lourd et on perd beaucoup en débit utile [33] .

I-8-Le protocole IPsec :

I-8-1.Présentation :

IPSec (Internet Protocol Security) est un protocole de la couche 3 du modèle OSI. Les concepteurs chez IETF ont proposé une solution en novembre 1998 afin de répondre aux besoins directs du développement des réseaux en matière de sécurité. En effet, en sécurisant le transport des données lors d'échanges internes et externes, la stratégie IPSec permet à l'administrateur réseau d'assurer une sécurité efficace pour son entreprise contre toute attaque venant de l'extérieur[34] .

son intérêt principal reste sans conteste son mode dit de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels (VPN). Cette technologie à pour but d'établir une communication sécurisée entre des entités éloignées, séparées par un réseau non sécurisé voir public comme Internet, et ce de manière quasi-transparente si on le désire [35].

Les services de sécurité fournis par IPsec sont la confidentialité, l'authentification et l'intégrité des données. Ces services sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé lorsqu'ils sont utilisés avec des algorithmes forts[34] .

I-8-2.Fonctionnement :

Lors de l'établissement d'une connexion IPsec, plusieurs opérations sont effectuées :

Échange des clés : Le protocole *IKE* (*Internet Key Exchange*) est chargé de négocier la connexion. Avant qu'une transmission IPsec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées. Ce protocole permet deux types d'authentifications, PSK (*Pre-Shared Key* ou secret partagé)[AN11] pour la génération de clefs de sessions *RSA*[AN12] ou à l'aide de certificats [36].

Transfert des données

un ou plusieurs canaux de données par lesquels le trafic du réseau privé est véhiculé, deux protocoles sont possibles [36]:

- Le protocole AH (Authentification Header),fournit l'intégrité et l'authentification .AH authentifie les paquets en les signant, ce qui assure l'intégrité de l'information .
- Le protocole ESP (*Encapsulating Security Payload*) fournit également l'intégrité mais aussi la confidentialité par l'entremise de la cryptographie [36].

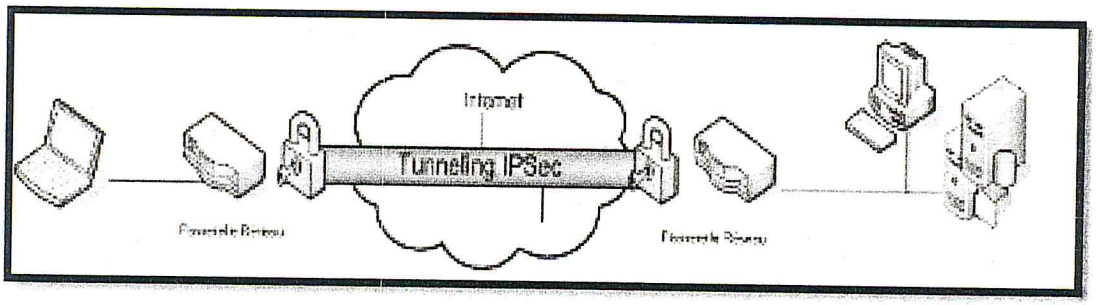


Figure I-6 :Le protocole IPsec [34]

I-8-3.Les avantages d'IPsec :

- Sécurité optimal et plus robuste que celle de PPTP [36].
- Le transparence de la sécurité par rapport aux applications [37] .
- Le faible cout grace au transfert via le domaine Internet public

I-8-3.Les inconvénients d'IPsec :

- Identifie les machines et non les utilisateurs [37].
- Possède de nombreux systèmes de sécurité ce qui le rend complexe [37].
- Alourdit les performances des réseaux du fait des opérations de cryptage/décryptage [37].
- Aucun mécanisme de la qualité de service (applis voies ou vidéos sur IP impossible) [37] .

IPsec permet une Sécurité totale grâce à la combinaison de certificats numériques et de PKI pour l'authentification ainsi qu'à une série d'options de cryptage mais il n'offre aucun mécanisme de Qos Ce qui limite ses applications : toutes les applications de voix sur IP ou de

vidéo sur IP sont impossibles ou seront amenées à être complètement dépendantes des conditions de traffic sur l'internet public.

I-9-Le protocole MPLS :

I-9-1.Présentation :

MPLS (Multi-Protocol Label Switching) a été développé à partir de 1997 avec la création de l' « IETF MPLS working group » suite à la présentation faite par trois constructeur, Cisco, Ipsilon et IBM, de leur technologie de commutation par label respectivement le Tag Switching, IP Switching et ARIS[AN13]. Le premier document (draft-ietf-mplsframework-01.txt) est publié le 2 Août 1999 et MPLS a été normalisé avec la RFC 3031 en Janvier 2001. MPLS comme son acronyme indique est un protocole capable de supporter les différents protocoles de niveau inférieur, au sens OSI (ATM, Frame Relay ...)et il se base sur la commutation d'étiquettes ou "labels". La notion d'étiquette provient du fait que les labels sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. Cette insertion s'opère entre la couche **2** de laissons de données et la couche **3** réseau .C'est pourquoi MPLS est qualifié de protocole de couche **2,5** [38].

Dans un réseau IP typique, le trafic n'emprunte pas de chemin particulier. Chaque routeur calcule le routage localement. Chaque paquet est routé d'un nœud à un autre, suivant l'adresse de destination portée par les paquets, chaque nœud recalculant à chaque fois la route. Cette architecture de routage IP est considérée comme conventionnelle [39].

Avec le MPLS, chaque paquet IP se verra assigner un " shim header " contenant un " label " à son entrée dans le réseau et le trafic empruntera un chemin défini préalablement. Le premier routeur calcule la route et assigne le label, les autres ne font que de la commutation [39].

Le rôle principal du MPLS est de combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2 telles que implémentée dans ATM ou FR (Frame Relay) [AN14]. MPLS doit permettre d'améliorer le rapport performance/prix des équipements de routage, d'améliorer l'efficacité du routage (en particulier pour les grands réseaux) et d'enrichir les services de routage (les nouveaux services étant transparents pour les mécanismes de commutation de label, ils peuvent être déployés sans modification sur le cœur du réseau) [40].

Les labels peuvent être associés à un chemin, une destination, une source, une application, un critère de qualité de service, etc. ou une combinaison de ces différents éléments. Autrement dit, le routage IP est considérablement enrichi sans pour autant voir ses performances dégradées (à partir du moment ou un datagramme est encapsulé, il est acheminé en utilisant les mécanismes de commutation de niveau 2). On peut imaginer qu'un des services les plus importants sera la possibilité de créer des réseaux privés virtuels (VPN) de niveau 3. Ainsi, des services de voix sur IP, de multicast ou d'hébergement de serveurs web pourront coexister sur une même infrastructure. La modularité de MPLS et la granularité des labels permettent tous les niveaux d'abstraction envisageables [41].

I-9-2.Les éléments de base d'un réseau MPLS :

Dans cette section nous allons définir les éléments qui participent aux mécanismes du protocole MPLS .

I-9-2.1.Le label :de manière basique le label identifie le chemin quel le paquet doit suivre, il s'agit d'un champ de longueur fixe (32 bits) transporté ou encapsulé dans l'entête de niveau 2 du paquet Le routeur qui le reçoit examine le paquet pour déterminer le saut suivant selon son label. Une fois qu'un paquet est labellisé, le reste de son voyage est basé sur la commutation de labels. Les valeurs du label ont simplement une signification local [42].

Le format générique d'un label est illustré par la figure ci-dessus :

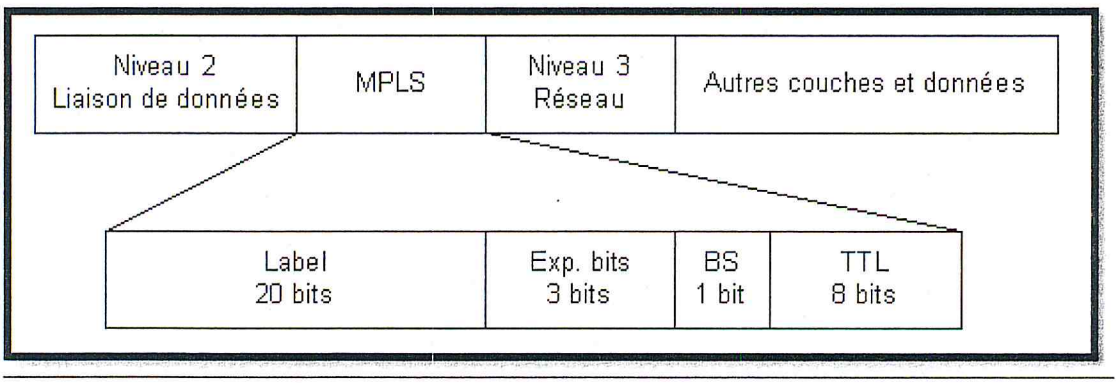


Figure I-7:Le format d'un Label [42].

- LABEL (20 bits): identifiant du label .

- EXP (3 bits): "Expérimental Field ", utilisé pour définir COS les classes de services.les implémentations utilise ce champ comme indicateur de QOS .
- S (1 bit): "Stack Bit", MPLS permet l'insertion de plusieurs labels dans le même paquet, ce bit, lorsqu'il est à 1, permet d'identifier si ce label et le dernier du paquet
- TTL (8 bits): "Time To Live". Ce champ donne la limite supérieure au nombre de routeurs qu'un paquet peut traverser. Il limite la durée de vie du paquet. Il est initialisé à une certaine valeur, puis décrémenté de un par chaque routeur qui traite le paquet. Lorsque ce champ atteint 0, le paquet est rejeté. L'utilisation de ce champ évite les boucles de routage [40].

I-9-2.2.Label Switch Path (LSP): La suite des labels définissant un chemin unique pour un flux traversant le réseau MPLS .Ce chemin peut être crée statiquement ou dynamiquement. Les LSP sont unidirectionnels, chaque LSP est crée sur le chemin le plus court sélectionné par l'IGP [40].

I-9-2.3.Forwarding Equivalence Class (FEC) : Classe d'équivalence dans la quelle on trouve un ensemble de paquets IP transmit de la même manière, et suivant le même chemin (LSP) au sein du réseau [40]. Contrairement aux transmissions IP classiques, dans le MPLS, un paquet est assigné à une FEC une seule fois, lors de son entrée sur le réseau. Les FEC sont basées sur les besoins en termes de service pour certains groupes de paquets ou même un certain préfixe d'adresses. MPLS constitue les FEC selon de nombreux critères : adresse destination, adresse source, application, QoS , etc….[43].

I-9-2.4.Label Switch Router (LSR) : C'est un routeur du réseau MPLS qui fait office de commutateur de labels, il est capable de transmettre les paquets en s'appuyant uniquement sur le mécanisme d'identification des labels [44] .

I-9-2.5.Label Edge Routers (LER) : C'est un routeur qui fait l'interface entre le réseau MPLS et l'extérieur, il possède des interfaces connectées au réseau MPLS et des interfaces IP traditionnelles. Il existe deux catégorie de LER:

- Le MPLS **Ingress Node** ou routeur d'entrée MPLS gère le trafic entrant sur le réseau MPLS, il ajoute un label à chaque paquet IP en fonction de la FEC et le transmet sur le bon LSP [40].
- Le MPLS **Egress Node** ou routeur de sortie MPLS gère le trafic sortant sur réseau MPLS,il retire le label du paquet et le transmet en fonction des entrées dans sa table de routage [40].

I-9-2.6.Label Distribution Protocol (LDP) :est un protocole permettant d'apporter aux LSR les informations d'association des labels dans un réseau MPLS. Il est utilisé pour associer les labels aux FEC, ce qui crée des LSP. Les sessions LDP sont établies entre deux éléments du réseau MPLS, qui ne sont pas nécessairement adjacents [43].

Ces éléments échanges les types suivants de messages LDP [43]:

- Messages de découverte : annoncent et maintiennent la présence d'un LSR dans le réseau .
- Message de session : Etablissent ,maintiennent et terminent les sessions LDP .
- Messages d'avertissement :créent ,changent et effacent des associations entre FEC et labels .
- Messages de notification :permettant d'apporter d'autres informations comme signaler une erreur .

I-9-2.7. Label information base(LIB) : Chaque nœud MPLS capable de transférer des paquets labellisés sur le réseau MPLS détient une base des informations de labels (LIB). C'est La première table construite par le routeur MPLS.C'est sur cette base d'informations que les décisions concernant la transmission des paquets sont fondées. En effet, les LIB (*Label Information Base*) contiennent, sous forme de table, la correspondance entre les différents FEC existant et les labels qui ont été attribués à chacun d'entre eux. Elle contient pour chaque sous-réseau IP la liste des labels affectés par les LSR voisins. Les informations contenues dans les LIB sont créés et mises à jour, grâce au protocole LDP [34].

I-9-2.8.Label Forwarding Information Base(LFIB): A partir de la table LIB et de la table de routage IP, le routeur construit une table LFIB qui contient que les labels du meilleur prochain saut qui sera utilisé pour commuter les paquets labélisés [44].

I-9-2.9.Penultimate Hop Popping (PHP) : C'est la technique d'optimisation qui évite au LER de sortie d'effectuer une double recherche dans la table de routage et dans le Label Forwarding Information Base (LFIB) [44],

I-9-3.L'architecture du réseau MPLS :

Comme le suggère l'acronyme MPLS, l'architecture supporte plusieurs protocoles. Cela signifie que le mécanisme n'est pas lié à une couche de niveau 2 ou de niveau 3 particulière. En effet, son utilisation est prévue pour un ensemble de protocoles. Par conséquent, cette technologie devient intéressante pour de nombreuses entreprises désireuses de changer leur réseau d'information sans avoir à modifier considérablement l'existant [45].

L'architecture logique MPLS est définie comme suit :

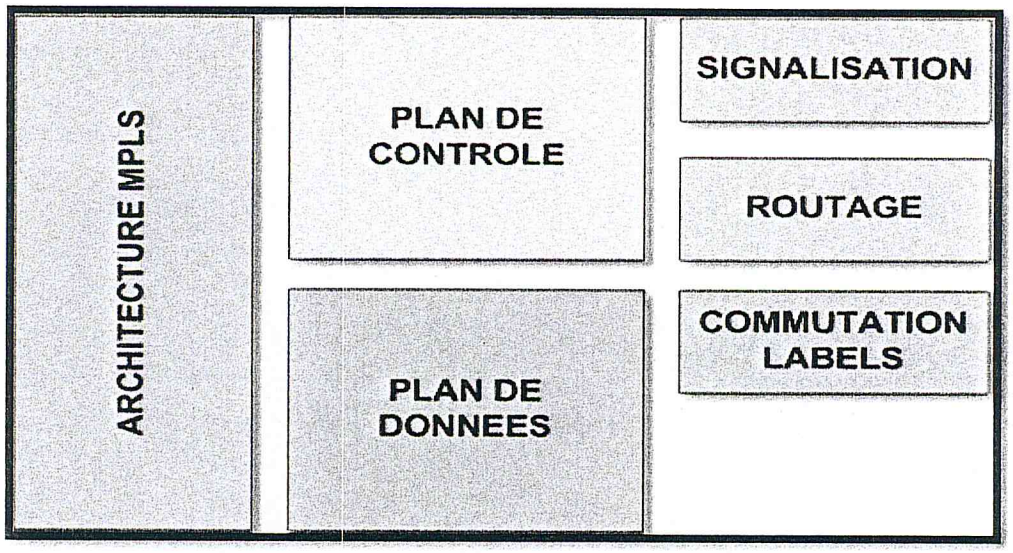


Figure I-8:L'architecture du MPLS [45].

On distingue deux parties logiques bien distinctes. Tout d'abord, le plan de contrôle qui va être chargé de gérer et maintenir les labels contenus dans chaque routeur du réseau MPLS. Ce plan de contrôle utilise des protocoles de routages classiques, tels que OSPF ou RIP afin de créer la topologie des nœuds du réseau MPLS, ainsi que des protocoles spécialement développés pour le MPLS comme Label Distribution Protocol (LDP) [45] .

La seconde partie, est le plan de données. Celui-ci contient le mécanisme de transmission des données et est complètement indépendant de la partie signalisation. Ce découpage est par exemple à la base des migrations ATM vers MPLS, car elle permet de conserver le matériel ATM utilisé en cœur de réseau. Grâce au simple changement logiciel du plan de contrôle, le commutateur ATM pourra être transformé en routeur MPLS [45].

I-9-4.Le principe de fonctionnement du MPLS :

Contrairement à IP qui utilise l'adresse de destination pour router les paquets saut par saut, MPLS définit des circuits permettant d'acheminer les paquets sur des mêmes chemins unidirectionnels dits LSP (Label Switched Paths)1. Chaque LSP interconnecte un nœud source à un nœud de destination et est formé d'une succession de LSR (Label Switched Routers) permettant aux paquets de suivre le même itinéraire pour atteindre leur destination.

Pour déterminer le LSP que doit emprunter un paquet (afin d'atteindre sa destination),MPLS utilise des étiquettes. Chaque étiquette identifie sur tout LSR un seul LSP associée à groupe de paquets (FEC ou Forwarding Equivalence Class) devant être transmis de manière identique sur le réseau MPLS [46].

Ainsi, à la réception d'un paquet par un routeur frontière d'entrée LER (Label Edge Router) à un domaine MPLS, ce dernier déduit la FEC associée au paquet à partir d'informations contenues dans son entête (comme l'adresse de destination, le numéro de port, etc.) et consulte sa table d'étiquettes LFIB (Label Forwarding Information Base) pour déduire l'étiquette et l'interface de sortie permettant l'acheminement du paquet. Ensuite, le LER d'entrée ajoute l'étiquette déterminée au paquet (opération push) avant de l'envoyer sur l'interface de sortie déduite précédemment et permettant d'atteindre le prochain LSR [46].

Une fois que l'étiquette MPLS est insérée dans le paquet envoyé, l'acheminement se fait par commutation d'étiquettes (opération swap) le long du LSP associé à la FEC. Typiquement, tout LSR recevant le paquet consulte sa table LFIB et déduit l'étiquette et l'interface de sortie à partir de l'étiquette d'entrée (resp. à partir de l'étiquette d'entrée et de l'interface d'entrée) lorsque l'allocation d'étiquettes est globale au LSR (resp. lorsque l'allocation d'étiquettes est locale à cette interface). Le paquet est ensuite envoyé sur l'interface de sortie déterminée précédemment en substituant l'étiquette d'entrée par l'étiquette de sortie. Lorsque le paquet arrive au routeur d'extrémité du LSP , la suppression d'étiquette MPLS est effectué par le LSR aval au routeur de sortie du LSP, cette opération est appelée PHP (Penultimate Hop Popping). Cette opération est souvent utile pour éviter au routeur de sortie d'effectuer deux recherches dans ses tables de routage [46].

Lorsque le LSR situé en aval du routeur de sortie n'est pas capable de dépiler l'étiquette ou lorsque le routeur de sortie ne désire pas le PHP, l'étiquette est supprimée par le routeur de sortie du LSP. la suppression de l'étiquette au routeur de sortie du LSP et non pas à son LSR aval est parfois nécessaire (ex. protection multicast par tunnels point à multipoint) [47].

I-9-5.Le routage et le MPLS :

Il existe de type de routage a savoir le routage implicite et le routage explicite

- Le routage implicite : Il n'y a pas de fonction d'établissement de route avec MPLS dans le mode implicite. La distribution de labels aux LSR est réalisée grâce au protocole LDP (Label Distribution Protocol). LDP définit une suite de procédures et de messages utilisés par les LSR pour s'informer mutuellement du mapping entre les labels et le flux. Le LDP qui n'a qu'un rôle d'information et non pas de calcul. Pour cela, il s'appuie sur un protocole de routage de niveau 3 comme OSPF par exemple. Il faut donc commencer par activer ce protocole de routage IP avant de mettre en œuvre le routage implicite avec LDP [48].

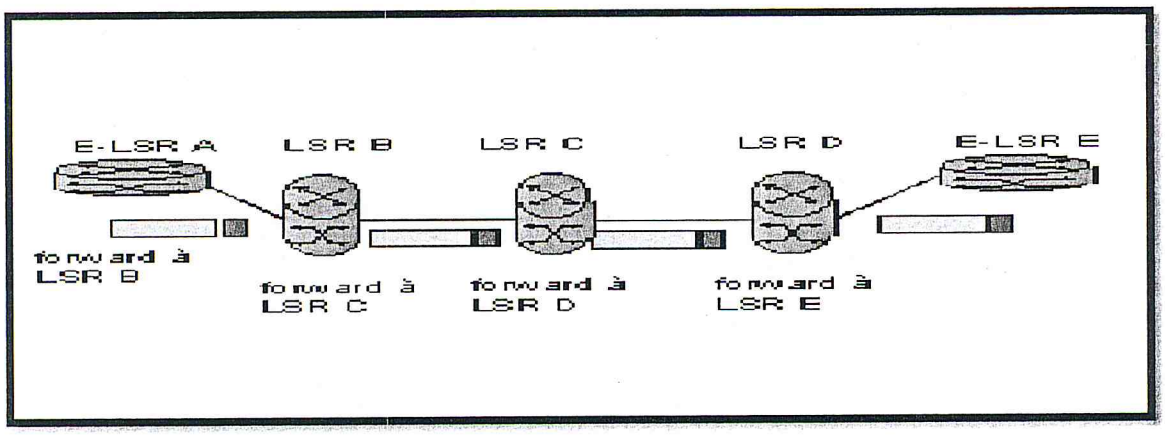


Figure I-9:le routage implicite avec MPLS [41].

LDP est bidirectionnel et permet la découverte dynamique des nœuds adjacents grâce à des messages Hello échangés par UDP. Une fois que les 2 nœuds se sont découverts, ils établissent une session TCP [AN15] qui agit comme un mécanisme de transport fiable des messages d'établissement de session TCP, des messages d'annonce de labels et des messages de notification [48].

- Le routage explicite : Un des avantages très important du protocole MPLS est de pouvoir conjuguer du routage automatique (implicite) recherchant les meilleures routes et de le compléter avec des paramètres manuels en imposant par exemple certaines liaisons (explicite). En effet, les routes optimales proposées par les protocoles de routage sont des chemins idéaux sans considérer les autres flux. Dit autrement, ce sont des configurations statiques calculées *a priori* et ne tenant pas compte de la réalité du trafic en cours.

Cette notion de dynamique peut être introduite dans les tables de commutation de label par la création de tunnel dédie. En effet, il est possible pour l'administrateur réseau de modifier certains acheminements provoquant des goulots d'étranglement dans son réseau pour soulager les liaisons les plus utilisées. Pour cela, il utilise des mécanismes de réservation de bande passante, mais il peut aussi expliciter une liste d'intermédiaires constituant un tunnel. Ce travail s'appelle l'ingénierie de trafic (*traffic engineering*). Ces fonctions explicites peuvent aussi être utilisees pour exprimer d'autres contraintes qui peuvent d'être d'ordre commercial, concurrentiel ou économique [48].

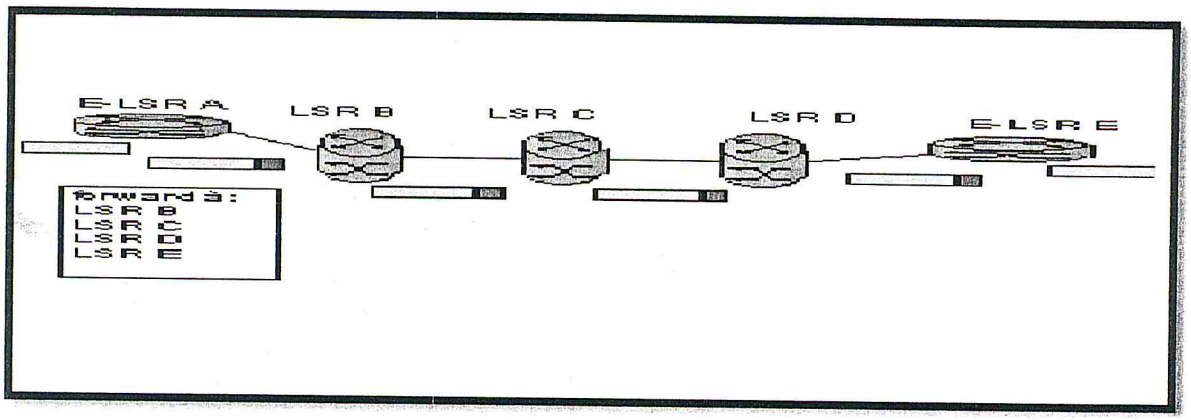


Figure I-10:le routage explicite avec MPLS [41].

I-9-6. MPLS et le trafic engineering :

L'ingénierie de trafic est une des principales applications de MPLS, elle permet de repartir la charge sur l'ensemble du réseau en établissement des chemins explicitement routés et en contrôlant la répartition du trafic sur différente liaison afin d'éviter la sous-utilisation de certaine partie du réseau [38].

Le fonctionnement par défaut de MPLS est de construire les LSP en fonction des informations de routage et égal au « plus court chemin » sélectionné par le protocole de routage IGP[AN16]. Cela entraîne la plus part du temps l'apparition de liaison surchargée ou sous utilisée[38]..

MPLS/TE est utilisé pour créer des LSP qui diverge du « plus court chemin ». Le RSVP-TE est utilisé pour créer ces LSP. MPLS/TE support la génération automatique de LSP mais permet aussi de spécifier explicitement par ou doit passer le LSP. RSVP-TE permet en outre d'associer des caractéristiques de qualité de service aux chemins et de subordonner l'établissement des LSP à la disponibilité de ressources dans les équipements intermédiaires. MPLS/TE autorise la mise en place de fonctions évoluées de partage de charge et de routage

différencié en fonction d'informations contenues dans l'en-tête du paquet ou de l'interface d'entrée. Il suffit pour cela de créer un ou plusieurs chemins concurrents pour une FEC donnée et de décider de la route empruntée en fonction d'informations complémentaires : champ dans l'en-tête IP, provenance du paquet, état d'occupation des liens, etc[38].
Le Traffic Engineering permet donc de mapper le flux de trafic par rapport à la topologie physique du réseau. Il fournit la capacité d'écarter le flux de trafic du « plus court chemin » calculé par l'IGP et de passer par des chemins moins utilisé. Le but du Traffic Engineering est d'équilibrer la charge du trafic sur diverse liens ou routeurs dans le réseau afin qu'aucun de ces composant ne soit sur ou sous utilisés. Cela permet donc à un ISP d'exploiter entièrement son infrastructure de réseau [38].

I-9-7. MPLS et le VPN :

Un réseau privé virtuel MPLS/VPN permet de connecter des sites distants sur un réseau partagé par tous les clients. Le trafic du réseau privé virtuel est isolé logiquement des autres trafics VPN. Cette isolation est réalisée par un mécanisme de routage fondé sur le protocole MP-BGP, qui est une extension du protocole de routage BGP (Border Gateway Protocol)[AN17] pour les réseaux MPLS. Le protocole MP-BGP fonctionne en collaboration avec un protocole de distribution de labels (Label Distribution Protocol) afin d'associer un label à une route externe. Dans ce cas, deux niveaux de labels sont utilisés, le premier label correspond à la route dans le VPN concerné et le second label correspond au PE(Provider Edge ou bien LER) permettant d'atteindre le prochain saut BGP. De plus, chaque VPN peut faire transiter les classes d'adresses IP qu'il désire sans qu'il y ait de conflit d'adresses IP avec d'autres VPN. Chaque VPN a en effet sa propre table de routage et la commutation du trafic réseau est réalisée sur des labels uniques et non sur des adresses IP. Pour cela, un identifiant appelé RD (Route Distinguisher) est accolé à chaque subnet IPv4 afin de créer une route VPNv4. En revanche, dans le cas d'un Extranet ou d'un accès à un fournisseur de services, les adresses IP devront être uniques afin de partager les ressources communes. Un réseau MPLS/VPN est composé de routeurs P (Provider : dédiés à la commutation), de routeurs PE (Provider Edge : dédiés à la création des MPLS/VPN ainsi qu'à la connectivité avec les équipements localisés chez les clients) et de routeurs CE (Customer Edge : installés chez les clients et connectés aux routeurs PE). Seuls les routeurs PE contiennent la définition des MPLS/VPN, les routeurs P et CE n'ayant aucune connaissance de la configuration des

MPLS/VPN. Les routeurs P commutent des labels, tandis que les routeurs CE commutent des adresses IP. La sécurité logique d'un MPLS/VPN repose principalement sur la configuration logique du VPN dans les configurations des routeurs PE. Pour mieux comprendre les enjeux de configuration des MPLS/VPN, prenons l'exemple de deux VPN A et B reliant deux sites différents pour chacun des VPN, comme illustré à la figure ci-après [49] :

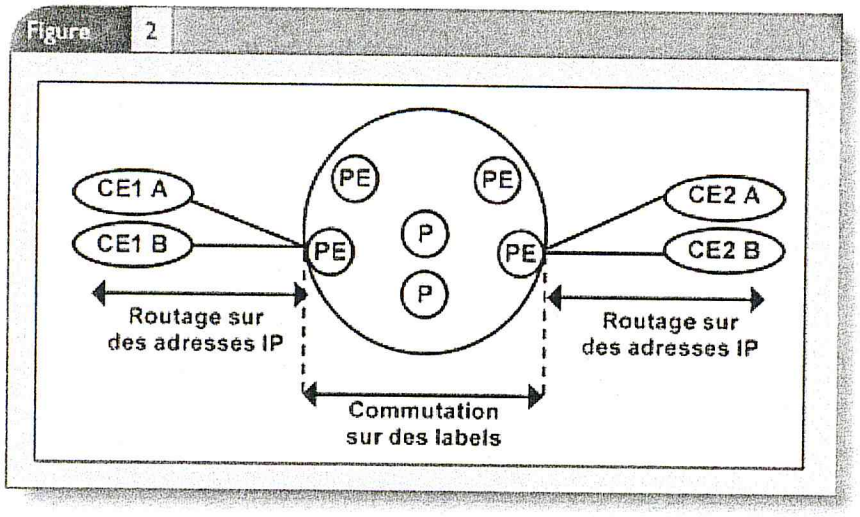


Figure I-11:Un exemple d'une connexion VPN [49]

I-9-8.L'objectif du MPLS :

Avec l'arrivée de MPLS (MultiProtocol Label Switching) dans la dernière décennie, la protection locale a été améliorée et rendue plus efficace. Grâce à sa grande flexibilité pour le choix des routes et à sa capacité de réserver explicitement les ressources (plus particulièrement la bande passante) et à pré-configurer des chemins de secours locaux, MPLS permet de [46]:

- réduire sensiblement les délais de récupération (jusqu'à 50 millisecondes)
- assurer la disponibilité des ressources après une panne .
- optimiser l'utilisation des ressources.
- Garantir Les débits par la qualité du service, la sécurité est renforcée .
- Grace au service SDSL d'envoyer des données et de recevoir avec la même quantité ce qui n'est pas possible avec l'ADSL standard.

- Traiter un grand nombre d'informations car les nouveaux matériels actifs sont plus performants, la commutation est de plus en plus rapide.
- Une économie des coûts de communication : la facture n'est pas calculée en fonction des temps de communication pour l'envoi ou la réception de données, ce qui était le cas auparavant dans les technologie de type numeris, transfix .
- Augmenter la bande passante, la quantité d'information est donc plus importante, cela permet d'envoyer ou de recevoir des données en permanence .
- Optimiser le traffic réseau puisque c'est le « chemin » le plus court qui est emprunter pour transporter l'information de l'émetteur au récepteur.

I-10-La comparaison entre ces différents protocoles:

I-10.1.Comparaison entre ATM et MPLS :

On a pu a partir des différents lectures et analyses d'extraire le suivant tableau de comparaison

Les contraintes	MPLS	ATM
La taille des paquets et la vitesse de transmission	-La taille des paquets est variable, en fonction de la quantité de données qui est envoyé, avec la commutation de labels la vitesse de transmission des paquets est plus grande que ATM	-ATM offre une vitesse accrue en utilisant une unité de taille fixe appelés cellules (53 octets), ce qui simplifie le traitement au niveau des nœuds, ce qui lui rend prévisible et efficace
Le débit	Avec MPLS, nous pouvons répondre à tous les besoins allant jusqu'à 50 Mbit/s".	En attendant ATM offre des vitesses d'accès de l'ordre de 25 Mbps .
Gigue "la variation de delai"	les délais de transmission est très petit, c'est pour cela le MPLS est adapté aux applications telles que la phonie et la vidéo .	une variation de délai inférieure à 5 ms, ce qui est approprié pour transporter la voix ou signal vidéo " particulier les services vidéo sous la norme MPEG [AN18] "

Le taux de pertes	garantir un taux de perte de paquet faible .	La couche AAL1[AN19] permet la détection des cellules perdues ou erronées. un taux de pertes de cellules inférieur à 10(puissance 10)
Contrôle et détection d'erreurs	MPLS ne met en œuvre aucun contrôle d'erreur ou de flux.	AAL 2 utilise 3 octets de la charge utile de la cellule ATM pour fins de détection et correction d'erreurs et pour y insérer un numéro de séquence
La latence "le délai"	Dans le MPLS le temps de latence est de 10 microsecondes .	ATM présente une latence peu a un débit plus élevé

Tableau I.1 :comparaison entre MPLS et ATM

Le protocole ATM répond a une partie de critères de la qualité de service mais comme c'est une technologie en perte de vitesse qui se base sur des cellules de taille fixe donc elle représente pas la solution d'avenir utilisable par les operateurs qui sont passes majoritairement a l'IP .

I-10.2. Comparaison entre les 3 protocoles PPTP et L2TP et IPsec :

L2TP est un protocole qui s'appuyé sur PPP et permettant l'établissement d'un tunnel. Ce protocole n'assure que le transport des données et leur intégrité, pas leur confidentialité. Ainsi les données qui transitent par l'intermédiaire de ce protocole ne sont pas cryptées et donc potentiellement lisible par quelqu'un. Pour cette raison, L2TP encapsule souvent des paquets IPSec pour assurer la confidentialité des données .Pour cela nous allons étudier la différence entre le protocole PPTP et L2TP /IPSEC

	PPTP	L2TP/IPsec
Le cryptage	PPTP utilise pour le cryptage un protocole de chiffrement Point-to-Point de Microsoft (MPPE).MPPE "met en œuvre l'algorithme RSA de chiffrement avec un maximum de 128 bits."	Les données sont cryptées grâce au protocole IPSec standard. "met en œuvre l'algorithme de chiffrement 3DES[AN20] pour la confidentialité. Avec un maximum de 256
Systèmes supportés	Windows / Mac OS X / Linux / iOS / Android / DD-WRT	Windows / Mac OS X / Linux / iOS / Android
Les défaillances de sécurité	La mise en œuvre de PPTP a des failles de sécurité graves . l'algorithme RCA est soumise à une attaque bit-flipping. Microsoft recommande fortement la mise à niveau IPSec où la confidentialité est une préoccupation.	IPSec est considéré comme extrêmement sécurisé car il Utilise le plus fort encryptage, vérifie l'intégrité des données, protège les données deux fois.
Stabilité	Très stable, compatible avec la plupart des hotspots Wi-Fi	Stable si votre appareil supporte NAT[AN21]
Installation	Facile à configurer.	Demande une configuration spéciale
Vitesse	Rapide grâce à un cryptage à fonctionnement allégé	Demande le plus du processeur (CPU)

Tableau I.2 :comparaison entre le protocole PPTP et L2TP/IPSec

Après cette comparaison nous arrivons a dire que L2tp/IPsec est un excellent choix car il permet une Sécurité totale grâce à la combinaison de certificats numériques et de PKI pour l'authentification ainsi qu'à une série d'options de cryptage mais pas aussi rapide et requiert une configuration additionnelle. Et il mais il n'offre aucun mécanisme de Qos Ce qui limite ses applications : toutes les applications de voix sur IP ou de vidéo sur IP sont impossibles ou seront amenées à être complètement dépendantes des conditions de trafic sur l'internet public.

Puisque le IPsec est le meilleur choix permet les 3 protocoles de tunnelisation citer précédemment nous allons faire une différence juste entre MPLS et le IPsec .

I-10.3.Comparaison entre MPLS et IPsec :

On a pu a partir des différents lectures et analyses d'extraire le suivant tableau de comparaison ;

	MPLS	IPsec
QoS	Permet d'attribuer des priorités au trafic par le biais de classes de service	Le transfert se faisant sur l'Internet public, permet seulement un service "best effort"
Cout	Inférieur à celui d'ATM mais supérieur à celui des autres VPN IP.	Faible grâce au transfert via le domaine Internet public
Sécurité	Les architectures MPLS/VPN offrent de bonnes garanties de sécurité si les conditions de contrôle sont réalisées sur les configurations des équipements réseau.	Sécurité totale grâce à la combinaison de certificats numériques et de PKI pour l'authentification ainsi qu'à une série d'options de cryptage, triple DES et AES notamment
Application compatible	Toutes les applications, y compris les logiciels d'entreprise vitaux exigeant une qualité de service élevée et une faible latence et les applications en temps réel (vidéo et voix sur IP)	Applications sous IP, notamment courrier électronique et Internet. Inadapté au trafic en temps réel ou à priorité élevée
Etendu	Dépend du réseau MPLS du fournisseur de services	Très vaste puisque repose sur l'accès à Internet

Tableau I.3 :comparaison entre le MPLS et le IPSec

IPSec est le meilleur protocole destiné à fournir différents services de sécurité, mais il n'offre aucun mécanisme de Qos Ce qui limite ses applications : toutes les applications de voix sur IP ou de vidéo sur IP sont impossibles ou seront amenées à être complètement dépendantes des conditions de trafic sur l'internet public.

Conclusion :

Après avoir vu les avantages et les inconvénients offert par chaque technologies et l'étude comparative entre ces différents protocoles nous avons constaté que Initialement, 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 donc MPLS avait été créée pour améliorer les performances des réseaux haut-débits, notamment en terme de routage la technologie MPLS s'était orientée vers le développement de la qualité de service. Elle apporte par exemple un mode connecté à IP et permet de différencier les types de fluxde données comme le proposait le modèle DiffServ. son principe de fonctionnement était assez proche de celui d'ATM tout en se substituant au routage de niveau 3. L'autre avantage de cette technologie par rapport à ATM est le prix des équipements deux fois moindre. Enfin, nous avons constaté que l'une des principales applications de ce protocole était la réalisation de VPN de type intranet ou extranet dont la sécurité était basée sur le principe d'étanchéité des tunnels MPLS.

Dans le chapitre suivant nous allons aborder on détail le critère Qualité De Service et voir comment le MPLS a la possibilité d'obtenir une Qos garantie .

Les références :

[1] : http://www.lirmm.fr/~ajm/Cours/04-05/DESS_TNI/Rapports/rapport_ATM.pdf -TER Réseau haut débit ATM fonctionnement- Oliveir Grudet .

[2] : http://www.reseaumaroc.com/files/CCNA4.pdf.

[3] : http://www.aconit.org/histoire/colloques/colloque_2004/ritzenthaler.pdf -Histoire d'ATM- Sylvie Ritzenthder .

[4] : http://www.funix.org/fr/reseau/main-reseau.php?ref=wan/atm&page=menu –Les réseaux ATM-

[5] : http://ad-network-informatique.fr/?page_id=14 –A.D.N.I- glossaire ATM

[6] : http://mathieu147.11vm-serv.net/cmsmadesimple/index.php?page=introduction-aux-reseaux-atm –Reseau ATM :principes et intégration avec IP .

[7] : http://fr.wikipedia.org/wiki/Asynchronous_Transfer_Mode -Wikipédia-

[8] :http://manu.lochin.net/qos/qoshtml/node6.html –

[9] : http://www.httr.ups-tlse.fr/pedagogie/cours/tcp-ip/rsvp/

[10] : http://fr.wikipedia.org IntServ

[11]: http://www.frameip.com/mpls/

[12]: http://www.voxpress.info VoixPress "Qualité de service sur IP "

[13] : http://www-rp.lip6.fr/~friedman/ens/03/im/C2.pdf

[14] : http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/NatchiaKouao-Benlahcen/index.htm

[15] : http://fr.wikipedia.org/wiki/Differentiated_services

Introduction :

Pendant longtemps, les réseaux de communication étaient spécifiques à un seul type d'information et un seul type de service : les réseaux à commutation de circuit pour la téléphonie, les réseaux hertziens pour la télévision, les réseaux IP pour les données... Ces différents types de réseaux ont aujourd'hui tendance à converger, chaque opérateur voulant offrir de multiples services à ses clients : accès à internet, téléphonie, télévision interactive, vidéo à la demande, visioconférence, télémédecine [51] .

Outre cette multiplication des services dans les réseaux, ceux-ci sont de plus en plus exigeants quant à la qualité des transmissions. La notion de *qualité de service* permet de formaliser ces exigences en terme de critères de performance : bande-passante, délai de transmission de bout en bout, taux de perte des paquets, gigue... et chaque service peut avoir des exigences différentes en terme de qualité de service. L'architecture *best-effort* établi par les réseaux IP ne permet pas de garantir une quelconque qualité de service et il a été nécessaire de définir de nouvelles architectures de réseaux [51].

Pour répondre à ces nouveaux besoins. Plusieurs protocoles ont apparu tel que réseaux ATM, modèle IntServ pour les réseaux IP et plus récemment les architectures à différentiation de services DiffServ et les réseaux MPLS qui effectuent un traitement différencié des trafics, regroupés en quelques classes de services, pour garantir la qualité de service.

nous décrivons dans ce chapitre les mécanismes de la QoS ainsi les différentes techniques, technologies et protocoles utilisés actuellement dans les réseaux pour garantir la QoS des paquets et des flux , ensuite nous passons a la limitations de ces derniers les travaux ayant déjà effectués pour améliorer la QoS dans les réseaux .

II-1- Présentation de la Qualité de service (QoS) :

La Qualité de service (Quality Of Service) se note en abrégé QoS. La définition de ce terme n'est pas unique et chaque communauté donne une définition qui lui est propre. Dans la norme ITU_T (International Télécommunication Union_ Télécommunication), la qualité de service est perçue comme un ensemble de critères de qualité requis pour le fonctionnement d'un ou plusieurs objets. Dans la terminologie ATM la QoS est définie a travers un ensemble de paramètres de performances et de QoS caractérisant une connexion virtuelle. Enfin l'IETF fait référence a la qualité de service pour désigner les paramètres caractérisant les exigences/contraintes des application et celle de l'ensemble du réseau [52] .

IP sans QoS est appelé Best Effort, ce qui signifie que l'on ne peut pas attendre qu'il gère de façon spécifique un flux. On ne peut pas prédire ni le délais ni la possible perte de paquets. Par opposition , la Qos réseau va nous permettre de privilégier des flux jugés plus importants voir de garantir une certaine bande passante à des applications critiques .Ce qui va nous permettre de diminuer la perte des paquets sur certains flux et donc, notamment de diminuer les délais .Donc la QoS est vu comme un ensemble des mécanismes permettant d'assurer un niveau de service donné à des flux particuliers [53] .

Il faut garder à l'esprit que la QoS ne crée pas la bande passante, mais la gère afin de donner différentes priorités ou différentes réservations a certains flux ou types de flux [53].

La QoS définit 4 types de services :

-**Services garantis** : il y a réservation de ressources tout le long du réseau pour un type de flux. Ce type de service est a réservé aux applications critique [53].

-**Services différenciés** : on privilégie statistiquement certains types de flux (ces flux sont donc statistiquement plus rapides, comportement en moyenne moins de pertes …). La garantie est donc relative. Ce type de service est à réserver aux applications nécessitant un traitement préférentiel [53].

-**Service Best-Effort** : il n'y a aucune garantie, c'est le fonctionnement normal d'IP sans QoS. Ce type de service est utilisé pour le reste des applications : celles qui n'ont pas de contraintes particulières(mail, web, ftp…….) [53].

-**Le service Less Than Best-effort** :ce type de service est a réservé aux services ayant des contraintes très faibles .En effet, tous les flux seront prioritaires les flux Less Than Best-Effort [53] .

II-2.Les caractéristiques de la QoS :

Afin de concevoir et de réaliser une architecture de QoS ,plusieurs paramètres non fonctionnels sont définis et pris en considération .Ces paramètres sont soit orientés technologie, tels que le débit et le delai, soit orientés utilisateur ,tels que la priorité et la confidentialité .Cependant ,la QoS se décline principalement en quelques paramètres, ces paramètres sont définis dans ce qui suit :

- **La bande passante :** correspond au débit possible entre deux points. Elle est limitée par le débit des liaisons physique traversées, mais également par les autres flux concurrents[53].
- **Le délai ou bien la latence :**caractérisé le temps de transfert de bout en bout. En d'autres termes, dans le cas de la téléphonie sur IP (ce qu'on appelle VoIP), c'est le temps qui sépare le moment où nous parlons et le moment ou notre interlocuteur nous entendre .ce délai tient compte du temps de propagation des paquets le long du chemin ainsi que du temps de traitement dans les systèmes intermédiaires [53].
- **La gigue :** caractérise la variation du temps de transfert pour des communications successives entre un émetteur et un récepteur donné .la présence de la gigue dans les flots peut provenir de changements d'intensité de trafic sur les liens de sorties des routeurs .Plus globalement, elle dépend du volume de trafic et du nombre d'équipements sur le réseau [53].
- **La fiabilité** traduit le taux d'erreurs moyen des différents supports et équipements de communication [53].
- **La perte des paquets :**Elle correspond aux paquets éliminés (rejetés) ou perdus lors de la transmission d'un flot. Ce paramètre est souvent exprimé en taux de perte .la perte de paquets apparait lorsque l'intensité du trafic sur les liens de sorties d'un nœud devient supérieures à sa capacité d'écoulement. Ce paramètre est donc une indication de la congestion [53] .

Ces quatre caractéristiques n'ont pas la même importance pour tous les type de logiciels par exemple une gigue faible est surtout nécessaire lors d'une transmission audio, en effet une forte gigue provoque une distorsion importante de la restitution du son. En revanche, une gigue importante ne gène pas un transfert de fichier par exemple [53].

Il existe un paramètre qui peut faire chuter ces caractéristique : la congestion [53].

La congestion : sur un réseau provient de façon générale d'un trafic trop important. Des problèmes de congestion survienne dans les cas suivant :

- l'ordinateur génère des données a un débit supérieur a celui de l'interface physique.
- des données sont envoyées d'un lien de débit élevé vers une même sortie.

- un routeur et surchargé par un traitement ce qui est d'autant plus probable dans les réseaux IP [53] .

II-3.Les classes de service :

Ces caractéristiques sont ensuite regroupes entre eux en fonction des besoins des applications et des services. Ces groupes forment alors des **Classes de Services** (Class of Services : CoS). Les requêtes de QoS des applications ou des services seront toujours affectées a une classe de service donnée. A chaque classe, correspond un ensemble de caractéristiques de QoS avec des objectifs quantifies. Plusieurs modèles de CoS ont été standardises et peuvent être utilisés indifféremment. Chaque operateur définit également ses propres classes de services avec des objectifs quantifiés différents. Il est très complexe de synthétiser les différentes propositions. En effet, même le nombre de classes de services est sujet a des débats intensifs dans les instances de standardisations, une classification des principales applications est fournie afin de faciliter la compréhension de la CoS [54] :

- **Voix :** Regroupe toutes les applications du type conversationnel (Voix, Conférence, ...) ayant pour contrainte forte des objectifs sur le délai et la gigue. Elles sont également sensibles au taux de perte bien qu'il ne soit pas possible de retransmettre les données et requièrent des débits assez faibles .
- **Video :** Regroupe toutes les applications multimédia diffusées ou non (Vidéo a la Demande – VoD, la télévision sur IP – IP TV, ...) ayant pour contrainte forte le taux de perte et le débit et dans une moindre mesure le délai et la gigue [54].
- **Donnée :** Regroupe toutes les applications de transfert de données ayant pour seule contrainte un taux de perte nul et qui s'accommodent d'un délai et d'une gigue quelconque. Un débit garanti caractérise cette classe sans toutefois en faire une contrainte stricte [54] .
- **Défaut :** Désigne toutes les applications n'exigeant aucune garantie de QoS. Bien connu sous l'anglicisme . **Best-Effort** . c'est le mode de transport du protocole IP [54].

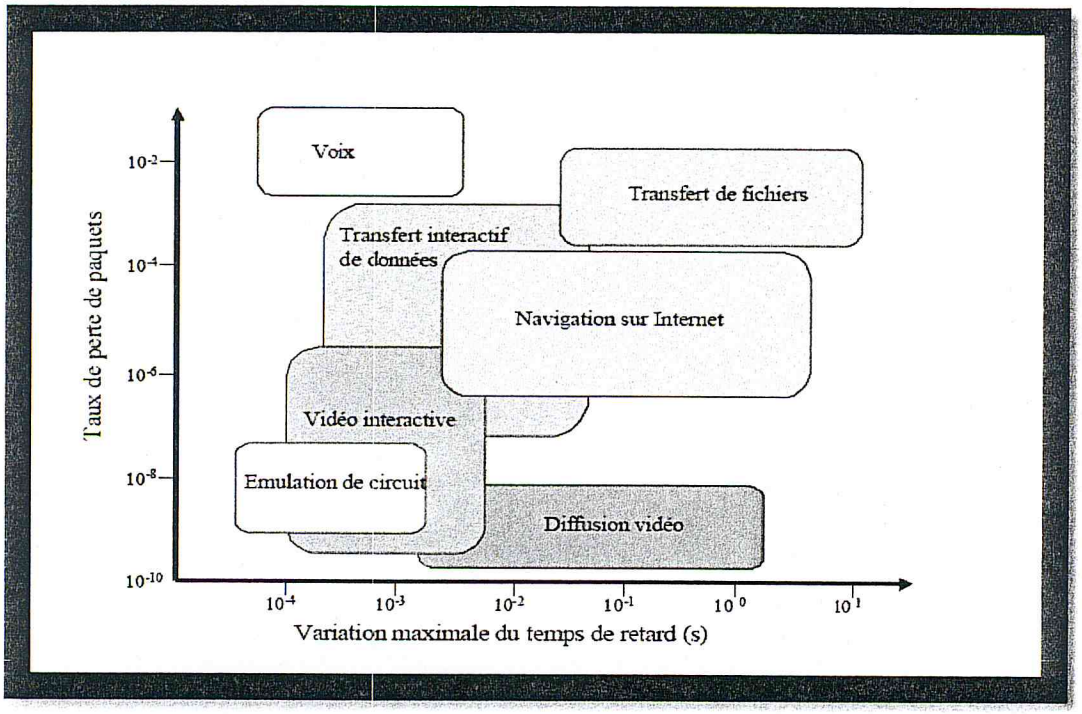


Figure II.1 : Spécifications de qualité de service pour différentes applications [55]

II-4.La gestion de la Qualité de service :

En premier lieu, la QoS doit être garantie au travers de la maitrise des ressources dans le plan de transfert. Ce niveau regroupe l'ensemble des mécanismes inhérents aux technologies de transfert tel que l'ATM, mais également les disciplines de gestion des files d'attentes des équipements. Il est symbolisé par 5 fonctions élémentaires (voir la figure 1) au sens large, que l'on retrouve dans toutes les technologies dans l'ordre suivant du traitement des données :

• **La classification** (C) : ou identification qui consiste a identifier le flux de données. Cette fonction utilise tous les types d'identifiants disponibles selon la technologie de transport. Ils sont soit logique (VP/VC pour l'ATM, LSP pour MPLS), soit du type adresse (IPv4). Il est quelque fois nécessaire de remonter dans les couches (numéro de port) afin de compléter ou distinguer au sein d'un flux différentes composantes.

Le type de service (ToS) est indiqué dans le champ type de service d'un datagramme IP, qui comprend un sous-champ classe de service (CoS) à spécifier. L'en-tête d'un paquet Ipv4 contient 3 bits qui à l'heure actuelle permettent en fait d'identifier quatre classes de service lors de l'initialisation n du champ ToS. Ces considérations sont illustrées sur la Figure suivante[55] :

II-6. Mécanismes de lutte contre la congestion:

Quelle que soit la politique de QoS mise en œuvre, c'est toujours au niveau des files d'attente des routeurs que cette politique est appliquée. Par défaut, dans la politique de l'Internet *best-effort*, tous les paquets arrivant dans le routeur sont placés dans une file d'attente FIFO. Cela permet de traiter tous les flux de la même manière [56].

Il existe deux méthodes permettant de traiter les paquets d'une manière plus évoluée que dans le *best-effort* :

- **La méthode proactive :** traite les congestions bien avant qu'elles se produisent. donc afin de prévenir une éventuelle congestion les routeurs détruisent des paquets aléatoirement, ce qui permet une régulation naturelle en profitant du mécanisme présent dans le protocole TCP. En effet, lorsqu'un paquet est perdu, l'émetteur ne reçoit pas d'acquittement de la part du récepteur et ralentit donc son émission. Le problème est que cela produit un phénomène d'oscillation étant donné que les émetteurs augmentent ou réduisent leurs débits en même temps. Pour pallier à ceci, un mécanisme s'appel RED(Random Early Detection)détecte la congestion avant que des pertes apparaissent en contrôlant le remplissage des files d'attente. En effet, dés qu'une file dépasse un seuil, RED rejette un paquet, ce qui a pour conséquence de faire diminuer le débit d'émission [56]. Dans RED les paquets sont détruits aléatoirement, ce qui ne permet pas de différencier les types de flux.

  Un autre mécanisme qui est WRED (Weighted Random Early Detection) de Cisco vient combler cette lacune en tenant compte de la priorité des paquets puisqu'il possède un seuil pour chaque file correspondant à une classe de trafic. C'est donc en fonction du champ IP Précédence que WRED pourra rejeter un type de paquet pour prévenir de la congestion. Alors que RED et WRED sont basés sur la destruction de paquets en fonction de la longueur moyenne des files d'attente, le mécanisme *Explicit Congestion Notification* (ECN) propose de marquer les paquets plutot que de les rejeter lorsque la longueur de la file dépasse un certain seuil [56].

  Ces méthodes sont relativement satisfaisantes pour les flux TCP, cela dit tous les flux ne sont pas basés sur TCP. Ainsi, si l'on met en concurrence un flux TCP et un flux UDP, le flux UDP en cas de congestion utilisera toute la bande passante disponible au détriment du flux TCP qui lui réduira toujours plus son émission pour arriver à un débit nul [56].

- **La méthode curative :** réagisse une fois que la congestion est arrivée. Lors d'un fonctionnement sans congestion, la mise dans des files d'attente des paquets après classification n'est d'aucune utilité car l'ordonnanceur du routeur pourra traiter tous les paquets. Cela dit, en cas de congestion l'intérêt est tout autre. En effet, en fonction de l'algorithme de gestion de files d'attente choisi, l'ordonnanceur pourra vider préférentiellement une file et laisser une file moins prioritaire se remplir et donc rejeter des paquets. Nous allons voir ici les algorithmes de gestion de files d'attente les plus courants [56].

PQ (Priority Queueing) Cet algorithme est le plus simple à mettre en place. Il permet d'affecter une priorité stricte à une file d'attente. Ainsi si le routeur possède trois files A, B et C, et qu'il est configuré avec un algorithme PQ spécifiant que A est prioritaire sur B qui est elle-même prioritaire sur C on aura le fonctionnement suivant :

– un paquet de la file B ne sera servi que si la file A est vide .

– un paquet de la file C ne sera servi que si les files A et B sont vides[56].

Cet algorithme est intéressant pour gérer le trafic critique mais ne doit pas être utilisé pour un nombre important de flux car les flux non prioritaires seraient systématiquement rejetés [56].

FQ (Fair Queueing) Cet algorithme permet le partage équitable des ressources. Si deux files d'un routeur utilisent FQ, les flux passant dans chaque file auront le même débit en cas de congestion [56].

WFQ (Weighted Fair Queueing) WFQ est identique à FQ mais il permet de pondérer certains flux. Il est ainsi possible de diviser la bande passante entre plusieurs files. WFQ est relativement couteux en ressources car le routeur doit calculer à chaque émission combien de paquets de chaque file seront émis [56].

CBQ (Class Based Queueing) CBQ permet d'allouer une certaine proportion de bande passante pour une classe de trafic. Il est aussi possible de spécifier combien de paquets seront émis à chaque service. CBQ est intéressant si l'on souhaite réserver une partie de la bande passante à un flux spécifique. Par exemple on peut consacrer 30% de la bande passante à un flux vidéo et laisser le reste en best-effort [56].

II-7.Les réseaux multiservices et la QOS :

Après avoir défini plus précisément la qualité de service, nous présenterons les architectures de réseaux multiservices existantes qui permettent d'assurer une certaine qualité de service aux clients.

III-7-1.Les réseaux ATM:

L'ATM se voulant un mode de transfert multi débit et multi service, a place la gestion de la qualité de service au cœur de son architecture. Plusieurs mécanismes ont été introduits afin de rendre une QoS la plus fiable possible. En premier lieu, la séparation en conduit VP(virtual path) et VC (circuit virtuel) permet de séparer les trafics et ainsi les protéger mutuellement les uns des autres. La mise en cellule de longueur fixe et courte permet en outre un multiplexage fin des trafics permettant de garantir un délai et une gigue très faibles pour les services temps réels et conversationnels. Les classes de services ATM les plus courantes sont les suivantes[57] :

• **DBR** (Deterministic Bit Rate) : concerne les applications a débit contant. Le contrat de trafic associe comporte deux paramètres essentiels tel que le débit et la gigue. C'est le plus haut niveau de garantie en terme de QoS mais également le plus contraignant tant pour le client qui doit scrupuleusement respecter son contrat de trafic que pour l'operateur qui ne peut compter sur un multiplexage statistique pour optimiser les ressources de ses réseaux. Elle est utilisée par les applications nécessitant une QoS stricte sur le délai et la gigue, c'est-a-dire celle de la classe de service Voix [57].

• **SBR** (Statistical Bit Rate) : concerne les applications a débit variable . Plus compliquée a utiliser, il faut déclarer a la fois un débit maximal, un débit soutenu, une gigue et une taille maximale de rafale (nombre de cellules émises consécutivement). Et il est utilisée que par les operateurs tant les paramètres a fournir sont complexes a caractériser pour le client. Elle est utilisée pour les applications a débit variable de la classe de service Vidéo [57] .

• **ABT** (ATM Block Tranfert) : permet de réserver des ressources grâce a des cellules spécifiques et de transmettre des données s'accommodant d'un débit variable tout en garantissant durant le transfert du bloc de cellules un niveau de QoS équivalent au DBR. Elle est utilisée pour le transfert de données en mode garanti telle que les applications de la classe de service Donnée [57],

• **ABR** (Available Bit Rate) : est la variante de l'ABT a l'ATM Forum. Elle permet d'obtenir au réseau le débit disponible ou un nombre de crédits plutôt que d'effectuer une réservation absolue [57] .

• **UBR** (Unspecified Bit Rate) : uniquement spécifiée a l'ATM Forum ne garantit rien en matière de QoS. C'est le pendant de la classe de service . Best-Effort . il est généralement associée au transfert de données dans un réseau surdimensionné ou conjointement avec la destruction sélective des cellules [54].

II-7-2.les réseaux IP :

Le réseau Internet est essentiellement basé sur la commutation de paquets et le protocole IP (*Internet Protocol*) qui implémente le modèle *best-effort* : tous les paquets de données suivant la même politique et leur acheminement est effectué de proche en proche. Ce modèle ne permet pas de garantir la QoS de flux multimédias. Pour pouvoir mettre en place des garanties de QoS dans les réseaux IP, l'*Internet Engeneering Task Force* (IETF) a proposé deux modèles d'architecture : IntServ et DiffServ [54] .

II-7-2-1 Le modèle IntServ :

Integrated Services (IntServ) consiste à fournir une QoS garantie stricte sur les réseaux IP. Dans un modèle IntServ, les applications envoient une requête RSVP à fin de réserver les ressources réseau nécessaires. Aprés une négociation avec les gestionnaires de QoS déterminant si le service peut être garanti, les ressources sont réservées ou alors un message d'erreur est renvoyé au demandeur. Une fois les ressources réservées, la QoS pourra être appliquée dans les routeurs avec des algorithmes de gestion de files d'attente [58].

Le but principal de IntServ est de fournir un lien de communication à qualité constante en termes de débit et de délai. La principale limitation de IntServ réside dans son passage à l'échelle, les requêtes RSVP doivent être mémorisées dans tous les routeurs concernés. Or dans un réseau à large échelle tel qu'Internet, il y a une quantité phénoménale de flux concurrents. Une telle quantité imposerait des stockages très conséquents dans la mémoire des routeurs, ce qui engendrerait un surcout inconcevable [58].

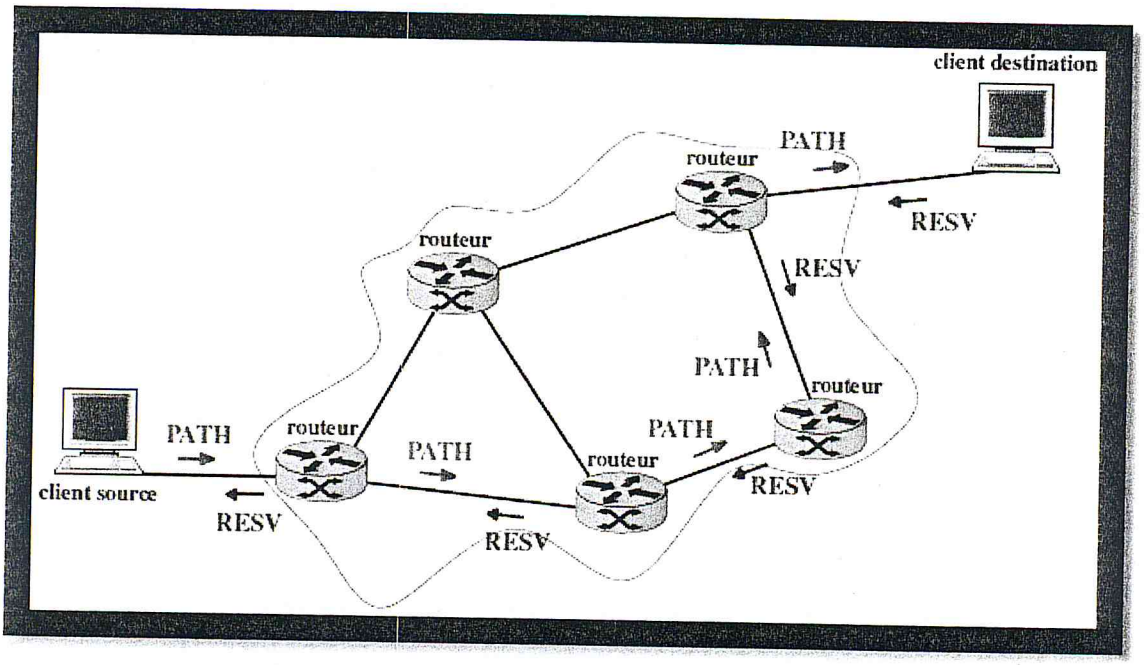


Figure II.5: Réservation de ressources dans les réseaux IntServ [57]

II-7-2-2 Le modèle DiffServ :

Le modèle à différentiation de Services (DiffServ) ajoute des nouvelles fonctionnalités aux routeurs de l'Internet afin d'améliorer la Qualité de Service offerte aux flux.

Des contraintes telles que la réduction du délai d'acheminement ou le contrôle dans la distribution de ressources peuvent être satisfaites grâce aux mécanismes proposés par ce modèle. A travers le Comportement Assuré, le modèle DiffServ introduit le concept d'élimination sélective basée sur un niveau de priorité [59].

D'un coté, cette notion peut être exploitée pour distribuer équitablement les ressources réseau indépendamment du comportement des sources. De l'autre, en utilisant des algorithmes de codage audio/vidéo multi- couches, la notion de priorités peut réduire considérablement l'effet de pertes sur la transmission de flux multimédia [58].

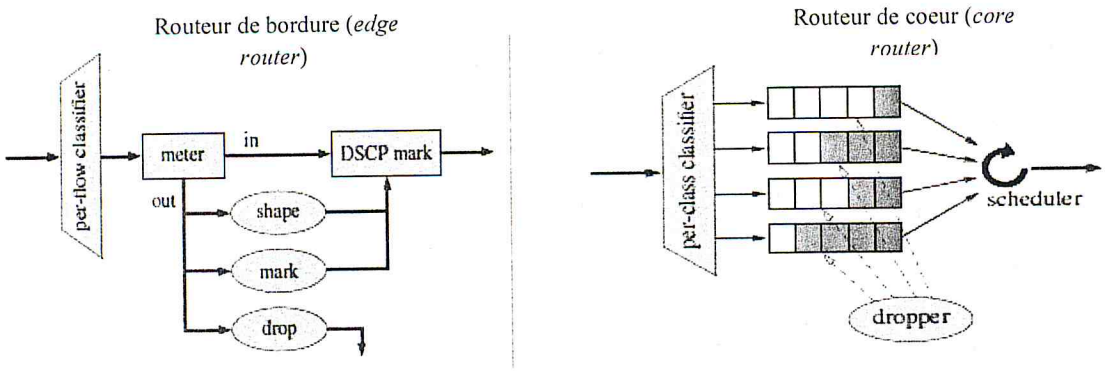


Figure II.6:Fonctionnement des routeurs *edge* et *core* dans une architecture DiffServ [57]

II-7-3 Les réseaux MPLS :

La fonction QoS MPLS assure qu'un trafic important est traité avec la priorité adéquate sur le réseau et que les exigences de latence sont respectées. Les mécanismes de qualité de service IP peuvent être mis en œuvre de façon transparente dans un environnement MPLS [60].

La gestion de la QoS et de l'ingénierie du trafic est réalisée sous MPLS grâce au plan de contrôle qui fournit une granularité suffisante pour la partition du trafic (FEC) et offre des moyens permettant d'associer à chaque partition du trafic un LSP établi avec ou sans réservation de ressource et non contraint par le protocole de routage employé (grâce au routage explicite). Ainsi, l'ingénieur réseau peut optimiser son réseau en répartissant le trafic en plusieurs classes. chaque classe assure une certaine QoS en utilisant un LSP qui réduit la consommation des ressources [61].

MPLS-TE permet de réserver de la bande passante pour des LSP aux classes de services. La réservation s'effectue selon deux modes. Le modèle conservateur . Maximum Allocation Model -MAM . qui n'autorise pas un LSP a prendre de la bande passante dans un LSP de priorité inferieure qui en disposerait ; le modèle dit des poupées russes . Russain Dol Model - RDM . qui permet le chevauchement des LSP de priorités supérieures sur les LSP de priorités inferieures. Le routage des paquets dans les LSP est effectué directement a partir du champ DSCP sans nécessiter de configurer une entrée dans la table de FEC [54].

Nous arrivons a conclure que Le support de la QoS peut être mise en œuvre de deux façons sur MPLS :

- 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 [62].
- L'utilisation du Traffic Engineering, MPLS-TE(MPLS-Traffic Engineering) est un terme générique qui englobe l'utilisation de plusieurs technologies telles que RSVP-TE, OSPF, le tunnelling, etc… afin de permettre le Traffic Engineering [62].

II-8-QOS et protocoles avantages et limitations:

Les architectures de réseaux multiservices avec un véritable support de la qualité de service pour tous les types d'applications montrent que celle-ci peut (et doit) être prise en compte dans tous les nombreux mécanismes impliqués dans le fonctionnement du réseaux : protocoles, ordonnancement, routage, admission, conception de réseau... Seulement, elle complexifie grandement la conception et la mise en place de tous ces mécanismes. Nous présentons dans cette section un aperçu (loin d'être exhaustif) des problématiques soulevées directement ou indirectement par la QoS.

- **Acquisition et synchronisation de données :** Les architectures basées sur la commande centralisée implémentant des fonctions d'admission d'appel et de réservation de ressources sont qualifiées de solution . Off-Path ..

  En effet, la demande de QoS ne suit pas le même chemin que les données. Afin de pouvoir réaliser une gestion efficace de la QoS, il est nécessaire de connaitre la topologie du réseau contrôle ainsi que le chemin que va emprunter les donnes. Les différentes implémentations utilisent en général une base de données qui contient les informations de topologie ainsi que les réservations en cours sur les différents liens et équipements. Il faut donc pouvoir alimenter cette base de données automatiquement surtout dans le cas du contrôle de réseaux de grande taille. De même, en cas de modification de ce chemin (re-routage dans les reseaux IP, pannes,ajout, ...), la fonction d'admission d'appel doit impérativement être informée de ces nouvelles données afin de mettre a jour sa base de données et exécuter de nouveau les algorithmes d'admission d'appel et de réservation de ressources sur cette nouvelle topologie [54].

- Hormis l'écoute des protocoles de routage des réseaux IP et le protocole MPLS qui à son tour basé sur un protocole de routage pour pouvoir diffuser des labels , il n'existe pas de solution satisfaisante pour acquérir automatiquement et maintenir a jour les topologies des réseaux. Cela rend, d'un point de vue opérationnel, l'utilisation de ces architectures complètement caduque [4].

- **Paramétrages et lien avec les applications** Si un operateur souhaite garantir une QoS relative, une gestion par classe de service et priorité des files d'attentes est suffisante. Par contre, il est vain de croire qu'une solution de gestion de la QoS peut être découplée des applications des lors qu'il souhaite garantir un niveau de qualité de service absolue. Pour cela, il est indispensable de pouvoir synchroniser la demande de QoS avec le début et la fin de l'application. En effet, la solution doit pouvoir gérer les erreurs engendrées par des pannes, des arrêts brutaux, ... sous peine de devoir gérer des réservations fantômes dans le réseau. Détecter les débuts et fins d'activités au niveau TCP est très délicat et encore moins faisable au niveau UDP. Il faut donc remonter dans les couches protocolaires, pour arriver finalement au niveau de l'application. En outre, il est impératif de disposer de paramètres fiables et correspondant aux données de service (débit et durée d'une video, nombre de flux),La difficulté vient a la fois pour les applications de spécifier correctement les paramètres de QoS associes a leur besoin réel et pour le réseau d'identifier les flux d'une application donnée [54].
  - la classification par adresse ip source et destination, port source et destination, protocole ne fonctionne pas dans tous les cas, notamment lorsque les paquets IP sont fragmentes ou lorsque les applications sont situées derrière une fonction de NAT. Le recours a des marqueurs simples, sans toutefois devoir gérer des agrégats comme avec le champ DSCP [AN24], est indispensable [4].
- **Performance et passage a l'échelle :**Toute solution se doit d'être extensible et pouvoir être appliquée a des réseaux de grande taille. Dans l'inventaire réalisé, seules les techniques garantissant une qualité de service relative peuvent prétendre a une application a toute échelle de réseau, y compris a l'échelle de l'Internet. Les signalisations telles que RSVP échoue dans cet exercice [54].
  - Seul MPLS-TE qui a été conçues des le départ avec un souci de hiérarchisation, supportent l'extensibilité.

Si l'augmentation de la taille des réseaux est déjà un problème en soi, il faut également compter avec l'augmentation du nombre d'utilisateurs. Ainsi, le nombre de requêtes de QoS par unité de temps va suivre une loi en $\Theta(n2)$ ou n désigne le nombre d'utilisateurs. Même si toutes les applications n'ont pas besoin de QoS particulière, et donc peuvent se contenter du mode . Best-Effort ., le nombre d'états a maintenir dans le réseau va également croitre selon la même loi.

- A nouveau, seules les solutions hiérarchiques abstrayant les niveaux inferieurs comme MPLS-TE, permettent de s'affranchir de ce problème en gérant, a un niveau donné, un nombre borné de réservations .

- **Le Routage et la QOS** :Les algorithmes de routage sont utiles bien évidemment pour l'acheminement des données mais aussi pour l'allocation de ressources le long des chemins. L'introduction de la qualité de service de bout en bout rend ces problèmes de routage plus complexes.

  L'approche la plus simple pour effectuer le routage d'un flot donné entre une source et une destination consiste à choisir le plus court chemin. C'est l'idée sous-jacente du routage *best-effort* des réseaux IP (c'est aussi le routage par défaut dans MPLS), qui utilise des algorithmes distribués de plus court chemin. La métrique utilisée pour calculer les plus courts chemins peut être choisie pour prendre en compte la QoS. Cette métrique peut être soit statique, la table de routage est alors elle aussi statique, soit dynamique c'est-à-dire qu'elle est déterminée par des échange de messages entre les routeurs, la table de routage est alors réactualisée régulièrement.

  Les protocoles classiques (comme RIP, *Routing Information Protocol*, ou OSPF, *Open ShortestPath First*) se contentent en général de découvrir la topologie du réseau et ainsi établir la connexité des nœuds. La métrique utilisée par défaut est alors simplement le nombre de sauts (ou de *hops*) entre l'origine et la destination. Ces protocoles sont parfois adaptés pour supportés des critères supplémentaires de QoS

  Le problème de routage avec des contraintes de QoS est par ailleurs intrinsèquement plus complexe que le problème du plus court chemin. La difficulté se concentre sur les critères de QoS qui s'expriment de façon additive ou multiplicative le long du chemin. Alors qu'une contrainte portant sur la bande passante est une contrainte «facile» car s'exprimant simplement sur les arcs, une contrainte sur le délai de bout en bout, la gigue ou sur le taux de perte rendent le problème de routage particulièrement difficile car elles s'expriment additivement ou multiplicativement le long du chemin. Ainsi

trouver un chemin optimal pour une paire origine-destination donnée avec une ou plusieurs contraintes additives (typiquement le délai) est, semble-t-il, un problème NP-complet [57].

- Le réseau MPLS utilise les fonctions de routage IP pour établir un LSP:le message d'établissement est alors routé comme le serait n'importe quel autre paquet IP contenant la même adresse destination. Dans ce cas, le routage se fait "hop by hop ", chaque routeur décidant par lui –même de l'interface de sortie vers la quelle il envoie le message, indépendamment de ce que les routeurs précédent ont pu choisir. Ce mode de fonctionnement permet à un opérateur d'établir simplement un LSP entre deux extrémités de son réseau. De plus, un tel mode de fonctionnement permet de sécuriser des LSP en autorisant leur re-routage en cas de faute dans le réseau.

  Le reroutage rapide avec l'architecture MPLS permet une reprise très rapide après la défaillance d'une liaison ou d'un nœud. Une telle rapidité de reprise empêche l'interruption des applications utilisateur ainsi que toute perte de données.

Jusqu'à présent nous avons présenté la qualité de service dans les réseaux multiservices tel que IP ATM et MPLS et relevé quelques grandes problématiques liées à la garantie de celle-ci pour tous les clients du réseau. Nous passons maintenant a définir les travaux ayant déjà été effectués dans le domaine de la Qualité de Service .

II-8-Les différents travaux sur la QOS dans les réseaux :

Voyons maintenant quelques travaux ayant déjà été effectués dans le domaine de la qualité de service .nous présentons plusieurs approches :

- La QOS au niveau application .
- QOS utilisant le réseau sous-jacent .
- Le mécanisme de QoS sur les nœuds .

1-QOS niveau application : Lorsque l'on conçoit une application utilisant le réseau, il peut être important de prendre en compte le fait que le réseau pourra perturber ou limiter le fonctionnement normal de l'application. Ceci est particulièrement vrai dans les applications multimédia, par exemple pour la diffusion de vidéo ou les contraintes de délai et de gigue sont prédominantes pour obtenir un résultat satisfaisant.

Afin de caractériser cela, nous allons donc prendre l'exemple de la diffusion de vidéo au format MPEG. Un flux MPEG est composé de trois types d'images que l'on appelle I, P et B. Ces images n'ont pas toutes la même importance, nous allons présenter leur rôle ici :

– les images I (Intra frame) sont celles qui contiennent le plus d'information, elles sont indispensables pour obtenir une qualité d'image satisfaisante mais elles sont les plus lourdes

– les images P (Predicted frame) contiennent un peu moins d'information mais sont plus légères que les images I, elles sont calculées à partir d'une image I ou P précédente ;

– les images B (Bi-directionnal frame) sont les plus légères mais celles aussi qui possèdent le moins d'information, elles contiennent les différences entre l'image I ou P précédente et l'image I ou P suivante.

Au vu du fonctionnement de MPEG, nous pouvons comprendre que dans un flux multimédia, tous les paquets n'ont pas la même importance. On pourra en effet perdre des images P ou B mais la perte d'une image I serait vraiment néfaste au rendu final puisque que cela entrainerait la perte de toute une séquence (*Group of Picture*, GoP), soit une perte d'une demi-seconde de vidéo utilisant 24 images par seconde.

- C'est sur cet aspect que portent les travaux de Bhattacharjee, Calvert et Zegura [63]. En effet, en cas de congestion dans le réseau, il peut être envisageable de supprimer des images de types P et B afin d'alléger le trafic.

  Cette suppression d'images est tout à fait faisable avec les réseaux actifs. Il suffit de regarder le type de l'image et dans le cas o`u il y a congestion on la supprime si elle n'est pas de type I. La vidéo sera ainsi de moins bonne qualité mais au moins elle sera diffusée.

  - Cette méthode est intéressante puisqu'elle résout en partie les problèmes de congestion réseau, donc on peut pas réellement parler de QOS pour deux raisons principale, parce que si l'on a déjà supprimé les images B et P et qu'il y a encore de la congestion il n'y a plus de solution, en plus si d'autres flux empruntent le même réseau, on ne peut pas être sur que le flux vidéo sera prioritaire ou même qu'il ne sera pas complètement écrasé (par un flux UDP par exemple).

- Une autre aidée mais toujours dans le cas de QOS au niveau application c'est dans [64],ou les auteurs se sont basés sur les réseaux de neurones, l'idée et de trouver une méthode pour modéliser la façon selon laquelle les auditeurs évaluent le son transmis à travers le réseau donc le principe et de construire un automate basé sur les réseaux de neurones pour mesurer en temps réel la qualité subjective de la parole, Les facteurs les plus importants que les auteurs ont pris sont les paramètres de réseau (cadence de perte de paquet, distribution des paquets…)et les paramètres de codages (le type de codec utilisé…)et aussi l'étude de différents modèles de pertes sur l'Internet, avec le but de raffiner la performance de leurs outils .ils ont aussi travaillé sur l'évaluation de la qualité subjective du flux vidéo dans un réseau de commutation de paquets tel qu'IP L'idée est de faire des mesures en temps réel et d'intégrer des facteurs tels que la cadence de perte, la largeur de la bande passante, le rapport du nombre de macro-blocs codés en intra et en inter dans la séquence vidéo, le type de codec visuel, etc.…

Le résultat obtenu de ce travail est un réseau neuronal pour lequel les expérimentations montrent de bonnes performances pour l'évaluation de la qualité du son.et une transmission plus au moins bonne pour les flux vidéo .

  - Cette approche a évalué la qualité de service mais juste pour les flux audio et vidéo .

2-QoS utilisant le réseau sous-jacent :Etant données les limitations de l'approche précédente, notamment pour donner priorité à un flux sur un autre, des travaux se sont focalisés plus précisément sur l'idée d'utiliser la QoS du réseau sous-jacent. L' intérêt d'utiliser les réseaux actifs est de pouvoir paramétrer dynamiquement les politiques de QoS au sein du réseau.

- Dans [65], les auteurs Omar Cherkaoui, Mauro Fonseca et Nazim Agoulmine mettent en œuvre un système visant à rendre possible le déploiement de politiques de QoS entre deux FAI. En effet, il est relativement aisé de faire de la QoS pour des utilisateurs d'un même FAI car le contrôle peut être centralisé, mais dés que les utilisateurs se trouvent connectés à des FAIs différents cela devient très difficile à contrôler. Les FAI utilisent dans ce cas des nœuds actifs pour détecter les congestions et négocier entre eux les choix de politiques de QoS à appliquer. Cela permet ainsi d'assurer un meilleur service de bout en bout pour des utilisateurs qui n'appartiendraient pas au même FAI.

- Une autre approche présentée dans [66] et [67] a consisté à développer un routeur virtuel. Ce routeur virtuel, programmé en C++ propose une émulation de la couche IP en implémentant par dessus TCP, UDP, ICMP et CIP (un interpréteur de capsules). Il comporte aussi : classifier, token bucket filter, drop tail queue, RED, WFQ, Round Robin et Priority Round Robin scheduler, marker for DiffServ. Un routeur virtuel peut être connecté à un autre routeur virtuel ou à un routeur traditionnel via une interface . Le principe est que les paquets arrivant sur le routeur (une machine sous Linux) sont transmis au routeur virtuel via d'autre interface. A partir de là, les paquets sont traités (routage, suppression) par le routeur virtuel. Les services actifs chargés de gérer la QoS modifient directement les règles de QoS du routeur virtuel à travers une API dédiée, ce qui aura pour effet de modifier le champ TOS des paquets. Cette méthode est intéressante puisqu'elle est trés performante étant donné que le routeur virtuel est implanté à un niveau très proche du système. Cela dit son implantation est contraignante puisqu'elle nécessite l'installation d'un module dans le noyau Linux.
    - Les méthodes présentées ci-dessus et qui utilisent les systèmes traditionnels comme base du réseau, ce qui est un avantage incontestable pour l'interopérabilité. Il peut être intéressant en effet d'avoir des routeurs actifs qui marquent les paquets en bordure de réseau et de laisser les routeurs et switchs traditionnels traiter les paquets au cœur du réseau tout en gardant les mêmes propriétés de QoS. Toutefois ces méthodes nécessitent des accès système à un relativement bas niveau, ce qui est difficilement réalisable si l'on est pas administrateur de la machine.

3-QOS sur un nœud : en traitant les paquets. On pourra distinguer dans ce cas deux méthodes :

- le contrôle de flux actifs, basé sur des techniques de différenciation de flux .
- l'´equilibrage de charge, basé sur le choix de routage en fonction de la congestion.

- Concernant le contrôle de flux actifs :Dans [68], les auteurs Rima Kilany, Eric Horlait , Nicolas Rouhana se sont basés sur ANTS pour y ajouté un mécanisme de files gérant des priorités de services comme dans DiffServ. L'idée est d'ajouter à chaque nœud

d'ANTS un scheduler qui pourra être chargé dynamiquement. DiffServ a été implanté pour gérer 3 types de trafics : premium, assured et *Best Effort*. Un module de classification permet de séparer les capsules en fonction d'un *id* et ainsi de traiter le trafic premium (avec une file traitée en priorité) et les deux autres trafics (avec une file et un algorithme RED). Des tests ont été effectués, toutefois aucun résultat n'a été publié. D'après les auteurs, le système était pénalisé par le lancement d'un grand nombre de threads et par l'utilisation de la JVM qui ralentit d'un facteur 10 le traitement des paquets.

- Concernant l'équilibrage de charge :Dans [69] Salvatore Gaglo et Guiseppe Lo Re proposent une manière originale de faire de la QoS à l'aide de réseaux actifs. En effet, ils utilisent la méthode de déplacement des fourmis pour résoudre les problèmes de congestion. Les fourmis constituent un modèle parfaitement décentralisé de communication puisqu'elles ne réagissent qu' à leur environnement local. Voyons comment les fourmis font pour

- trouver par exemple le plus court chemin de leur fourmilière à une ressource de nourriture. Au départ, les fourmis peuvent emprunter toutes les routes possibles. De plus, elles libèrent des phéromones tout au long de leur chemin. D`es que certaines fourmis ont commencé à revenir à la fourmilière, celles qui vont partir iront l`a ou il y a le plus de phéromones, et vu que c'est à l'endroit ou le chemin est le plus court que les fourmis seront les premières arrivées, c'est aussi sur ce chemin qu'il y aura le plus de phéromones.

  Pour appliquer ceci à la congestion dans une route réseau, les auteurs utilisent la même approche. En effet, chaque nœud possède une table de routage qui contient toutes les routes vers une destination avec le temps qu'il faut pour atteindre cette route. Périodiquement le nœud envoie aléatoirement des paquets à une destination, en mesure le temps et met à jour sa table de routage. Ainsi lorsqu'un paquet actif arrive sur un nœud, il consulte la table de routage pour savoir ou il y en a le plus (c'est-`a-dire ou la route est la plus courte) et il prend cette direction.

- Une approche basée sur les algorithmes génétiques à été proposée dans [70]. Ici tout est basé sur l'adaptabilité du réseau. L'idée est d'évoluer en n'utilisant pas un système stochastique mais en expérimentant et en apprenant. L'adaptation est réalisée en

sélectionnant certaines actions que le système a appris (comme un réseau Bayésien) et en implémentant ces actions. Il a été prouvé que les algorithmes génétiques offrent de très bons résultats pour l'adaptabilité. Leur approche de DiffServ est un peu différente d'une approche traditionnelle puisqu'ils partent du principe que la qualité de service se fait sur le temps de latence accepté des paquets. En effet un type de paquet demandant une faible latence aura un taux de perte plus grand qu'un autre puisque il faut dans ce cas que les files d'attente soient courtes. Ce temps de latence peut être modifié en ajustant le *Time To Live* (TTL) des paquets. Dans ce contexte, les serveurs rapides ont une petite file d'attente et un haut taux de perte alors que les serveurs lents ont une grande file d'attente et un taux de perte bas. L'adaptation du nœud actif peut se faire en ajustant la taille de sa file d'attente.

Dans ce système, chaque nœud DPS (Dynamic Proxy Server) est responsable de son propre comportement (chaque DPS optimise de manière *égoïste* son état). Chaque service est représenté par 3 gènes {x,y,z} ou :

– x représente le type de service ;

– y représente une valeur telle que : une requête de type x est acceptée si la file de x est inférieure à y ;

– z représente une valeur telle que : une requête de type x est acceptée si le taux d'occupation de x est inférieur à z.

Au départ, le système est initialisé en plaçant aléatoirement les services sur les DPS. Le système s'équilibre ensuite tout seul (mutations et migrations). Les mutations consistent à changer aléatoirement un paramètre d'un gène (ie. d'un triplet {x,y,z}) et les migrations consistent à prendre de nouveaux gènes du pool de gènes ou à en donner aux autres en fonction de la charge.

Lorsqu'un paquet arrive sur un nœud qui ne possède pas de DPS, il est envoyé au voisin. Si la requête en tète de file d'attente correspond au service propos´e et qu'elle possédé un nombre de jetons suffisant (inclus par le client), le service va être effectué et le nœud reçoit une nombre équivalent de jetons. Si la requête ne correspond pas, aucun jeton n'est donné et le paquet est envoyé selon une table maintenue par le DPS (les paquets avec un petit TTL iront vers un DPS avec une file d'attente courte). A priori cette méthode permettant d'avoir des nœuds actifs autonomes donne de bons résultats pour une QoS de bout en bout. Ces méthodes basées sur l'´equilibrage de charge sont fonctionnelles mais ne permettent pas de s'adapter rapidement aux

fluctuations de débit. De plus les approches de contrôle de flux ne sont en aucun cas opposées à l'équilibrage de charge mais au contraire elles sont complémentaires.

- Pour les méthodes appliqués au niveau des nœud et qui sont basées sur l'équilibrage de charge sont fonctionnelles mais ne permettent pas de s'adapter rapidement aux fluctuations de débit. De plus les approches de contrôle de flux ne sont en aucun cas opposées a l''equilibrage de charge mais au contraire elles sont complémentaires.

II-9-Les limites des travaux :

Les différents travaux ayant déjà été effectués dans le domaine de la qualité de service surtout dans le but d'éviter la congestion se devisent en 2 grands catégories de méthodes soit proactives ou curatives.

Les méthodes proactives traitent les congestions bien avant qu'elles se produisent. Elles permettent de répartir la charge dans le réseau et d'éviter qu'une demande supplémentaire ne soit créée lorsque celui-ci atteint un certain niveau d'encombrement. Ou bien les routeurs détruisent des paquets aléatoirement, ce qui permet une régulation naturelle en profitant du mécanisme présent dans le protocole TCP. En effet, lorsqu'un paquet est perdu, l'émetteur ne reçoit pas d'acquittement de la part du récepteur et ralentit donc son émission.

Le problème avec les mécanismes proactifs c'est que ceux-ci limitent le trafic sur le réseau de façon importante. En effet, la plupart de ces techniques réservent une bande passante maximale pour des flux alors que celle-ci n'est pas toujours utilisée. Il est également possible que le niveau maximum de bande passante utilisée ne soit pas le niveau maximum offert. Certains mécanisme bloquent les flux lorsque 80 % de la bande passante offerte a été atteinte. Dans ces cas, beaucoup de demandes de clients peuvent être bloquées alors que le réseau n'est pas utilisé à son maximum.

Les mécanismes curatifs réagissent une fois que la congestion est arrivée. Cela veut dire que le délai s'est allongé de manière importante et que des paquets ont été détruits.

L'ensemble de ces techniques génère deux types de problèmes. Tout d'abord une mauvaise utilisation des capacités du réseau qui pourrait être plus chargé. Mais on peut aussi faire face à des dégradations de services. Ces techniques agissent donc trop tôt ou trop tard. Il est donc important de trouver une méthode agissant entre les deux et pouvant s'adapter au comportement du trafic.

Conclusion :

ce chapitre a été consacré pour définir en général la QOS dans les réseaux multiservices. dans une partie de ce dernier nous sommes intéressés aux différentes architecture de réseaux multiservices en vigueur aujourd'hui qui permettent de garantir cette qualité de service . Parmi ces architecture , L'architecture MPLS est certainement l'une des plus abouties en matière de gestion de la QoS dans les réseaux IP. La signalisation MPLS permet au final de recréer un mode connecté par commutation de label au dessus de l'IP tout en gardant la souplesse du routage de bout en bout.

Aussi nous avons effectué un tour d'horizon des problématiques liées a la QOS dans les réseaux multiservices et que MPLS répond a certain d'eux. Pour cela Nous avons vu qu'il existait quelques travaux dans ce domaine, mais il sont limités et permet de répondre a une partie de besoins de la QOS, En se basant sur tout ce qu'a été présenté dans ce chapitre nous proposerons par la suite notre propre solution développé dans le but d'améliorer la QOS dans les réseaux multiservices .

Dans le chapitre suivant, nous allons étudier le réseau actuel de la société SONATRACH voir ses besoins et ses limitations et nous passons en deuxièmes partie a implémenter une nouvelle architecture capable a répondre au besoins de SH .

Introduction :

L'étude de l'existant est une étape essentielle dans notre démarche, qui vise à représenter l'architecture du réseau informatique déployée au sein de l'entreprise SONATRACH et de comprendre son fonctionnement. Elle permet de souligner les anomalies présentent dans le réseau et pouvant affecter son bon fonctionnement, afin de proposer des solutions qui résolvent les insuffisances relevées.

Nous commençons par une vue globale sur l'entreprise SONATRACH, sa structure, et son objectif ainsi ses diverses activités et nous passon par la suite a décrire le réseau WAN actuel .

III -1-Présentation de SONATRACH :

III -1-1.Définition :

SONATRACH est une entreprise publique économique à caractère industriel et commercial dénommée **S**ociété **Na**tional de **Tran**sport, transformation et **C**ommercialisation des **h**ydrocarbures. Elle a été créée par le décret présidentiel **N 63-49**, du **31** décembre **1963**.elle exerce ses métiers en Algérie et partout dans le monde ou des opportunités d'investissement existent.

III -1-2.Organisation de SONATRACH :

Le schéma de la macrostructure de SONATRACH s'articule autour de la direction générale, des activités opérationnelles et des directions fonctionnelles.

- ***la direction générale du groupe***

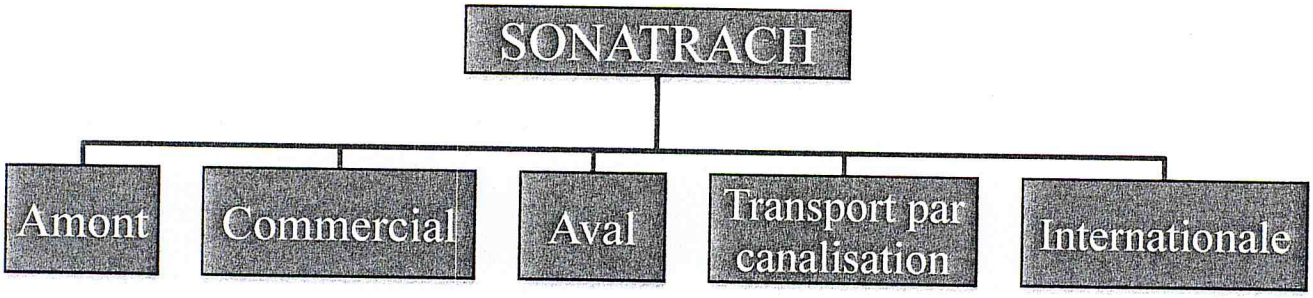
Elle est assurée par le Président Directeur Général qui est chargé d'apporter l'appui nécessaire dans le monitoring et la coordination de management du groupe,

- ***Les activités opérationnelles***

Elles exercent les métiers du groupe et développent son potentiel d'affaires qui tant en Algérie qu'à l'étranger, elles sont au nombre de cinq:

- *Activités Amont (AMT) :* qui comprennent la recherche et le développement des hydrocarbures, le forage, la production, l'engineering et les associations.

- *Activités Aval (AVL)* : qui comprennent la liquéfaction du gaz naturel, le raffinage du pétrole, la pétrochimie et les études.
- *Activités transport par canalisation(TRC)* : qui comprennent l'exploitation des ouvrages de transport des hydrocarbures et des installations portuaires.
- *Activités commerciales (COM)* : spécialisées dans la commercialisation des hydrocarbures et du transport maritime.
- *Les activités internationales* : sont chargé de l'élaboration et de l'application de la politique et de la stratégie de développement d'expansion en International.



Après avoir défini la société SONATRACH nous passons a présenter la division ou nous avons effectué notre stage.

III-1-3.La division Production (DP) :

Dans le cadre de l'exploitation, de la maintenance et du développement des champs pétroliers (gaziers et industriels) et des bases de vie et de communication, la division de production s'est dotée :

- ❖ D'une structure au niveau de chaque région et secteur, chargée de l'approvisionnement, du transport sur site, du stockage et de la gestion de matières et matériels
- ❖ Au niveau de son siège à Alger, d'une direction d'approvisionnement et au transport des régions et des secteurs .

La division production (SH/DP) est organisée comme suit :

- o Direction centrale dont le siège est sur Alger.
- o Neuf directions régionales réparties dans le sud du pays.

Au niveau central au siège d'Alger la DP est structurée en six directions et deux départements:

- Direction finances et comptabilité.
- Direction ressources humaines et organisation.
- Direction opérations.
- Direction approvisionnements et transport.
- Direction moyennes généraux.
- Direction sécurité industrielle.
- Département sécurité industrielle.
- Département informatique.

Nous passons maintenant a défini la direction ou on a réaliser notre étude .

III-1-4.La Direction informatique

Dans le cadre de l'exploitation la maintenance et le développement des systèmes d'informatique.la division production à crée la direction informatique au siège pour s'est besoin informatique dont les objectif son le développement des systèmes d'exploitation ; la gestion des projets ; et ainsi la partie qui fait objet de notre sujet la partie de développement des réseaux. Cette direction contient quatre départements :

- Département réseaux et télécommunication.
- Département systèmes et exploitations.
- Département maintenance.
- Département développement.

Le département réseaux et télécommunication a pour missions :

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

III-2-Architecture de l'existant:

III-2-1.Matériels existant :

III-2-1-1.Equipements :La visite de la salle des équipements informatique et de la salle télécom nous a permet de connaitre que Le matériel réseau actif est composé de routeurs, commutateurs L2, L2/L3 de marque CISCO essentiellement.

Type de l'équipement	Abréviation	Modèle de l'équipement	Niveau de l'équipement	Le symbole
Routeur	R	7200VXR	L3	
Switch d'accès	ASW	6500, 4500	L3	
Switch de distribution	DSW	3750, 2900	L2/L3	
Cisco ASA firewall	ASA	ASA5520	L3	

Tableau III.1 : liste des équipements

III-2-1-2.Câblages :le câblage utilisé par SONATRACH est présenté dans le tableau ci-dessous .

Le symbole	Le nom et le type
	fastEthernet
	Ligne spécialisé de type 1 X E1 = 32 lignes E0 (2Mbps)
	Ligne spécialisé de type 2 X E1
- - - - - - - - - -	Ligne spécialisé de type 3XE1

Tableau III.2 : liste de câblage

III-2-2. La topologie LAN existante:

Le réseau local de siège Amont de SH suit le modèle de conception en couche "hiérarchique" dont chaque couche joue un rôle spécifique.

- **La couche d'accès :** sert d'interface avec les périphériques finaux, tels que les ordinateurs, les imprimantes…etc. Cette couche inclut onze 11 ASW-4550-L1(Switch d'accès) qui sont distribués sur les 6 niveaux constituant le siège amont de SH. Des Vlan sont configurés sur les Switch d'accès et les périphériques finaux, ce qui permet à plusieurs sous réseau d'exister sur le même réseau commuté.

- **La couche distribution :** elle relie la couche accès à la couche cœur du réseau, son principale rôle est le regroupement des données reçues à partir des commutateurs de la couche d'accès avant leur transmission vers la couche cœur de réseau pour les filtrer, router, autoriser ou non les paquets. cette couche inclut deux DSW-6506-L3.

- **La couche cœur de réseau :** elle constitue le réseau fédérateur, d'une part elle est reliée avec la couche distribution, d'une autre part elle sert d'interface entre le réseau local et le réseau extérieur. cette couche inclus quatre routeurs C 7200, deux DSW-3750-L3, un par feu de type ASA 5520.

Le réseau de données s'appuie sur une infrastructure principale composée de deux liaisons en fibre optique, une vers le site distant avec 2Mb/s et l'autre pour internet.

- **Les serveurs :** SONATRACH dispose d'un parc de serveur qui son installé dans la salle réseau ils sont relié avec le SW-3750-L3 pour fournir des applications tels que Outlook, l'Active Directory, Windows server et autre.

Le schéma suivant est une description de réseau LAN de siège Amont au niveau de SONATRACH

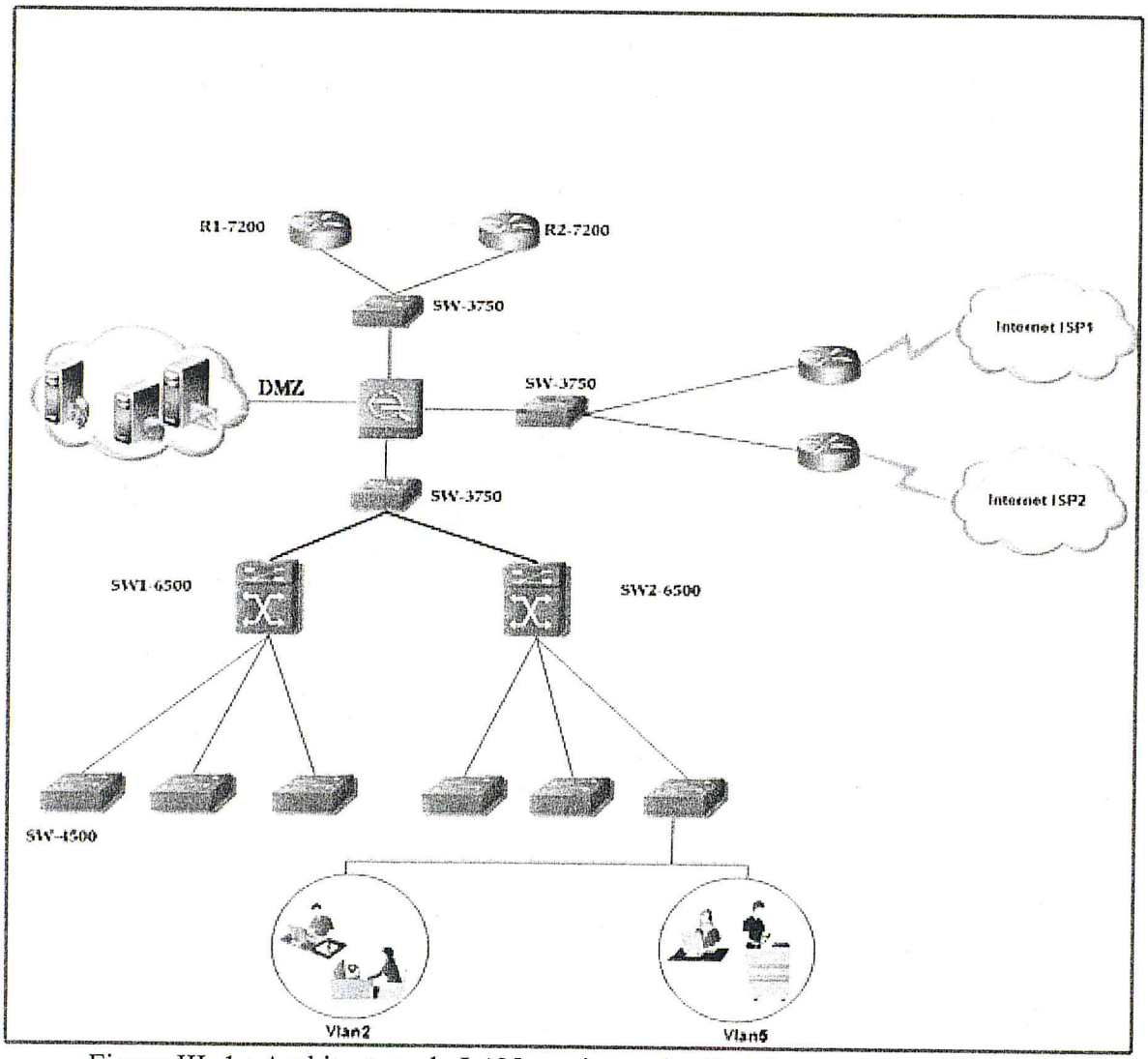


Figure III. 1 : Architecture de LAN au niveau de siège Amont SONATRACH

III-2-3.La topologie WAN existante:

SONATRACH est l'une des sociétés qui dispose d'un réseau informatique homogène. Elle a besoin de communiquer quotidiennement entre ses différents sites distant, pour répondre à ce besoin.

SONATRACH dispose d'un réseau de transmission de données a couverture nationale de type WAN (Wide Area Network) comportant des routeurs 7206-VXR a intégration de services du fournisseur CISCO permettant d'acheminer le trafic données et voix en utilisant le protocole TCP/IP ainsi que le protocole du routage dynamique OSPF.

SONATRACH dispose de 25 sites répartis dans l'Algérie, les 4 sites : Alger siège Amont Hydra, Hydra 10,Rue du Sahara, HASSI MESSAOUD et HASSI R'MEL sont considérés comme des sites principaux ou bien ''les backbones''.

Ses 4 sites sont interconnectés par des liaisons de la fibre optique réalisons une architecture full mush .

SONATRACH dispose de 8 sites dans le sud de pays ,Chacun de ces sites est relié au deux principaux sites Hassi R'mel et Hassi Messaoud par des liens 2 x E1 ,et chaque deux routeurs adjacents a coté sont reliés par des liens 1 x E1 .

Le schéma ci-dessous représente l'architecture actuelle de ce réseau :

SONATRACH dispose de 25 sites répartis dans l'Algérie, les 4 sites : Alger siège Amont Hydra, Hydra 10,Rue du Sahara, HASSI MESSAOUD et HASSI R'MEL sont considérés comme des sites principaux ou bien ''les backbones''.

Ses 4 sites sont interconnectés par des liaisons de la fibre optique réalisons une architecture full mush .

SONATRACH dispose de 8 sites dans le sud de pays ,Chacun de ces sites est relié au deux principaux sites Hassi R'mel et Hassi Messaoud par des liens 2 x E1 ,et chaque deux routeurs adjacents a coté sont reliés par des liens 1 x E1 .

Le schéma ci-dessous représente l'architecture actuelle de ce réseau :

III-2-4.Le protocole utilisé:

Le réseau actuel de SONATRACH est basé sur le protocole du routage dynamique OSPF .

Pour bien comprendre comment les informations sont transmises et échangés au niveau des sites de SONATRACH voici une description de ce protocole .

III-2-4-1.Présentation :

OSPF Open Shortest Path First est un **protocole de routage** interne IP de **type a état de lien**, il a été développé au sein de l'internet Engineering Task Force , est caractérisé par :

Il utilise IP multicast pour envoyer ses mises à jour d'état de lien : Cette méthode prend moins de ressources aux routeurs qui n'écoutent pas de paquets . Aussi, ces mises à jour sont envoyées uniquement lors d''un changement de topologie. On économise de manière évidente la bande passante. Les mises à jour sont seulement incrémentielles.

Le choix du meilleur chemin est basé sur le coût (la bande passante inversée) : Cette métrique peut être définie manuellement sur les interfaces.

permet une définition logique des réseaux : où les routeurs peuvent être répartis en zones (*area)*. Cela évitera une explosion de mises à jour d'états de lien sur l'ensemble du réseau.

Il n'y a pas de limite du nombre de sauts : étant un protocole de routage à état de lien, chaque routeur possède une connaissance complète des réseaux au sein d''une zone (*area*). Aussi, le danger de boucles de routage n'étant *a priori* plus présent, la limite du nombre de sauts n'est plus nécessaire.

Il permet l'authentification de routage : par l''utilisation de différentes méthodes d''identification avec mots de passe [71].

III-2-4-2.Fonctionnement :

Cette section traite du fonctionnement d'OSPF au sein d'une seule zone et de la manière dont la topologie table ou la link-state data base est construite. La table de routage est constituée à partir de cette base de donnée. Ce résultat est obtenu grâce à l''application de l''algorithme de routage SPF. En voici les différentes étapes :

1. D'abord, un routeur doit trouver ses voisins. Pour ce faire, il utilise des paquets Hello. Dès son initialisation ou à la suite d'un changement de routage, un routeur va générer un *link-state advertisement* (LSA). Cette annonce va représenter la collection de tous les états de liens de voisinage du routeur.
2. Tous les routeurs vont s''échanger ces états de liens par inondation. Chaque routeur qui reçoit des mises à jour d''état de lien (*link-state update*) en gardera une copie dans sa *link-state database* et propagera la mise à jour auprès des autres routeurs.
3. Après que la base de données de chaque routeur soit complétée, le routeur va calculer l''arbre du chemin le plus court (*Shortest Path Tree*) vers toutes les destinations avec l''algorithme Dijkstra. Il construira alors la table de routage (*routing table*), appelée aussi *forwarding database,* en choisissant les meilleures routes.
4. S'il n'y a pas de modification topologique, OSPF sera très discret. Par contre en cas de changement, il y aura échange d'informations par des paquets d'état de lien et l'algorithme Dijkstra recalculera les chemins les plus courts.[1]

III-2-4-3.Les fonctionnalités d'OSPF au réseau SH :

La hiérarchie d'OSPF : Une caractéristique principale d''OSPF est de supporter des inter-réseaux très larges. Elle est possible grâce au regroupement des routeurs dans des entités logiques appelées area ou zone.[71]

- En raison du nombre limité de nœuds et des parcours(routes) dans le reseau SH, une seule zone(area) est préférée pour le réseau; le réseau sera la zone 0 (area 0)

L'ID d'un routeur 'identificateur': Chaque routeur intérieur d'un réseau exécutant l'OSPF doit disposer d'un ID de routeur unique qui va lui identifié .

Pour attribuer l'ID de routeur par défaut ,l'OSPF utilise la plus grande adresse IP de l'un des interfaces actifs du routeur.si l'interface loopback est configuré avec une adresse IP le logiciel Cisco IOS software va utiliser cette adresse comme ID du routeur ,même si d'autre s interfaces ont des adresses IP grandes .

- Le tableau suivant présente les id-router pour les 4 sites du cœurs réseau .

Le N° du site	Le nom du site	router-id
01	ALG	1.1.1.1
02	HRM	2.2.2.2
03	HMD	3.3.3.3
04	RSD	4.4.4.4

Tableau III.3 : liste des router-id

La bande passante : La métrique OSPF par défaut est la bande passante. Chaque liaison reçoit une valeur de métrique basée sur sa bande passante. La métrique d'un lien est l'inverse de la bande passante du lien.

- afin d'éviter d'avoir calculer la bande passante de référence pour chaque lien, on peut utiliser la plus grande vitesse de lien dans le réseau au niveau du SH la haute vitesse est égale a 100Mbps ou 1Gbps, donc il est conseillé d'utiliser une largeur de bande passante de 10 gigabit qui est de 10000 [72] .

Le DR et le BDR : Dans les réseaux gérés par OSPF, l'un des routeurs connectés sur le réseau doit être élu routeur désigné (DR pour Designated Router) et un autre doit être élu routeur désigné de secours (BDR pour Backup Designated Router). Ces élections de routeurs permettent ainsi de réduire le trafic de mise à jour de routage

En effet, le DR et le BDR agissent comme un point central de contact pour les échanges d'informations d'état de lien. Plutôt que les routeurs échangent leurs informations d'état de

lien avec tous les autre routeurs, chaque routeur doit établir une communication avec le DR et le BDR. Ces derniers utilisent ensuite un processus d'inondation pour renvoyer ces informations à tous les autres routeurs [72] .

- Pour les 4 sites qui présentent les sites principaux(ALG, HRM ,HMD,RSD), chacun de ces sites contient a l'intérieur 2 routeurs de type C7200 un joue le rôle d'DR et l'autre le rôle d'un BDR .

III-2-5.Les technologies de sécurité existantes:

La politique de sécurité déployée au sein de l'entreprise SH, définit un certain nombre de règles, de procédures et de bonnes pratiques, permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation. Cette politique prend en compte les deux aspects de la sécurité suivants :

III-2-5-1.La sécurité physique:

elle concerne l'installation informatique, pour répondre a ce type de sécurité l'entreprise SONATRACH consacre deux salles du bâtiments pour héberger les équipements du réseau, ces salles regroupe les armoires de protection utilisées pour les routeurs, les Switchs de distribution, les pare-feu, les serveurs et le PABX, pour plus de protection l'entreprise maintien les mesures de sécurité suivantes :

- **L'accès au équipements** : l'accès à ces lieu est strictement sévère, seul les installateurs, les agents de maintenance, les administrateurs et les agents de sécurité qui ont le droit d'entrer au salle, en utilisant des cartes magnétique spéciale pour pouvoir ouvrir le ports .

- **Equipement d'alimentation** : l'alimentation des systèmes est composée de deux entrées électriques, la première est celle de l'onduleur (220v), la deuxième est un ensemble de batteries reliées en série qui se met en marche en cas de coupure d'alimentation de l'onduleur .

- **La ventilation du systèmes** : la salle est équipée par des systèmes de climatisation pour maintenir une température ambiante de plus chaque armoire est dotée d'un processus de ventilation qui se situe a l'arrière pour faire circuler l'air a l'intérieur .

III-2-5-2.La sécurité logique:

elle concerne l'accès aux données de l'entreprise et sert a protéger le réseau contre les attaques, les intrusions, les virus et tout type de menace.

- **ASA5520:** l'équipement ASA est installé dans l'infrastructure de SH il est utilisé pour fournir ces fonctionnalités de gestion de risques, tel que l'antivirus, anti-spam, système de prévention d'intrusion et filtrage de contenu web. le firewall est configuré selon une politique, cette dernière nécessite que chaque interface dans le ASA appartient à un sous réseau différent et que ces interfaces sont nommés et configurés "en attribuant un niveau de sécurité" ,le tableau suivant montre la façon dont les noms sont attribuer aux interfaces ainsi le niveau de sécurité utilisé sur chaque interface .

Interface physique	Nom	Degré de sécurité	Description de l'interface
Giga0/0	Inside	100	Connexion avec le LAN
Giga0/1	WAN	90	Connexion avec le site distant
Giga0/2	DMZ	80	Connexion avec la zone des serveurs
Giga0/3	Outside	0	Connexion Internet

Tableau III.4 : politique de sécurité de l'ASA5520 dans SH

L'ASSA 5520 est un dispositif de sécurité de la gamme CISCO 5500 qu'il a une plateforme modulaire capable de fournir des services de sécurité, l'ensemble de réseau dans le siège Amont compte sur cet équipement, pour satisfaire leur besoin en terme de sécurité. Cet équipement opère en mode firewall et aide a la protection de réseau, contre les intrusions et les attaques, il est installé au cœur du réseau, ce qui fait toute la circulation entre réseau passe a travers le mur pare-feu qui exécute une politique dépond de l'organisation. l'équipement Cisco présent un dispositif de sécurité tout d'en un qui peut fonctionner comme suite :

- Une appareil de sécurité qui peut masquer l'adresse du réseau interne pour accéder en externe en utilisant un espace d'adressage différent, cette technique est communément connu sous le nom dde traduction NAT "Network Address Translation".

- supporter la technique PAT (Port Address Translation) [AN23] qui est la traduction des ports ,elle est effectuée pour associé une adresse d'application globale à une application d'un hôte interne qui entame un dialogue avec extérieur .
- spécifier des règles identifiant le trafic qui permet à traverser les différentes interfaces ,cette application de sécurité utilise les ACL (Access Control List)[AN24]. ACL sera configuré pour éliminer le trafic non connu ou non désirable .

pour faciliter l'administration, des ACL sont appliqués et des degrés sécurité sont attribuer aux interfaces, le schéma suivant décrit cette politique qui est met en place sur l'ASA 5520 de siège Amont .

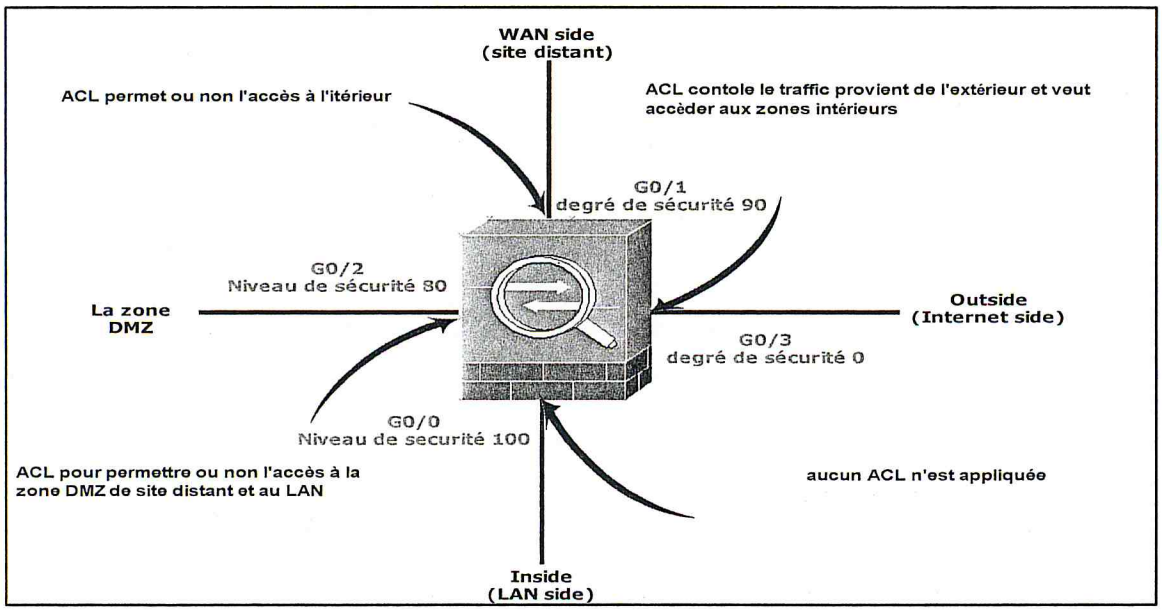


Figure III.3 : politique déployée sur l'équipement ASA

- ACS (Access Control Serve) : est un serveur Cisco qui est installé dans le réseau de SH pour gérer l'authentification, l'autorisation et la comptabilité (AAA "Authentication, Authorization, Accounting") sur les sur les équipements de l'entreprise. Ces fonctions sont implémenter dans le serveur Cisco et sont basées sur le protocole d'authentification RADIUS (Remote Authentification Dial-In User Service), la certification assurée par le serveur identifie les utilisateurs avant qu'ils soient autorisés d'accéder au réseau et au service de réseau.

- Deux types de **PROXY** pour la connexion internet :
  - **Blue Goat SG Proxy Edition(Secure Web Gateway)** :est une appareil opére de la m éme manière qu'un serveur proxy pour sécuriser les communications WEB et d'accélérer la livraison des applications de l'entreprise, SH utilise cette appareil comme boitier de sécurité complémentaire aux firewall existants..
  - **Blue Coat Proxy AV(Antiverus Web) :** permet aux SH de détecter les virus, les vers et les chevaux de Troie qui peuvent pénétrer dans leur système à travers des failles web, comme par exemple des comptes personnels de courrier électronique , des contenus web ou des messages non sollicités (spam), des fichiers téléchargés par des navigateurs Web .

Le **Blue Coat ProxyAV** combiné au **Blue Coat ProxySG** garantit une détection évolutive, ainsi qu'une visibilité et un contrôle complets des communications web de l'entreprise.

- **DMZ(De-Militarized Zone)** :une zone démilitarisée est mise en ouvre derrière le ASA, cette zone regroupe un ensemble de serveur qui peuvent être accessible par l'extérieur, elle sert d'éviter les connexions direct au réseau interne.
- Concernant **le filtrage web** Sonatrach utilise des logiciels Websense Security, cette dernière permet aux administrateurs système de bloquer l'accès aux sites Web comme (Youtube, Facebook) afin de décourager les employés de passer leur temps de naviguer sur des sites Web non liés aux leur travaux.

III-3-Les besoins de SONATRACH :

L'organisation logique actuelle du WAN permet de couvrir la quasi totalité des besoins en échange d'information entre les structures de l'activité amont, cette architecture logique dont le plan d'adressage épouse la répartition des unités opérationnelles au sud et fonctionnelles au nord du pays, doit être réaménagée pour prendre en charge un plus grand nombre de sites et de services. La généralisation de ce réseau étendu à l'ensemble des structures et activités de l'entreprise impose une reconsidération des objectifs et des résultats attendus. En effet, cette montée en charge du nombre de sites connectés avec la diversités des services acheminés conduit à un choix d'une technologie hautement performante induisant le moins de tâches administratives possible .

Le réseau SH se base sur le protocole de routage OSPF, l'algorithme utilisé par ce protocole pour calculer ses routes est extrêmement gourmand en ressources processeurs. les routes ne sont calculées qu'en fonction de l'adresse de destination, et non de la qualité de service souhaité, et d'autre part à chaque saut le routeur doit rechercher la meilleure solution possible pour acheminer le trafic, d'autant plus que les tables de routages ont une déplaisante tendance à voir leur taille augmenter ces derniers temps. Il est devenu alors intéressant de trouver une technologie pouvant associer la puissance de la commutation de la couche 2 avec la flexibilité du routage de la couche 3.

Les applications déployées à SONATRACH sont de plus en plus gourmandes en ressources, comme par exemple en bande passante avec la vidéo conférence pour éviter le déplacement des employés et permettre le gain du temps ou pour le transfert de fichiers volumineux. Combiné à l'extension de certaines technologies, comme la VoIP nécessitant d'avoir un faible délai, tant dis que le réseau actuel de SONATRACH est incapables de supporter ce genre de trafic sans mécanisme de QoS. Certes un surdimensionnement du réseau est beaucoup plus simple à mettre en place mais dans la plupart des cas coûteux, c'est donc pour cette raison que la QoS devient indispensable.

Concernant l'aspect sécurité Sonatrach veut étendre son WAN à moindre coût et en toute sécurité vers des entités non desservies , telles que des filiales internationales, des

succursaleset des partenaires commerciaux par le biais d'un accès Internet tiers plutôt que par le biais de liaisons WAN dédiées coûteuses ou de liaisons d'accès longue distance.

III-4-Les objectifs :

Pour répondre aux besoins cités précédemment on va faire un travail dont l'objectif est :

- **Extensibilité :** possibilité d'ajout des sites sans impact sur l'infrastructure existante.
- Assurer **la flexibilité** dans la transmission des données .
- Améliorer/augmenter **la bande passante** .
- Apporter l'intelligence du routage avec les performances de la commutation .
- Accélérer la transmissions des données au sein du backbone IP .
- Simplifier le protocole pour permettre aux routeurs de fonctionner plus rapidement et réduire la taille des tables de routage .
- Améliorer le rapport performance/prix des équipements de routage .
- **Implimentation du Traffic Engineering**: qui permet d'optimiser l'utilisation des ressources d'un réseau afin d'éviter la congestion. C'est la prise en compte de la bande passante disponible sur un lien lors des décisions de routage qui rende possible cette optimisation.
- Permettre la gestion de la qualité de service en gérant les priorités en fonction de la nature des flux (flux voix et vidéos prioritaires par rapport aux flux transactionnels eux-mêmes prioritaires par rapport aux flux de transfert de messages et de fichiers).
- **Garantir la sécurité** :on utilisant le VPN(Virtual Protocol Network) site-à-site qui qui consiste à mettre en place une liaison permanente, distante et sécurisée entre deux ou plusieurs sites de SONATRACH, le trafic qui passe entre 2 sites sera sécuriser et ne permet a personnes a écouter le trafic ou bien a crypter le message

Deuxième partie : Implémentation des solutions qui mènent a répondre au besoin du SH

III-1-Déploiement de la solution:

Une fois une étude sur le réseau actuel du SH est faite et une spécification des besoins a été élaborée , il est primordial de définir une nouvelle architecture permettant d'atteindre notre objectifs .

III-1-1.Choix du matériels:

III-1-1-1.Les équipements : Nous avons choisis la même marque des équipements ce qui évite tous problèmes de compatibilité entre les protocoles propriétaires. Et même plus il nous permet d'exploiter pleinement les protocoles développés par le constructeur. Nous avons donc choisi de prendre du matériel Cisco puisque ce sont des équipements fiables qui ont fait leur preuve, ainsi que l'on connaît très bien. Pour la nouvelle topologie nous utiliserons ls routeurs Cisco 7200XR .

III-1-1-2.Le câblage :

- Câbles droits et croisés Ethernet :pour les connections entre équipements du réseau .
- Câbles séries DCE/DTE :pour des connections entre routeurs .
- câbles console :pour les connections entre terminaux et routeurs .

Après avoir décrire dans le chapitre 2 les différents protocoles en vigueur aujourd'hui qui permettent de garantir la qualité de service et la sécurité VPN et a l'aide de l'état de l'art présenté dans le chapitre précédant, nous aboutirons a choisir un protocole parmi tout ces protocoles qui permet de répondre aux besoins citer précédemment .

III-1-2.Choix du protocole:

Les partisans du « tout commuté » exposent que si on veut un réseau très rapide il faut que les paquets passent un minimum de temps dans chaque composant du reseau.par conséquent, il faut que les éléments du réseau fassent le minimum de traitements sur les paquets. Dans cette approche, l'idéal est que les routeurs de bordures soient « intelligents »et fixent certains paramètres qui seront valables sur tout le reste du réseau et que les routeurs du cœur de réseau

ne fasse que commuter les paquets qui ont de taille variable ne faut surtout pas de file d'attente qui ralentisse le transit des paquets .

un exemple caractéristique de cette approche est le protocole MPLS. En effet dés l'arrivé d'un paquet IP en bordure d'un réseau MPLS ,on ajoute au paquet IP une étiquette sera lue afin d'effectuer la commutation des paquets(de taille variable qui est l'intérêt de cette technologie) a la vitesse maximale. A la sortie du réseau MPLS, l'étiquette du paquet est retirée, le paquet est alors routé sur IP de manière classique .Le MPLS offre une meilleur rapidité de commutation des paquets, en effet la décision de routage se fait en analysant le label. Ainsi chaque routeur possède une table associant un port/label d'entrée à un port/label de sortie. Cette table est rapide à parcourir, ce qui a pour but d'accroître la rapidité de routage par rapport à un réseau IP.

Le MPLS offre aux opérateurs 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. Le fonctionnement des labels facilite considérablement la reprise du routage après des défaillances du réseau. Ceci garantit une pérennité des accès aux données. La labellisation des paquets : « le chemin le plus court n'est pas toujours le meilleur », avec le MPLS, une politique peut être établie afin que les paquets suivent un chemin défini. Ainsi, il est possible d'alléger les liaisons, favorisant le confort et évitant la congestion des liens .

L'ingénierie de trafic a été effectuée au début soit par IP ou par ATM, mais il a atteint la popularité dans le contexte de MPLS TE aujourd'hui . Le principal avantage de la mise en œuvre MPLS TE est qu'il offre une combinaison de capacités TE(traffic engineering) de l'ATM avec la classe de service (CoS).

Le MPLS sert ainsi à la gestion de la qualité de service c'est-à-dire d'autoriser de nouvelles routes à certains paquets IP par rapport à la route par défaut c'est-à-dire appliquer des règles de priorité selon le besoin et selon le besoin et l'importance d'un trafic par rapport à d'autres.

Les VPN en environnement MPLS permettent d'obtenir une liaison sécurisée à moindre coût et de réduire la complexité d'un grand réseau et le cout en bande passante WAN tout en augmentant les vitesses de connectivité, grâce à une technologie de connectivité Internet à haute bande passante telle que DSL, Donc il sera possible d'utiliser des adresses privées dans un réseau public .

A la fin nous concluons que le MPLS la meilleure solution qui répond aux exigences du Sonatrach .

III-1-3.Choix de la topologie:

Notre travail consiste à améliorer l'interconnexion des sites de SONATRACH on appliquant le protocole MPLS et pour bien bénéficier des avantages du MPLS nous avons mis quelques modifications dans l'architecture actuelle du réseau SH et nous allons nous focaliser sur huit sites : le siège amont, le site de Rue du Sahara(RSD) site de HassiR'mel(HRM), site de Hassi Messaoud (HMD) ainsi le site de RNS(Rourd Nouss) et les 3 sites de sud TFT et HBK(Haoud BerKaoui) et INA(IN Amenas) la figure suivante nous démontre l'emplacement de chaque site :

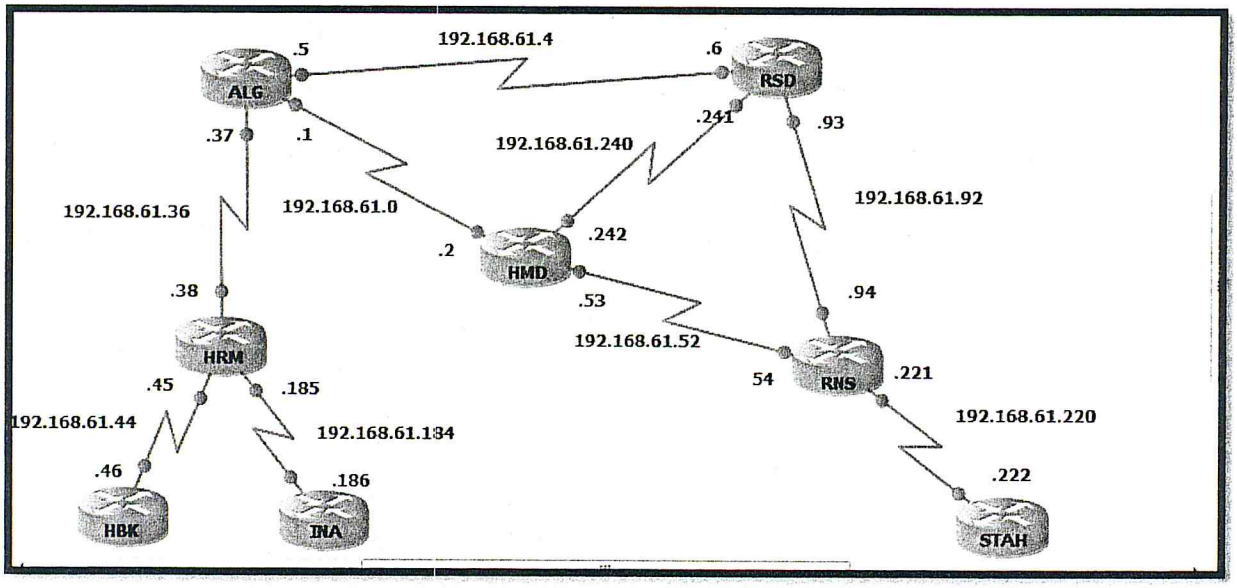


Figure III.4 :La nouvelle topologie du 8 sites du réseau SH

Après avoir étudié tous les avantages qu'offre MPLS dans les réseaux cœurs, le matériels a utiliser ainsi la nouvelle architecture du réseau WAN-SH nous passons maintenant a

implémenter le protocole MPLS au sein du réseau WAN qui relie les différents sites de SH pour l'amélioration de la gestion des données de différentes activités de Sonatrach.

III-2-Implémentation du protocole MPLS :

SH est en mesure de tester une approche de développement international à faible risque Le réseau MPLS fournit un accès fiable dans les réseaux WANs (Wide Area Networks), et cela, avec un faible investissement financier initial et un déploiement rapide, comme nous avons déjà cité auparavant SH a son propre réseaux de fibre optique. Ce qui fait de cette solution une solution idéale qui propose un accès direct à ses différents sites basés au quatre coin de l'Algérie (nord, est, sud, ouest).

III-2-1.Choix du routeurs LSR et LER:

Pour mettre en œuvre quelques fonctionnalités liées au protocole MPLS, il convient de créer des réseaux assez grands. Il faut avoir des routeurs frontières (edge LSR= LER) qui constituent le tour du nuage MPLS et des routeurs internes ayant toutes leurs interfaces réseau dans le nuage MPLS. Et des routeurs de cœurs dit des LSR .

Nous avons désigné les routeurs LER, et les routeurs LSR au niveau du réseau WAN-SH :

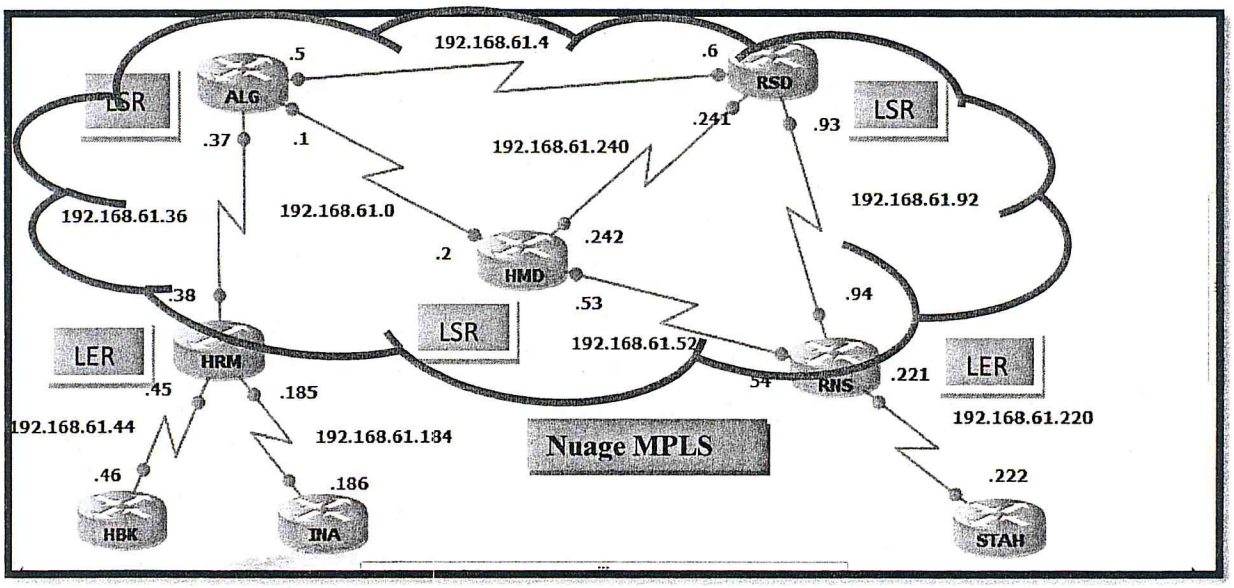


Figure III.5 :Les routeurs LSR et LER dans le réseau SH

Donc notre réseau MPLS contient trois routeurs LSR, et deux routeurs LER, au sud, comme présenté dans la figure ci-dessus. Le MPLS sera configurer dans tous les interfaces des routeurs du réseau cœur (les LSR), et dans les interfaces d'entré aux backbone MPLS dans les routeurs LER.

III-2-2.Activation du MPLS :

La mise en œuvre du protocole MPLS sur les routeurs Cisco est très simple. La création des tables de forwarding est faite dynamiquement grâce au protocole de distribution de label (LDP).

- Pour pouvoir utiliser MPLS sur les routeurs Cisco, il faut d'abord activer le Cisco Express Forwarding (CEF).
- Ensuite sélectionner le protocole utilisé pour la distribution des labels. Par défaut, c'est le protocole propriétaire Cisco TDP (Tag Distribution Protocol) qui est utilisé. Pour notre réseau, nous utilisons LDP (Label Distribution Protocole).
- Les interfaces doivent encapsuler les paquets avant de les envoyer sur le réseau MPLS. Pour cela, il faut ajoutée dans la configuration de chaque interface l'activation du MPLS. Cette configuration n'est pas utilisée pour les interfaces des LER connectées aux ordinateurs, car ces machines utilisent des paquets IP standards.

Jusqu'a présent, le protocole MPLS est activé. L'encapsulation a l'entrée du nuage MPLS est effective. La commutation de label fonctionne sur les routeurs internes a MPLS. La dé-encapsulation en sortie du nuage MPLS est effectuée pour restituer a l'identique le paquet afin que l'action MPLS soit transparente.

III-3-Les applications du MPLS :

Apres avoir implémenté le MPLS dans le réseau de SONATRACH, et pour améliorer encore plus la performance du réseau, nous passons a mis en ouvre ses différentes applications.

III-3-1.Implémentation du Trafic Engineering :

MPLS-TE permet l'établissement de LSP-TE (Label Switched Path – Traffic Engineering), routés explicitement ou dynamiquement, en fonction de contraintes relative à une topologie TE. Ces LSP-TE peuvent être assimilés à des connexions point-à-point, un mode « circuit » est alors créé dans les réseaux IP/MPLS, s'appuyant sur le routage interne, mais fonctionnant en parallèle.

La première étape dans la réalisation d'une architecture MPLS-TE est de créer une topologie TE. Cela consiste à déclarer pour toutes les interfaces du réseau ces 2 paramètres :

Bande passante physique du lien et Bande passante réservable par le TE avec le protocole RSVP .

III-3-1-1Etablissement d'un tunnel TE à chemin explicite :

Le chemin explicite est une succession d'adresses de liens ou de nœuds que le LSP-TE doit emprunter ou exclure. Il peut s'agir d'un chemin explicite complet, ou d'un chemin explicite partiel, indiquant une suite non continue de liens et/ou de nœuds à emprunter.

tunnel explicite numéro 1: qui est réalisé entre le routeur d'Alger et le Routeur RNS, passant par les routeurs ALG->HMD->RNS ; avec une priorité de P(1,1), et une bonde passante de 800Kbps, le tunnel est représenté dans la figure suivante :

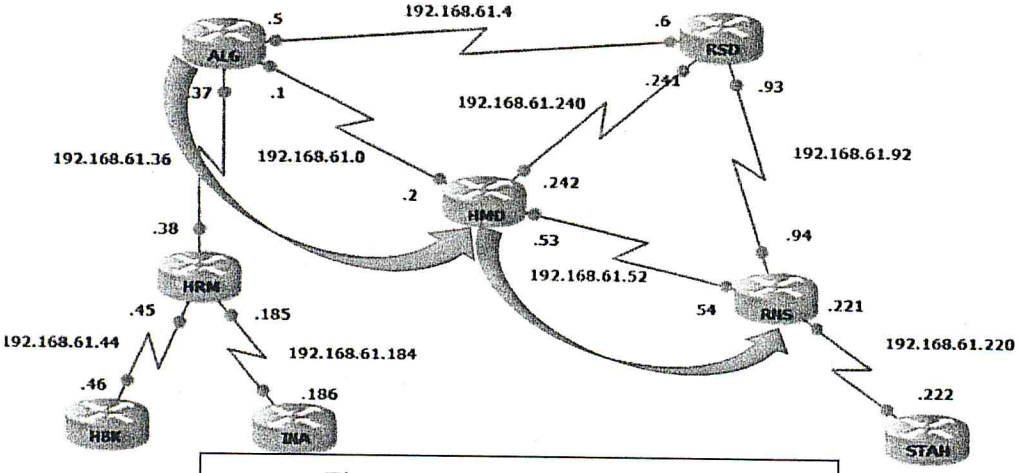


Figure III.6 :le tunnel explicite

Nous créons tout d'abord le détail du chemin explicite. C'est une liste ordonnée des routeurs à inclure, ou à exclure . Ensuite on configure :

- L'adresse de Loopback du routeur cible de sortie du tunnel .
- La priorité d'établissement et de maintien du tunnel .
- la bande passante TE requise pour l'établissement du tunnel .
- le chemin explicite associé au tunnel.
- annonce le tunnel dans la table de routage IGP du routeur de tête du tunnel .

```
!
interface Loopback0
 ip address 10.250.1.130 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 10.250.5.130
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 500
 tunnel mpls traffic-eng path-option 1 explicit name TUN1
 tunnel mpls traffic-eng fast-reroute
 no routing dynamic
```

Figure III.7 :Implémenter un tunnel explicite

III-3-1-2.Etablissement d'un tunnel TE à chemin dynamique:

Lorsque le chemin est explicite partiel ou qu'il n'est pas spécifié, on parle de chemin dynamique. Le chemin dynamique est alors calculé, soit par le routeur de tête soit par un serveur central, à l'aide d'un algorithme de calcul de chemin contraint (Constraint Shortest Path First, CSPF). Le calcul des chemins dynamique par les routeurs de tête pose toutefois un problème d'optimisation de l'usage de la topologie TE. En effet, chaque routeur de tête ne connait l'état que de ses propres LSP-TE.

Tunnel dynamique numéro 2 : le tunnel 2, aussi réalisé entre le routeur d'Alger et le routeur RNS, avec une priorité P(2,2),et la bande passante égale à 500KBps .

La création de chemin dynamique est presque pareille a c'elle du chemin explicite sauf que le chemin dynamique utilise l'algorithme CSPF pour s'établir

```
!
interface Tunnel2
 ip unnumbered Loopback0
 tunnel destination 10.250.5.130
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 300
 tunnel mpls traffic-eng path-option 1 dynamic
 no routing dynamic
```

Figure III.8 :Implémenter un tunnel dynamique

III-3-1-3. Protection des tunnels MPLS-TE :

Pour pallier les éventuelles défaillances d'un LSP-TE, il est possible de paramétrer pour chaque LSP-TE des chemins de secours explicites. Ces chemins de secours peuvent prendre la forme d'un LSP-TE global préétabli dans la topologie TE, ou de LSP-TE de protection locale de lien ou de nœud (Fast Reroute). Si aucun LSP-TE de secours n'est configuré, le trafic suivra le chemin de l'IGP.

- **Un tunnel de protection global :**

nous allons crée un autre chemin qui sert a protégé le tunnel 1 ce tunnel devra être explicite est passera par les nœuds ALG->RSD->RNS . avec une priorité (7,7) .

Sur le routeur de tête du tunnel MPLS-TE à protéger, il faut d'abord configurer un chemin explicite pour le tunnel de protection .

Il est possible de déclarer jusqu'à 8 tunnels de protection globale, identifiés par niveau de priorité.

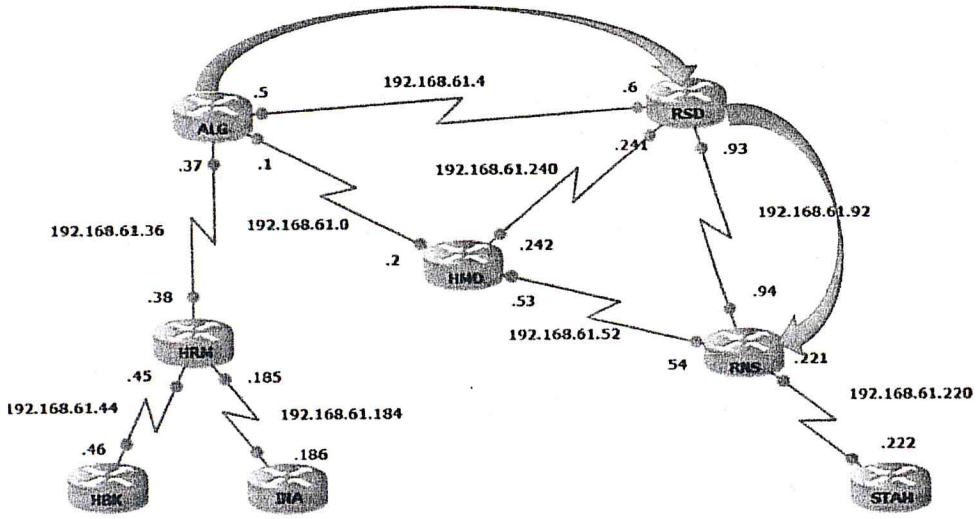


Figure III.9 :le tunnel de protection globale

- **Un tunnel de protection local :**

Le mode de protection « Fast Reroute » permet d'améliorer les lacunes des modes précédents en termes de temps de convergence.

La protection locale d'un lien ou d'un nœud s'effectue sur le nœud en amont, où est créé un tunnel de protection locale unidirectionnel FRR de type « Next HOP » .

Dans notre configuration un seul type de tunnels de Fast-Reroute sera testé :

Un tunnel NHOP qui protège le tunnel principal d'une défaillance du lien entre HMD et RNS .Ce tunnel est unidirectionnel, ils ne protège le tunnel principal que dans le sens ALG->RNS.et il va passé par ALG->HMD->RSD->RNS .

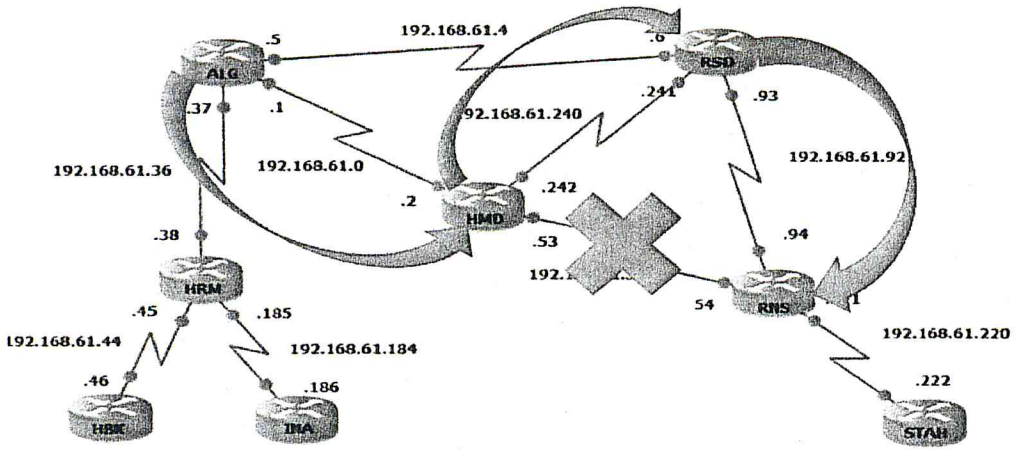


Figure III.10 :La protection locale

III-3-2.Implémentation de la QOS :

Pour implémenter de la qualité de service dans le réseau WAN de SONATRACH nous devons suivre les étapes suivantes :

Après avoir présenté un Etat de l'art de la Qualité de service dans les réseaux MPLS, nous avons décidé d'orienter notre mise en œuvre sur Diffserv, car cette solution est la plus utilisée et semblait donc la plus intéressante pour la réalisation de la QOS.

L'objectif de notre démarche fut de réaliser un système dans lequel un client (sur un réseau IP) pourrait classifier ces flux (par exemple 0 pour les flux normaux jusqu'à 7 pour les flux les plus importants) avant de les envoyer à son fournisseur (sur un réseau MPLS). Le fournisseur pourrait ensuite récupérer ces flux « classés » et leur attribuer une qualité de service correspondant au besoin du client (en priorisant les flux, attribuant de la bande passante, ou même en faisant transiter certains flux dans un tunnel).

Nous avons configuré le DiffServ en mode uniforme ,DiffServ dans ce modele a un tunnel a une seule couche de la QoS, qui atteint de bout en bout. Le routeur PE d'entrée copie le DSCP du paquet IP entrant dans les bits d'EXP MPLS des étiquettes imposées. Comme les bits EXP voyage à travers le noyau, ils peuvent ou ne peuvent pas être modifiées par les

routeurs intermédiaires P. Dans cet exemple, les routeurs du nuage MPLS modifie le champ EXP . Au P route sortie (P2) nous copions les bits d'EXP aux bits d'EXP de l'étiquette nouvellement exposée après le PHP (Penultimate-Hop-Pop). Enfin au PE routeur de sortie (PE2), nous avons ensuite copier les bits d'EXP aux bits DSCP du paquet IP nouvellement exposée.

Voici la configuration au niveau de routeur HRM c'esl le routeur PE1 d'entrée :

```
class-map match-all IP-AF11
  match ip precedence 0
class-map match-all IP-AF12
  match ip precedence 1
class-map match-all IP-AF21
  match ip precedence 2
class-map match-all IP-AF22
  match ip precedence 3
class-map match-all IP-AF31
  match ip precedence 4
class-map match-all IP-AF32
  match ip precedence 5

class-map match-all MPLS-AF11
  match mpls experimental topmost 0
class-map match-all MPLS-AF12
  match mpls experimental topmost 1
class-map match-all MPLS-AF21
  match mpls experimental topmost 2
class-map match-all MPLS-AF22
  match mpls experimental topmost 3
class-map match-all MPLS-AF31
  match mpls experimental topmost 4
class-map match-all MPLS-AF32
  match mpls experimental topmost 5

policy-map set-MPLS-PHB
  class IP-AF11
   police 8000 conform-action set-mpls-exp-imposition-transmit
                                        0 exceed-action drop
  class IP-AF12
   police 10000 conform-action set-mpls-exp-imposition-transmit
             1 exceed-action set-mpls-exp-imposition-transmit 0
  class IP-AF21
   police 12000 conform-action set-mpls-exp-imposition-transmit
             2 exceed-action set-mpls-exp-imposition-transmit 1
  class IP-AF22
   police 12000 conform-action set-mpls-exp-imposition-transmit
             3 exceed-action set-mpls-exp-imposition-transmit 2
  class IP-AF31
   police 12000 conform-action set-mpls-exp-imposition-transmit
             4 exceed-action set-mpls-exp-imposition-transmit 3
  class IP-AF32
   police 12000 conform-action set-mpls-exp-imposition-transmit
             5 exceed-action set-mpls-exp-imposition-transmit 4
```

```
policy-map output-qos
  class MPLS-AF11
   bandwidth percent 5
   random-detect
  class MPLS-AF12
   bandwidth percent 10
   random-detect
  class MPLS-AF21
   bandwidth percent 10
   random-detect
  class MPLS-AF22
   bandwidth percent 15
   random-detect
  class MPLS-AF31
   bandwidth percent 20
   random-detect
  class MPLS-AF32
   bandwidth percent 30
   random-detect

interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0
 max-reserved-bandwidth 90
 service-policy output output-qos
 tag-switching ip
!
interface Ethernet1/0
 ip vrf forwarding v1
 ip address 10.0.0.2 255.255.255.0
 service-policy input set-MPLS-PHB
!
```

Figure III.11 :Configuration de la QOS au niveau du PE d'entrée

sur les routeurs PE, les paquets sont reçus avec différentes valeurs de précédence IP des routeurs CE annexées. Par conséquent, les routeurs PE peuvent mapper ou attribuer classe basée sur l'infiltration paquet IP priorité. Une class-map est configurée sur les routeurs PE pour sélectionner les paquets basés sur IP précédence 0,1,2,3,4,5, et une policy-map est configuré pour une QoS *mesures* de fixer les bits d'EXP MPLS cartographie à la pénétration IP priorité.

La configuration du routeur P le routeur ALG :

```
class-map match-tout MPLS-en
  correspondre MPLS expérimental 3 le plus haut
!
policy-map MPLS-en
  classe MPLS-en
   ensemble MPLS expérimental le plus élevé 2
!
Ethernet0 interface / 0
 adresse IP 192.168.1.1 255.255.255.0
 ip-tag commutation
!
Interface Ethernet1 / 0
 adresse IP 192.168.0.2 255.255.255.0
 entrée de service politique MPLS-en
 ip-tag commutation
!
```

La configuration du routeur P le routeur HMD :

```
class-map match-tout MPLS-AF11
  correspondre MPLS expérimental 0 supérieure
class-map match-tout MPLS-AF12
  correspondre MPLS expérimental le plus élevé 1
class-map match-tout MPLS-AF21
  correspondre MPLS expérimental le plus élevé 2
class-map match-tout MPLS-AF22
  correspondre MPLS expérimental 3 le plus haut
class-map match-tout MPLS-AF31
  correspondre MPLS expérimental 4 le plus haut
class-map match-tout MPLS-AF32
  correspondre MPLS expérimental le plus élevé 5
!
class-map match-tout QoS-groupe-AF11
  correspondre QoS-groupe 0
class-map match-tout QoS-groupe-AF12
  correspondre QoS-groupe 1
class-map match-tout QoS-groupe-AF21
  correspondre QoS-groupe 2
class-map match-tout QoS-groupe-AF22
  correspondre QoS-groupe 3
class-map match-tout QoS-groupe-AF31
  correspondre QoS-groupe 4
class-map match-tout QoS-groupe-AF32
  correspondre QoS-groupe 5
!
policy-map QoS-groupe en
  classe MPLS-AF11
   mettre QoS-groupe MPLS expérimental le plus haut
  classe MPLS-AF12
   mettre QoS-groupe MPLS expérimental le plus haut
  classe MPLS-AF21
   mettre QoS-groupe MPLS expérimental le plus haut
  classe MPLS-AF22
   mettre QoS-groupe MPLS expérimental le plus haut
  classe MPLS-AF31
   mettre QoS-groupe MPLS expérimental le plus haut
  classe MPLS-AF32
   mettre QoS-groupe MPLS expérimental le plus haut
!
policy-map QoS-groupe-out
  classe de QS-groupe-AF11
   pour cent de la bande passante 5
   -détecter aléatoire
   mettre MPLS expérimentale la plus haute qualité de service-groupe
  classe de QS-groupe-AF12
   pour cent de la largeur de bande 10
   -détecter aléatoire
   mettre MPLS expérimentale la plus haute qualité de service-groupe
  classe de QS-groupe-AF21
   pour cent de la largeur de bande 10
   -détecter aléatoire
   mettre MPLS expérimentale la plus haute qualité de service-groupe
  classe de QS-groupe-AF22
   pour cent de la largeur de bande 15
   -détecter aléatoire
   mettre MPLS expérimentale la plus haute qualité de service-groupe
  classe de QS-groupe-AF31
   pour cent de la largeur de bande 20
   -détecter aléatoire
   mettre MPLS expérimentale la plus haute qualité de service-groupe
  classe de QS-groupe-AF32
   pour cent de la largeur de bande 30
   -détecter aléatoire
   mettre MPLS expérimentale la plus haute qualité de service-groupe
!
```


Figure III.13 :La QOS au niveau du P2

Nous passons maintenant a mettre en place le VPN sur MPLS .

III-3-3.Implémenter la sécurité via VPN :

Une terminologie particulière est employée pour désigner les routeurs (en fonction de leur rôle) dans l'environnement VPN/ MPLS :

- P (Provider) : ces routeurs, composant le cœur du backbone MPLS, n'ont aucune connaissance de la notion de VPN. Ils se contentent d'acheminer les données grâce à la commutation de labels ;
- PE (Provider Edge) : ces routeurs sont situés à la frontière du backbone MPLS et ont par définition une ou plusieurs interfaces reliées à des routeurs clients ;
- CE (Customer Edge) : ces routeurs appartiennent au client et n'ont aucune connaissance des VPN ou même de la notion de label. Tout routeur « traditionnel » peut être un routeur CE, quelle que soit son type ou la version d'IOS utilisée.

La figure ci-dessous montre pour chaque site de SH leur emplacement dans l'architecture VPN :

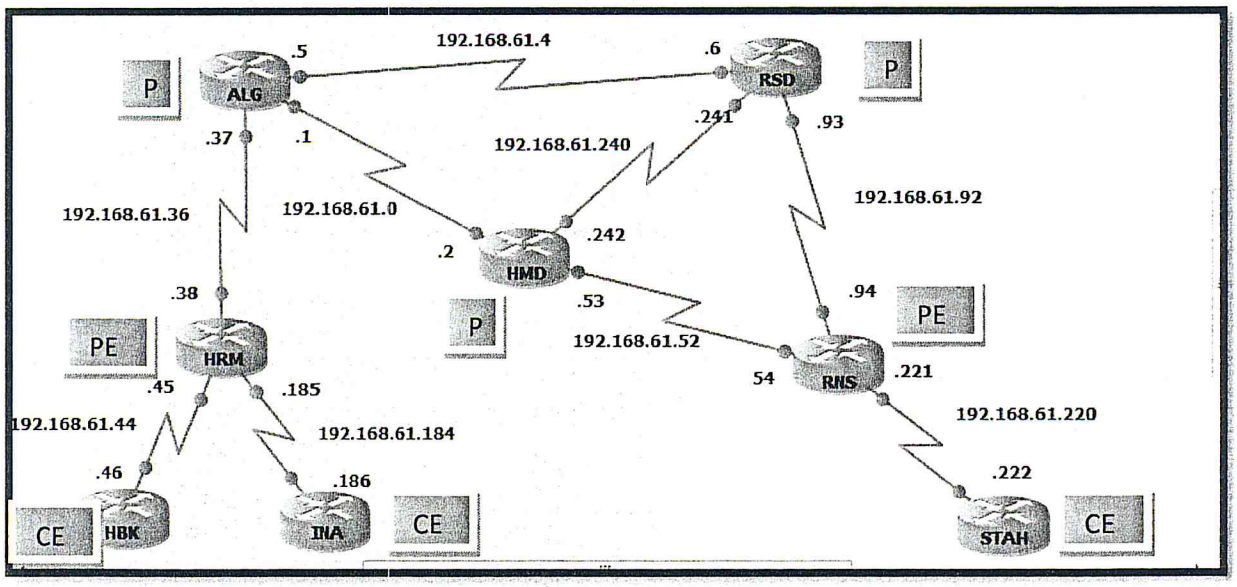


Figure III.14 : le VPN/MPLS sur le réseau SH

Nous aurons mis en place un VPN d' Intranet simple entre deux sites appartenant au client 1 qui est le site de HBK et site 2 du STAH. La configuration de la transmission de MPLS est la première étape à la disposition du backbone VPN MPLS du fournisseur de service. Cette étape assure la promptitude du fournisseur de service pour fournir des services MPLS-connexes aux clients éventuels :

Routeur virtuel VRF : La notion même de VPN implique l'isolation du trafic entre sites clients n'appartenant pas aux mêmes VPN. Pour réaliser cette séparation, les routeurs PE ont la capacité de gérer plusieurs tables de routage grâce à la notion de VRF (VPN Routing and Forwarding). Une VRF est constituée d'une table de routage, d'une FIB (Forwarding Information Base) et d'une table CEF spécifiques, indépendantes des autres VRF et de la table de routage globale. Chaque VRF est désignée par un nom (par ex. RED, GREEN, etc.) sur les routeurs PE. Les noms sont affectés localement, et n'ont aucune signification vis-à-vis des autres routeurs. Chaque interface de PE reliée à un site client est rattachée à une VRF particulière. Lors de la réception de paquets IP sur une interfaces client, le routeur PE procède à un examen de la table de routage de la VRF à laquelle est rattachée l'interface, et donc ne consulte pas sa table de routage globale. Cette possibilité d'utiliser plusieurs tables de routage indépendantes permet de gérer un plan d'adressage par sites, même en cas de recouvrement d'adresses entre VPN différents.

- **Etape 1 :**configurer une VRF sur chaque PE concerné (HRM et RNS)
  - Créer la VRF on tapant la commande dans le mode config .
  - Créer un identifiant route distinguisher (RD) pour chaque VRF .

    ➢ Des sites appartenant à des VPN isolés ayant la possibilité d'utiliser des plans d'adressage recouvrants, les routes échangées entre PE doivent être rendues uniques au niveau des updates BGP. Pour cela, un identifiant appelé RD (Route Distinguisher), codé sur 64 bits, est accolé à chaque subnet IPv4 d'une VRF donnée. Le RD s'écrit sous la forme « ASN:nn » ou « IP-Address:nn ».

    Créer une route target .

```
no ip domain lookup
ip vrf client
 rd 10:10
 route-target export 2:2
 route-target import 5:5
!
```

Figure III.15 : configuration de VRF

➢ Le RD permet de garantir l'unicité des routes VPNv4 échangées entre PE, mais ne définit pas la manière dont les routes vont être insérées dans les VRF des routeurs PE. L'import et l'export de routes sont gérés grâce à une communauté étendue BGP (extended community) appelée RT (Route Target). Les RT ne sont rien de plus que des sortes de filtres appliqués sur les routes VPNv4. Chaque VRF définie sur un PE est configurée pour exporter ses routes suivant un certain nombre de RT. Une route VPN exportée avec un RT donné sera ajoutée dans les VRF des autres PE important ce RT.

- Associer la VRF a l'interface du HRM et RNS faisant face a deux routeurs HBK et STAH (les CE)

Etape 2 :configurer le protocole BGP(vu dans le chapitre précédent) l'instance VRF dans sur chaque PE :reviens a définir la famille d'adresse et redistribution des connexions et configuration des voisins CE .

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.250.5.130 remote-as 1
 neighbor 10.250.5.130 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 10.250.5.130 activate
  neighbor 10.250.5.130 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf client
  redistribute eigrp 1
  no synchronization
 exit-address-family
!
```

Figure III.16 :configuration de BGP

Etape 3 : configurer le routage PE vers PE :utiliser dans cette étape l'adresse loopback comme adresse source et définir les voisins PE (HRM et RNS)et activer la famille d'adresses VPN .

```
router eigrp 1
 auto-summary
 !
 address-family ipv4 vrf client
  redistribute bgp 1 metric 1000 100 255 1 1500
  network 192.168.61.44 0.0.0.3
  no auto-summary
  autonomous-system 1
 exit-address-family
!
```

Figure III.17 :configuration de EIGRP

En terme de deux critères de base qui sont la QOS et la sécurité, on peut dire que MPLS présente un très bon choix pour la sécurité car il permet la transmission des données en toute sécurités en se basant sur les VPNs . Mais toutefois cette architectures ne permet pas de résoudre tous les problèmes de la OQS et la maîtrise de cette dernière reste aujourd'hui un défi majeur pour la recherche sur les réseaux multiservices tel que MPLS c'est dans ce but que nous allons développer une approche permettant d'améliorer encore bien la QOS dans le réseau SH on ce basant sur le terme congestion qu'est l'évènement critique dans le fonctionnement des réseaux .

Basant sur tout ce qui a été décrit dans les chapitres précédents et pour accomplir le travail du MPLS l'objectif de notre approche est de trouver un moyen de prévoir les congestions dans les réseaux .

Notre approche permet de prédire les congestions . elle doit permettre de savoir si il va y avoir une congestion dans le futur ou non. L'application ne vise que les prévisions de congestion à court terme. L'échelle de temps des prévisions est donc de quelques secondes ,et elle permet par la suite générer des alarmes .

Nous passons a définir l'architecture de notre approche afin de bien comprendre le comportement de cette dernière pour prédire la congestion .

III-4-La conception de notre approche:

Nous commençons par une petite représentation du protocole SNMP qui est été utilisé comme base pour le mécanisme développé .

III-4-1.Le protocole SNMP:

SNMP signifie Simple Network Management Protocol (traduisez *protocole simple de gestion de réseau*). Il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau .

SNMP est un protocole de la famille TCP/IP , et peut donc être utilisé sur tous les réseaux de type Internet. Il exploite les capacités du protocole de transport UDP(User Datagram Protocol), chaque trame possède une adresse source et une adresse destination qui permettent aux protocoles de niveaux supérieurs comme SNMP de pouvoir adresser leurs requêtes.

SNMP a pour rôle exclusif la gestion réseau, et offre en conséquence un grand nombre d'avantages que n'ont pas les autres protocoles. Il propose une interface de transaction commune à tous les matériels, et donc la plus homogène possible .

III-4-2.Le principe de fonctionnement:

Le protocole SNMP se base sur le fait qu'il existe une station de gestion réseau, le manageur, dont le rôle est de contrôler le réseau et de communiquer via ce protocole avec un agent. L'agent est de manière générale une interface SNMP embarquée sur le matériel destiné à être administré à distance.

Le système de gestion de réseau est basé sur deux éléments principaux : un superviseur et des agents. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface connectant l'équipement managé au réseau et permettant de récupérer des informations sur différents objets.

Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets manageables. Ces objets manageables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont

directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données appelée **MIB** ("*Management Information Base*"). SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc basée sur trois principaux éléments :

- Les équipements managés (managed devices) sont des éléments du réseau (ponts, hubs, routeurs ou serveurs), contenant des "objets de gestion" (*managed objects*) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;
- Les agents : c'est-à-dire une application de gestion de réseau résidant dans un périphérique et chargé de transmettre les données locales de gestion du périphérique au format SNMP ;
- Les systèmes de management de réseau (*network management systems* notés NMS), c'est-à-dire une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration.

III-4-3.L'architecture du système sécurisé avec QOS :

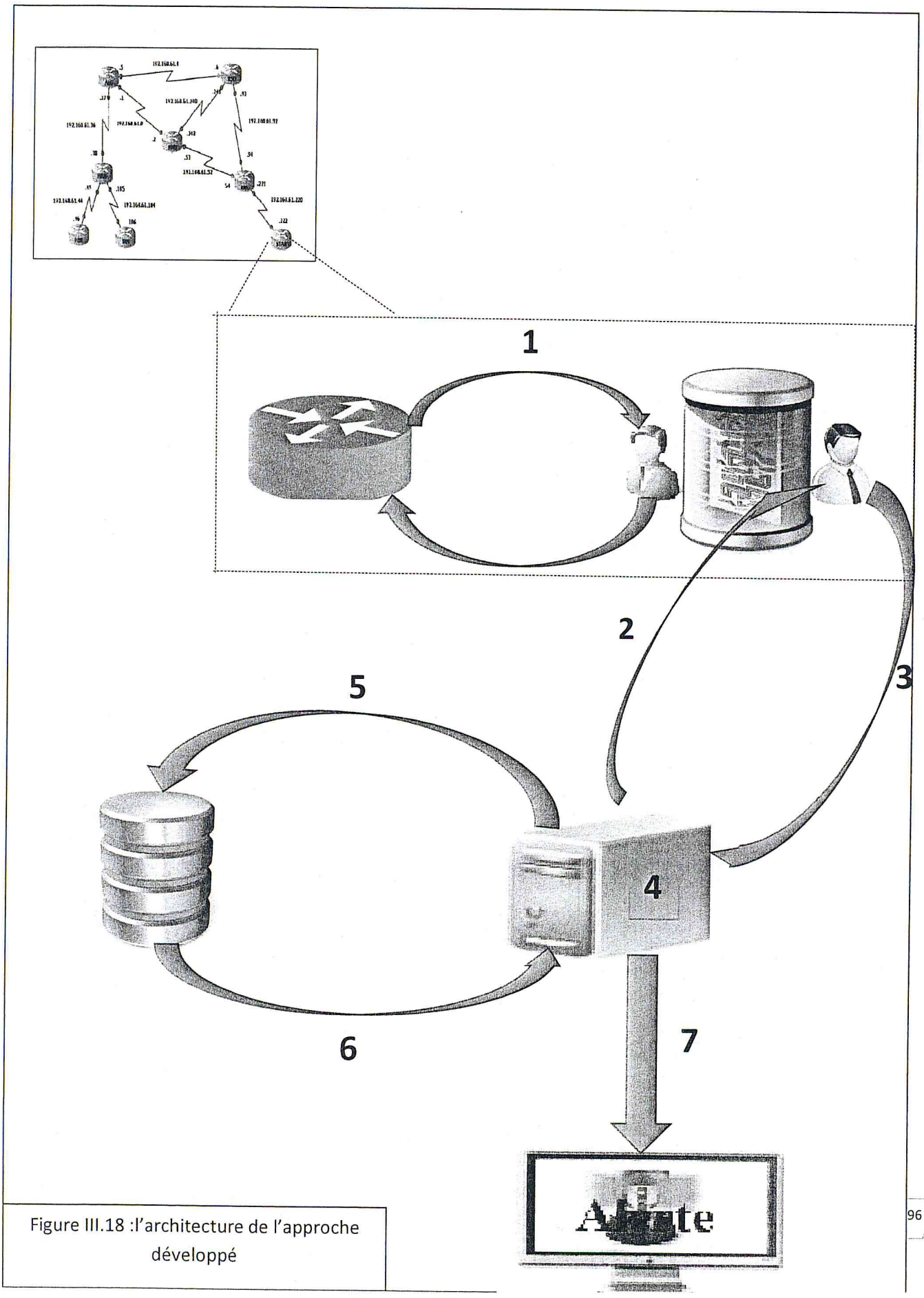


Figure III.18 :l'architecture de l'approche développé

Les détails de l'architecture :

1 : Les agents SNMP sont des entités qui se trouvent au niveau de chaque interface d'un routeur et permettant de récupérer des informations sur des différents objets ,ces derniers peuvent être des informations matérielles ,des paramètres de configuration, des statistiques de performance ,ils sont classés dans une sorte de base de données appelée la MIB, c'est cette base a quelle on va demander les informations .

2 : Le Manger SNMP demande une information a un agent SNMP via une requête, pour chaque envoi de message,

3 : Une réponse est retournée par l'agent via la MIB .

4 : C'est le serveur qui contient notre application de gestion de la congestion .

5 : Les données récupérées par SNMP sont enregistrées dans une base de données

6 :Les données stockés dans la base sont traité par notre module périodiquement .

7 :le déclanchement d'une alerte lors de l'analyse des données .

La figure suivante présente le diagramme de classe de la base de données :

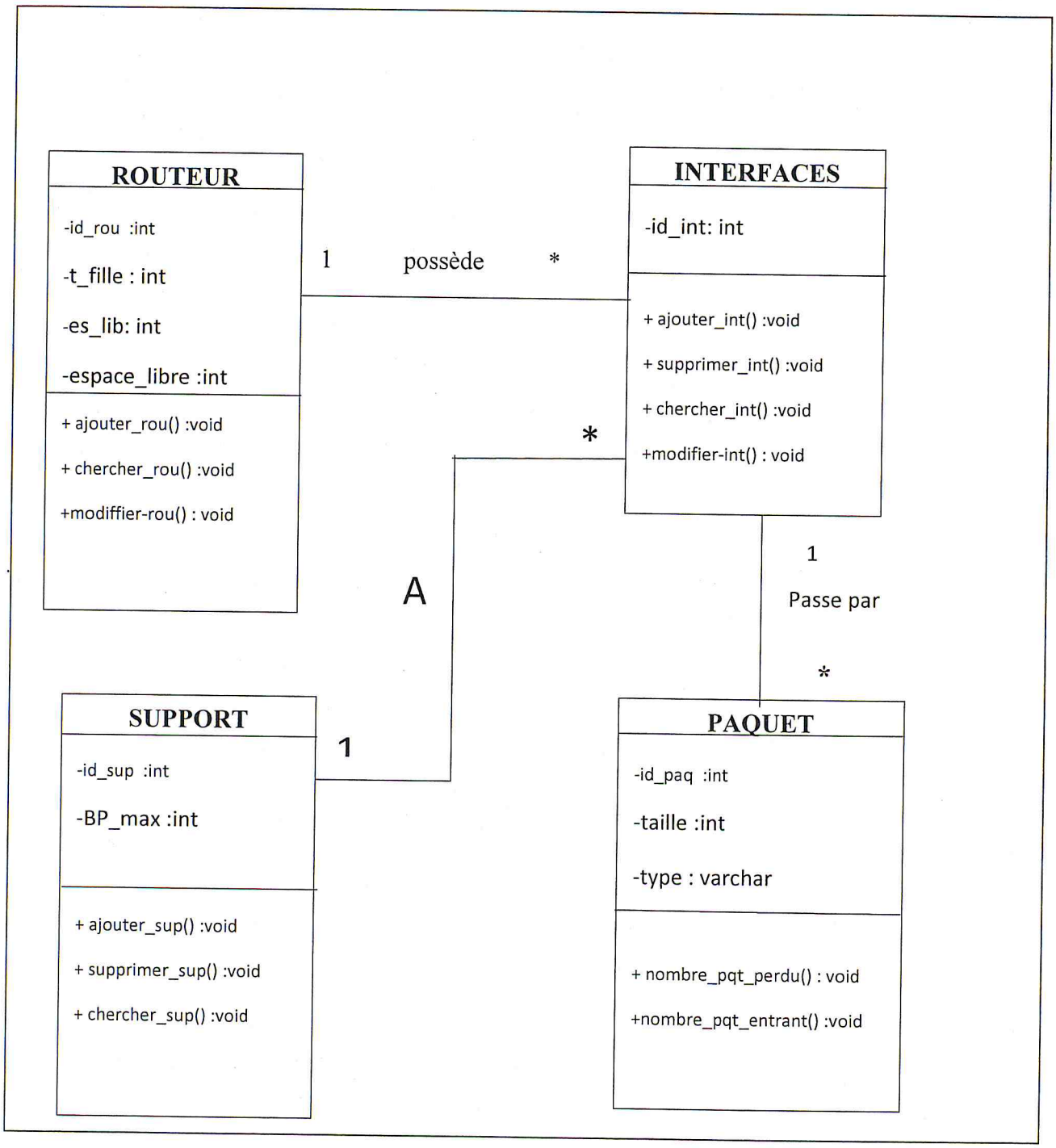


Figure III.19 : diagramme de classe

le test de congestion :

L'algorithme est composé de 6 parties, ou chaque partie utilise les informations fournies par la partie précédente.la description de chaque partie est présenté ci-dessous :

La première partie de l'algorithme : récupère les informations sur notre réseau à partir de la base de donnée qu'elle est remplie par le protocole SNMP chaque 0.2 secondes pour chaque information de trafic, "ce délai 0,2 Sec a été choisi car il permet une réaction rapide pour les trafics en temps réel ".

La deuxième partie : L'indicateurs à calculer dans cette partie est le débit à recevoir pour chaque routeur durant ces intervalles à partir des routeurs voisins, donc nous mettons une fonction de supervision sur les interfaces connectées directement au routeur et comme la taille de chaque paquet est connu alors il est facile avec une opération d'addition de connaitre le débit totale. Le changement de ce dernier pour chaque routeur et finalement représenter par un graphe.

La troisième partie : Avec une comparaison entre le débit totale calculé précédemment et l'espace libre dans le routeur (information retourné par SNMP et stocké dans la base de données) on peut indiquer s'il y a une congestion ou non.

La quatrième partie :A partir du graphe qui représente le changement de débit, cette partie utilise les dernières valeurs de débit pour calculer le temps avant une possible congestion. Dans notre étude nous utilisons la méthode linéaire afin de pouvoir décider s'il peut y avoir congestion ou non (à partir de la partie précédente). On peut ainsi estimer le temps nécessaire à la congestion.

Pour la méthode linéaire, on prend les deux dernières mesures de débit afin de calculer la pente entre les deux points. Avec le coefficient directeur de la pente, on peut ensuite calculer à quel moment la congestion peut arriver.

Le calcul global : Le modèle linéaire se base sur deux points de mesure. Il est donc très sensible aux variations du trafic.

Calcul de la pente :

$$\alpha = \frac{\mathrm{DBT\_t2} - DBT\_t1}{\mathrm{T}} \qquad \Delta$$

Ou : **DBT_t2**: mesure du débit à l'instant t.

DBT_t1: mesure du débit à l'instant t – 1.

Δ : la défaisance entre t et t-1.

α : coefficient directeur de la pente.

Calcul du temps avant la congestion:

$$TAC = \frac{BP\_max - DBT\_t2}{\alpha}$$

Ou : **TAC** : le temps (en secondes) restant avant la congestion.

BP_max : bande passante maximum du lien.

La cinquième étape :Un autre indicateur à calculer pour les étapes qui suit, est le nombre de paquets qui va être supprimer dans un intervalle de mesure si l'espace vide des filles de routeur est insuffisant, il est calculé par une soustraction de l'espace vide des filles et le débit à recevoir.

La sixième étape : La phase de décision a prendre pour lancer un traitement de contre congestion elle est très sensible, pour cela un certain nombre d'information est nécessaire a être fourni, l'un de ces information le type de l'alarme qui est défini dans notre algorithme comme suit :

Dans un cycle si l'espace vide des filles de routeur est inférieur à 50% de la taille totale, un traitement ce lance sur le nombre de paquets calculés , si est le cas un déclanchement d'un traitement ce lance qui définit 3 types d'alerte selon le niveau de charge de routeur :

-alerte1 si la charge de routeur est entre 50% et 65%,

- **alerte2** si la charge de routeur est entre 65% et 80%,

-alerte3 si la charge de routeur est >= 80%) et à chaque alerte y a une politique de contre congestion mise en œuvre .

Le pseudo algorithme :

```
Répeter à chaque 0.2 seconde
    Pour R_TOP de 0 à NBR_R
        Select INT_CONECTE _A_R ;
        Pour INT_CONECTE _A_R de 0 à NBR_INT
            Calcul DBT ;
            DBT_TOTAL = DBT_TOTAL + DBT ;
        Tracer_graphe (DBT_TOTAL);
        Si esspace_occupé _R > 50% ( taille_total_R) alors
            DECISION := congestion ;
        Sinon :
            DECISION := pas_de_congestion ;
        Si esspace_libre_R =< 80% ( taille_total_R) alors
            ALPHA = (DBT_t2 – DBT_t1) / le_cycle ;
            TAC = (BP_lien - DBT_t2) / ALPHA ;
            DBT_t1 := DBT_t2 ;
        Si DBT_TOTAL > esspace_libre_R alors
            DBT_depassé = DBT_TOTAL - esspace_libre_R ;
            NBR_PQT_perdu = DBT_depassé / taille_PQT ;
        Si congestion alors
            Esspace_occupé_congestion =
            Si Esspace_occupé_congestion > = 50% et <=65%( taille_total_R) alors
                Déclanché Alarme I
            Si Esspace_occupé_congestion > = 65% et <=80%( taille_total_R) alors
                Déclanché Alarme II
            Si Esspace_occupé_congestion > 80%( taille_total_R) alors
                Déclanché Alarme III
```

Conclusion :

Dans ce chapitre nous avons étudié le réseau WAN actuel et voir ces différentes lacunes nous avons fixé nous objectifs et ensuite nous sommes passés a implémenter le protocole MPLS qui doit répondre aux exigences de SONATRACH ,et pour encore bien gérer la congestion dans les réseaux nous avons développé une application permettant de prévenir la congestion .

Les tests et les résultats de ces deux solutions sont présentés dans le chapitre suivant .

Introduction :

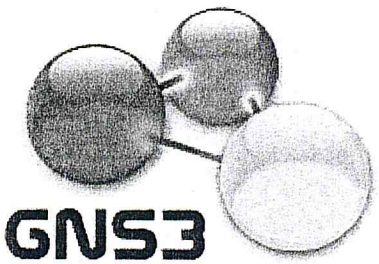
Nous décrivons dans ce chapitre les outils logiciels utilisés pour arriver a implémenter le protocole MPLS ,nous présenterons aussi le langage utilisé pour développer notre approche .

Ensuite nous passerons a l'étape de test du chaque solution proposé soit coté configuration soit le coté application et a la fin les résultats obtenues de ce travail .

IV-1-La migration vers le MPLS :

IV-1-1.les logiciels utilisés :

GNS3 :est un logiciel freeware qui permet d'émuler des routeurs et commutateurs de la marque CISCO, il se base sur l'utilisation des serveurs appelés DYNAMIPS et DYNAGEN [73].
GNS3 nécessite une vraie image IOS pour fonctionner, pour cela nous nous sommes procurés d'un routeur CISCO de type 7200 de la gamme c7200.



VMwareWorkstation :Est un logiciel de vitalisation qui permet d'avoir plusieurs machines avec des systèmes d'exploitations différents qui s'exécutent sur le même ordinateur, ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique . Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

Wireshark : est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sue un réseau [74].

Comme un grand nombre de programmes, Wireshark utilise la librairie réseau pcap pour capturer les paquets .

.

IV-1-2.les tests sur les différentes applications du MPLS:

IV-1-2-1.Activer le MPLS :

```
!
interface Serial1/0
 ip address 192.168.61.5 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 clock rate 64000
 ip rsvp bandwidth 1000
!
interface Serial1/1
 ip address 192.168.61.1 255.255.255.252
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 clock rate 64000
 ip rsvp bandwidth 1000
!
interface Serial1/2
 ip address 192.168.61.37 255.255.255.252
 mpls ip
 serial restart-delay 0
 clock rate 64000
!
```

Figure IV.1 :activation du MPLS

Apres l'activation du MPLS et le protocole de distribution des labels LDP La commutation de label fonctionne sur les routeurs internes a MPLS.et des labels sont distribués comme ci-dessous :

```
ALG#sh mpls forwarding-table
Local  Outgoing      Prefix            Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
16     Pop Label [T] 10.250.5.130/32   0             Tu2         point2point
       Pop Label [T] 10.250.5.130/32   1991          Tu1         point2point
17     Pop Label     10.250.3.130/32   0             Se1/1       point2point
18     Pop Label     10.250.2.130/32   1884          Se1/2       point2point
19     Pop Label     192.168.61.240/30 0             Se1/1       point2point
       Pop Label     192.168.61.240/30 0             Se1/0       point2point
20     Pop Label     192.168.61.92/30  0             Se1/0       point2point
21     Pop Label     192.168.61.52/30  0             Se1/1       point2point
22     Pop Label     10.250.4.130/32   0             Se1/0       point2point
23     Pop Label     192.168.61.184/30 0             Se1/2       point2point
```

```
HRM#sh mpls forwarding-table
Local  Outgoing      Prefix            Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
16     16            10.250.5.130/32   0             Se1/0       point2point
17     17            10.250.3.130/32   0             Se1/0       point2point
18     Pop Label     10.250.1.130/32   0             Se1/0       point2point
19     19            192.168.61.240/30 0             Se1/0       point2point
20     20            192.168.61.92/30  0             Se1/0       point2point
21     21            192.168.61.52/30  0             Se1/0       point2point
22     Pop Label     192.168.61.4/30   0             Se1/0       point2point
23     Pop Label     192.168.61.0/30   0             Se1/0       point2point
24     22            10.250.4.130/32   0             Se1/0       point2point
25     No Label      10.250.11.130/32[V]   \
                                       0             Se1/2       point2point
26     No Label      192.168.61.44/30[V]   \
                                       0             aggregate/client
```

Figure IV.2 :la distribution des labels au niveau des routeurs LSR et LER

Nous remarquons une différence dans la façon de distribution de label, le routeur LSR et le routeur LER ne génère pas les labels de la même façon .

IV-1-2-2.Le trafic Engineering:

- Un test sur les tunnels :Le test suivant va nous permettre de confirmer le bon fonctionnement des 2 tunnels :

le tunnel explicite :

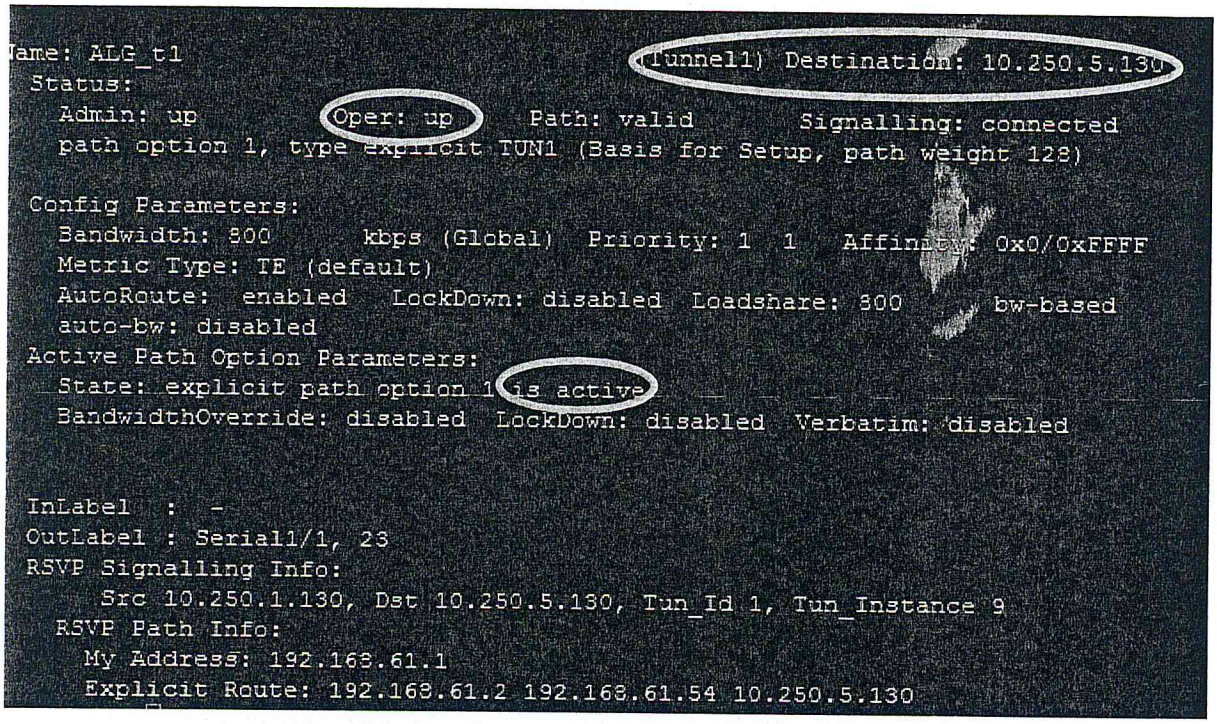


Figure IV.3 :le tunnel explicite

le tunnel dynamique :

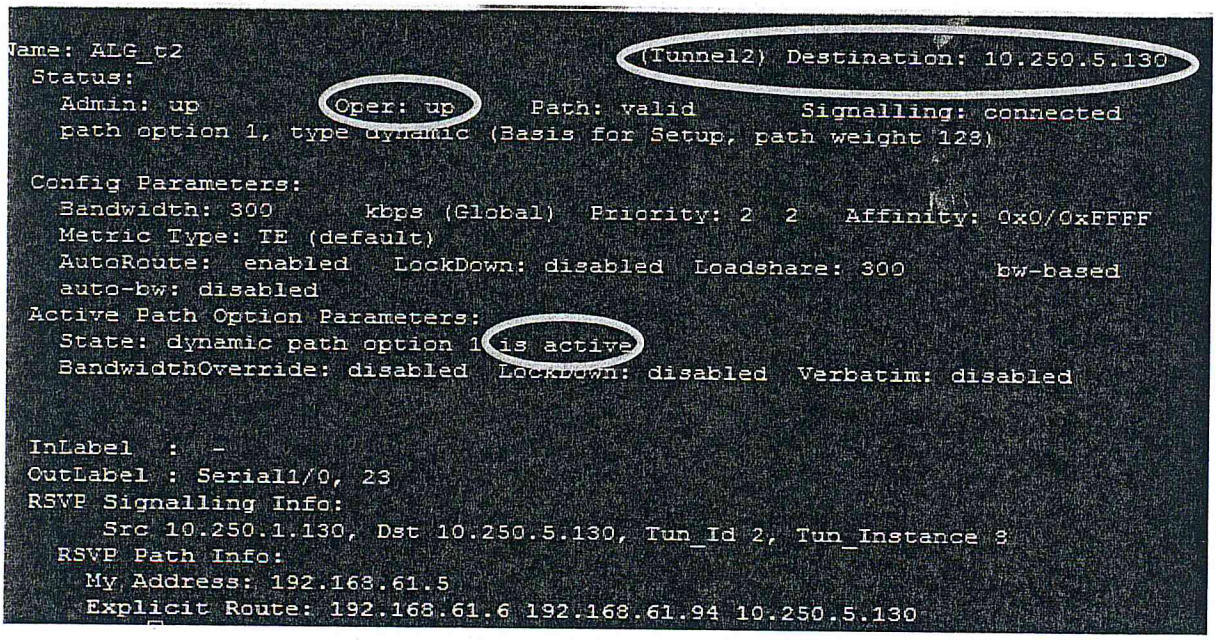


Figure IV.4 :le tunnel dynamique

Le fast reroute :

```
LSP midpoint frr information:
LSP identifier                In-label Out intf/label    FRR intf/label    Status
10.250.1.130 1 [9]            23       Se1/2:implicit-n Tu100:implicit-n ready
```

Figure IV.5 :le chemin Fast reroute

La figure ci-dessus indique que le tunnel fast-reroute est ready c'est-à-dire que pour le moment ne fait rien .

On va imposer une coupure dans le lien que le tunnel fast-reroute protège

```
LSP midpoint frr information:
LSP identifier                In-label Out intf/label    FRR intf/label    Status
10.250.1.130 1 [9]            23       Se1/2:implicit-n Tu100:implicit-n active
HMD#
```

Figure IV.6 :le chemin Fast reroute activé après une coupure

Et voila la figure ci-dessus indique que le fast-reroute est activé après la coupure de lien entre HMD et RNS

IV-1-3-3.Le VPN:

Le routeur CE1 :

```
HBK>en
HBK#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HBK(config)#exit
HBK#s
*Sep  5 07:50:19.347: %SYS-5-CONFIG_I: Configured from console by console
HBK#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.61.0/30 is subnetted, 2 subnets
C       192.168.61.44 is directly connected, Serial1/0
D       192.168.61.220 [90/2681856] via 192.168.61.45, 00:02:20, Serial1/0
     10.0.0.0/32 is subnetted, 2 subnets
D       10.250.19.130 [90/2309856] via 192.168.61.45, 00:02:20, Serial1/0
C       10.250.11.130 is directly connected, Loopback0
HBK#
```

Figure IV.7 :la table de routage au niveau du CE1-le routeur HBK-

Après avoir configurer le VPN une route vers CE2 qui est le routeur du STAH est affiché dans la table du routage de routeur HBK .

La figure du routeur CE2 :

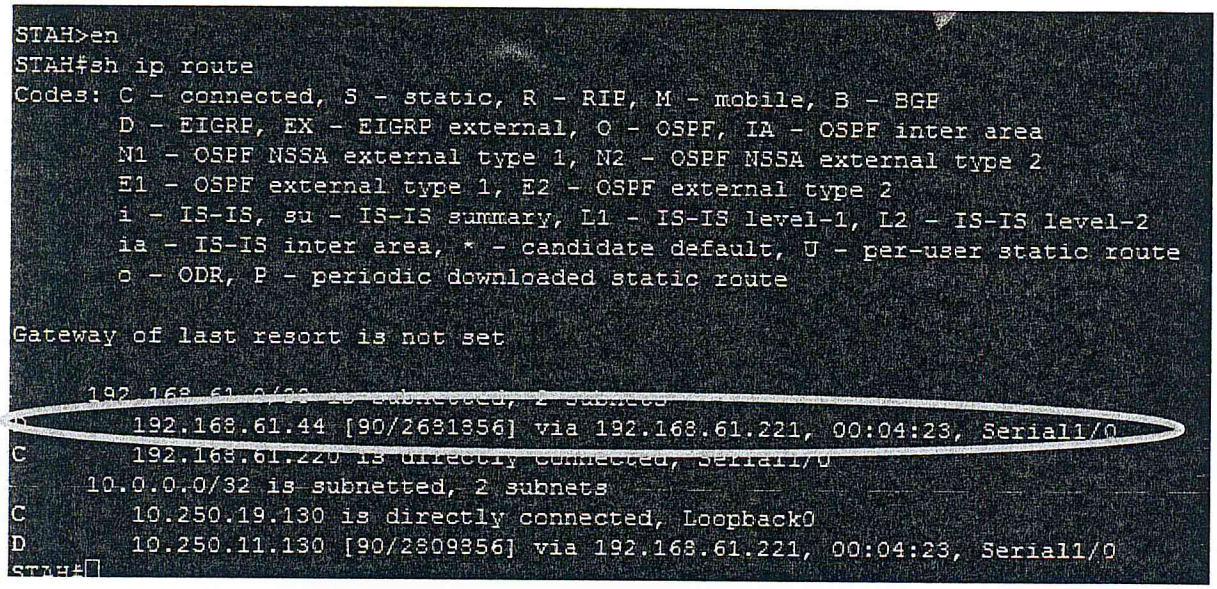


Figure IV.8 :la table de routage au niveau du CE2-le routeur STAH-

Le contraire pour le routeur du STAH .

Les VPN BGP MPLS possèdent plusieurs avantages :

- **Recouvrement possible des classes d'adresses :** Plusieurs sites peuvent partager un même subnet IPv4. Deux sites distants peuvent faire partir d'un VPN BGP MPLS même si il possède la même classe d'adresses IPv4. La seule contrainte de cet avantage est que deux adresses IPv4 identiques ne peuvent communiquer ensemble .
- **Montée en charge :** Les VPN BGP MPLS utilisent des technologies existantes (BGP et MPLS sont déjà utilisées sur les réseaux opérateurs). Ainsi la montée en charge est très bien supportée dans la mesure ou la complexité est repoussé aux extrémités du VPN dans le routeur PE. BGP, grâce à ses optimisations et extensions supporte également très bien la montée en charge.
- **La Flexibilité accrue :** En effet, le type de connexion Internet des sites est peu important. De plus, la RFC définit comment doivent être mis en œuvre les interconnexions opérateurs au niveau de BGP (qui assure la communication entre systèmes autonomes), même si celles ci encore un fois, existe déjà dans les interconnexions opérateurs.

- **Pas d'overlay :** Etant donné que BGP et MPLS sont déjà utilisés par les opérateurs, il n'y a pas de surcouche pour créer le VPN. Le VPN BGP MPLS a l'avantage d'être mis en œuvre via des protocoles déjà en exploitation sur les backbones opérateurs .

Un autre intérêt du MPLS réside dans le faite que deux sites distants peuvent avoir la même adresse IP et cela ne va poser aucun problème le contraire dans les réseaux traditionnels ou nous devons implémenté le NAT pour régler ce problème .

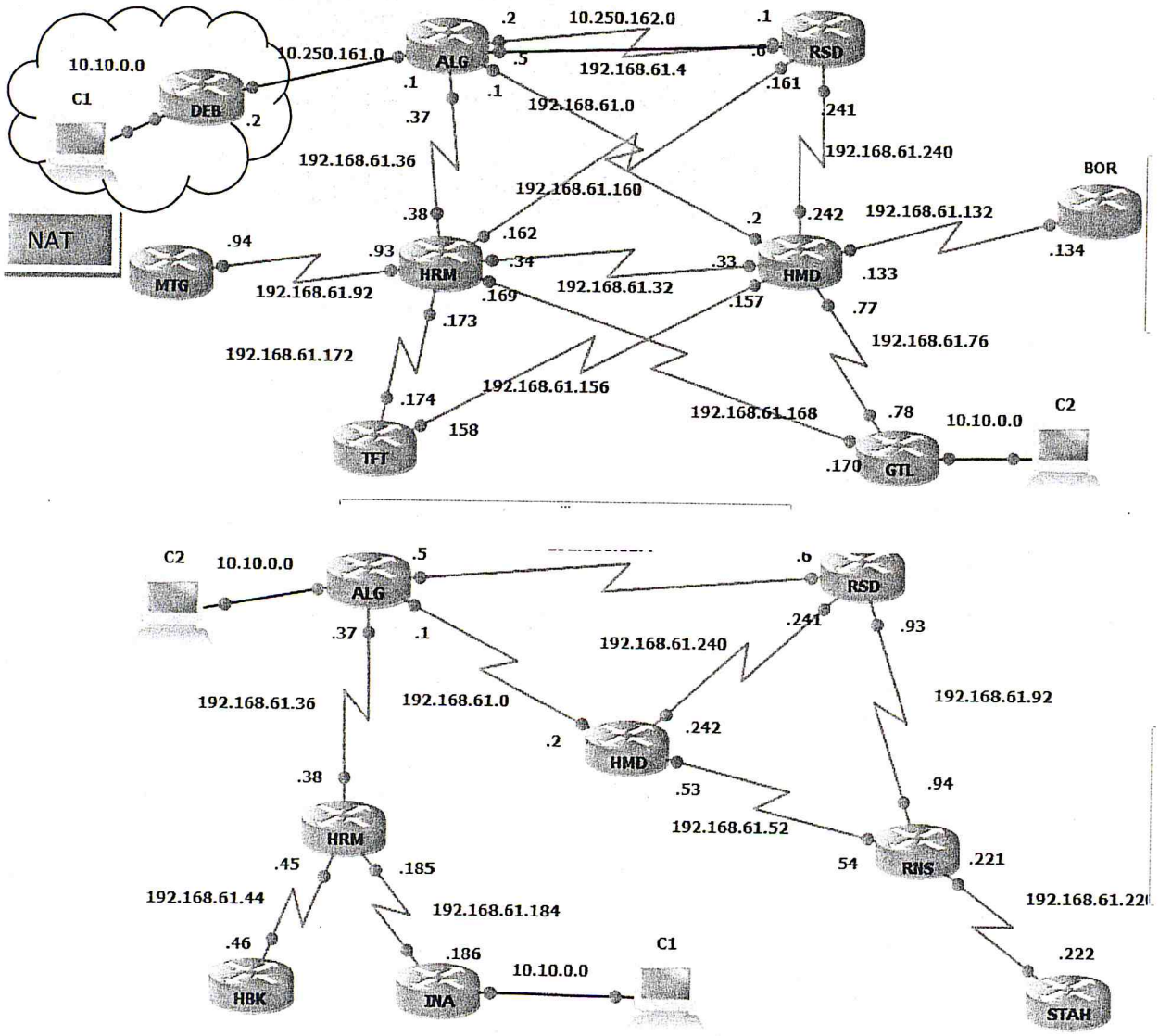


Figure IV.ç :le MPLS et le NAT

IV-2-L'approche développé :

Pour développer notre approche nous avons utilisé le langage de programmation PHP .

Le **langage PHP** est un langage de programmation web côté serveur, ce qui veut dire que c'est le serveur qui va interpréter le code PHP (language de scripts) et générer du code HTML qui pourra être interprété par votre navigateur.
Le php permet d'ajouter des fonctionnalités de plus en plus complexe, d'avoir des sites dynamiques, de pouvoir gerer une administration de boutique en ligne, de modifier un blog, de créer des réseaux sociaux...
Le php fut crée en 1994 par Rasmus Lerdorf, c'est un language libre et gratuit, avec une grande communauté mondiale.

Et nous avons implémenté notre base de données avec MySQL :

MySQL est un système de gestion de base de données (SGBD). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde[1], autant par le grand public (applications web principalement) que par des professionnels,

Authentification

Lorsque l'administrateur lance l'application, une demande d'authentification apparait, l'administrateur doit introduire un login et un mot de passe puis il valide.

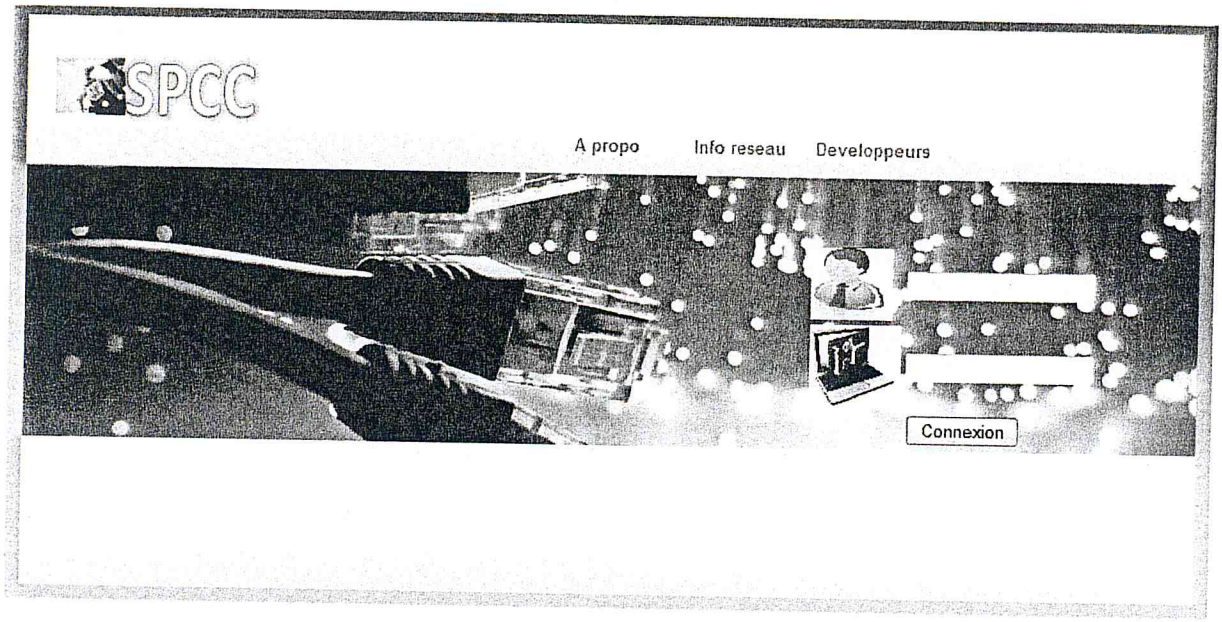


Figure IV.10 la page d'authentification

Activation des alarmes :

Pour notre test nous avons choisis le routeur R01, le trafic est généré depuis les Routeurs R02 et R03 et R04 vers le Routeur R01(ou le débit et la taille de paquet est généré automatiquement pour réaliser tous les cas possible),

Nous allons généré 3 types de trafic qui ce diffère dans les débits pour voir le déclanchement des larmes

au premier temps en vas mis en place un trafic ou le débit a recevoir plus l'espace occupé est inferieur a 50% de la taille de la fille dans le R01 .

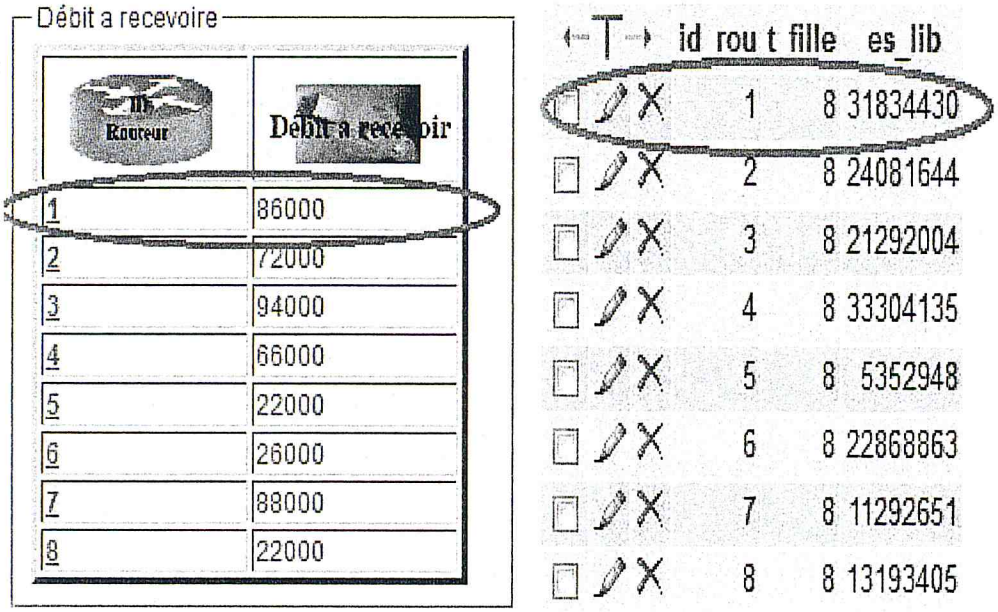


Figure IV.11 le débit reçu et l'espace libre

Un trafic inferieur a 50% de la taille de la fille ne pose aucun problème pour le routeur récepteur et donc l'algorithme déclare que il **n'y a pas congestion**.

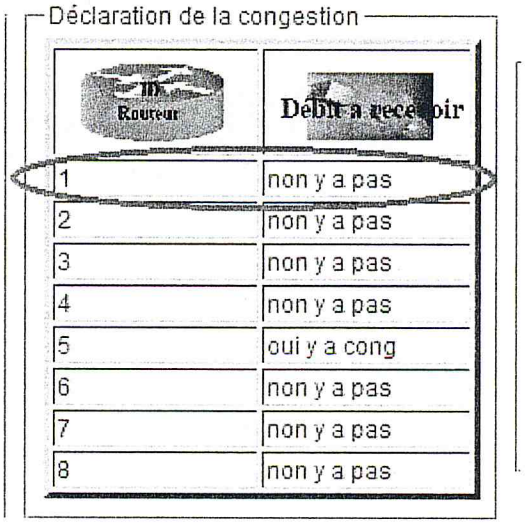


Figure IV.12 ;déclaration de la congestion

Il n'a pas une congestion dons le temps avant la congestion est nul .

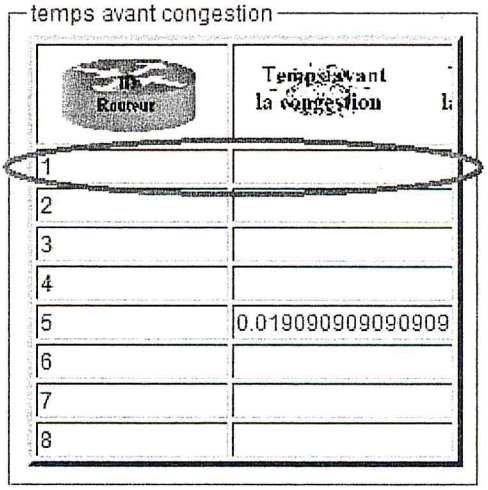


Figure IV.13 ;le temps avant la congestion

Ainsi le nombre de paquets qui vont être supprimé est nul

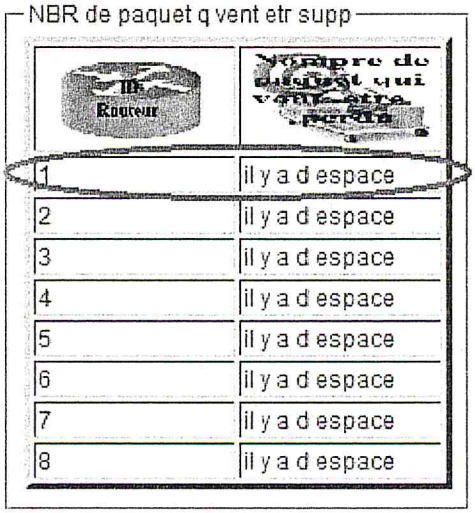


Figure IV.14 :les paquets a supprimer

Et a la fin l'algorithme ne déclenche aucune alerte

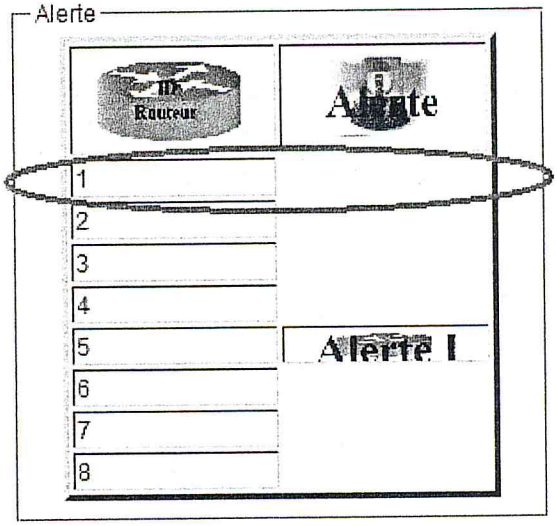


Figure IV.15 :le déclanchement d'une alarme

L'affichage finale est de la forme

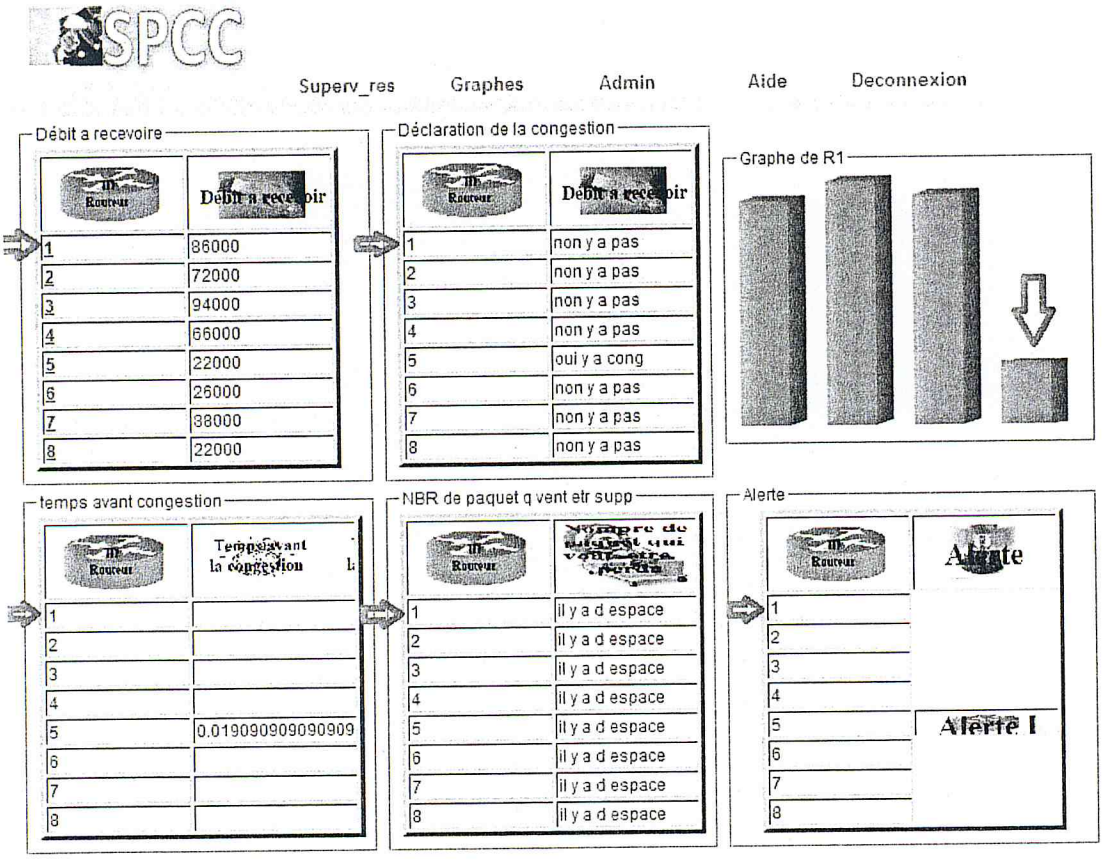


Figure IV.16 :L'affichage final de toute les résultats

Nous passons maintenant au deuxième trafic qu'a un débit plus l'espace occupé est supérieur à 50% et inferieur a 65% de la taille de la fille dans le R. Comme résultat l'algorithme déclenche alerte 1 ainsi nous donne le temps avant la congestion et le nombre de paquets qui vont être supprimé .

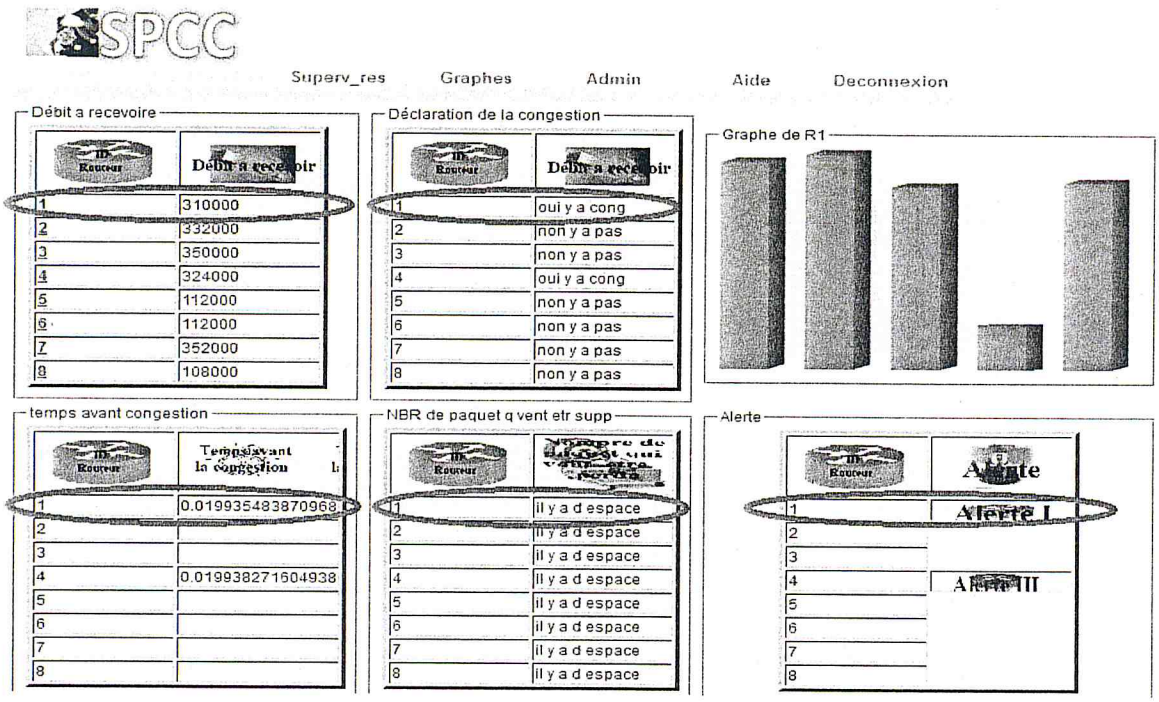


Figure IV.17 :Le déclanchement d'une alarme de type 1

Pour un trafic supérieur a 65% et inferieur a 80% une alarme de type 2 sera généré

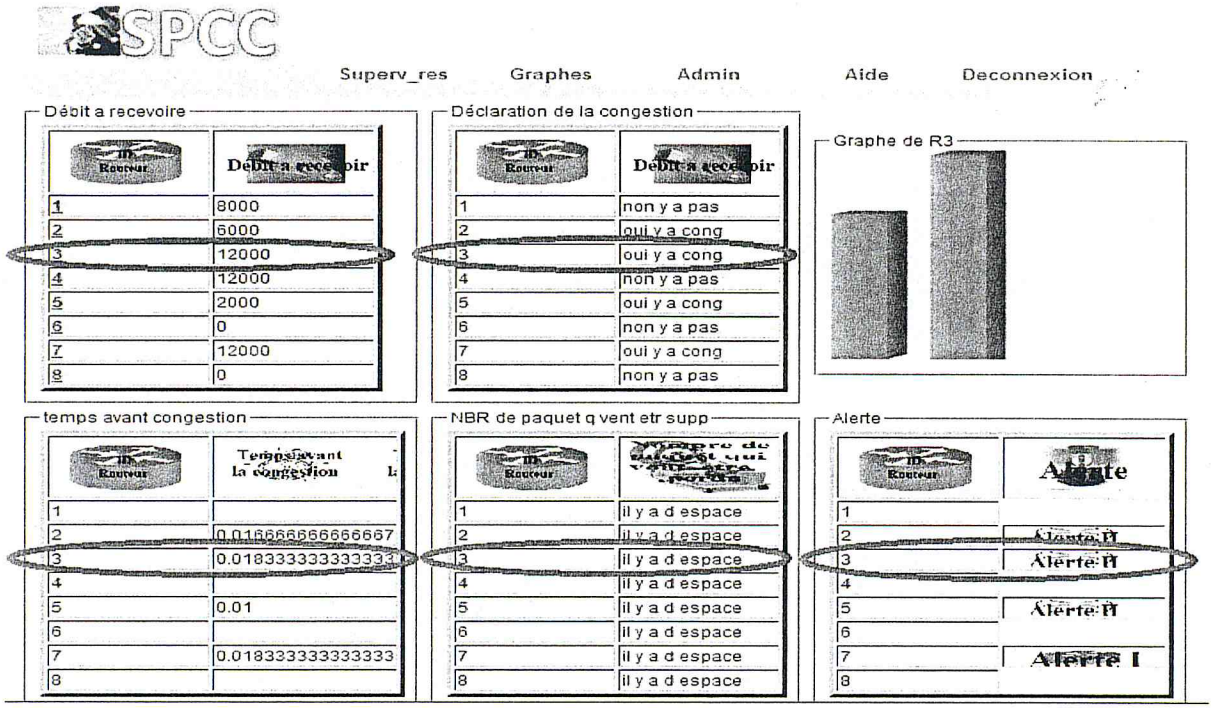


Figure IV.18 :Le déclanchement d'une alarme de type 2

Une fois le trafic génère (le débit + l'espace occupé) est supérieur à 80% de la taille de la fille de routeur R01. L'alarme III se d'éclanche .

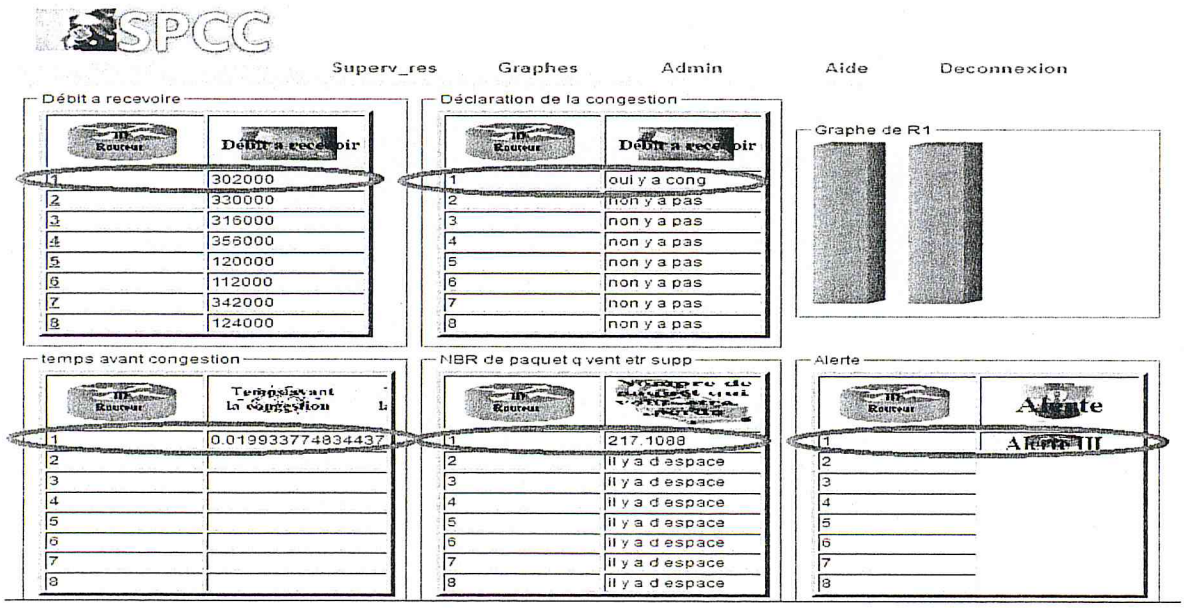


Figure IV.19 :Le déclanchement d'une alarme de type 3

IV-3-Résultats des tests :

L'objectif de notre travail été de trouver un moyen de prévoir les congestions sur les réseaux pour utiliser le réseau au maximum afin de ne pas répartir le trafic trop tôt ou trop tard. Cela permettrait en effet d'utiliser un maximum de bande passante en limitant les pertes de paquets ou le délai lors d'un reroutage. L'hypothèse qui est faite ici est qu'il est possible de prévoir cette congestion à l'aide des informations de trafic contenues dans les équipements réseau. Par exemple, le nombre de paquets dans la file d'attente ou le débit demandé.

Les travaux présentés dans le chapitre de la QOS attendent la congestion pour qu'ils réagissent dans notre cas nous allons cité juste les methodes qui agissent avant que la congestion provienne c'est les deux solutions cités précédemment le RED et le PCN .
Ces solutions existantes génèrent toutes une réaction après l'atteinte d'un niveau fixe. Ces niveaux n'étant pas intelligents, c'est-à-dire qu'ils ne prennent pas en compte le comportement des flux, le trafic est souvent coupé très en amont. Les résultats des expériences réalisées dans les parties précédentes montrent que l'utilisation de la bande passante n'est pas optimale pour les solutions PCN. Ils montrent que le gain possible de débit peut-être de près de 10 % avant que l'alerte ne se déclenche. De plus l'utilisation de RED qui se base sur le nombre de paquets dans la file d'attente montre une réaction tardive. Malgré une limitation du nombre de paquets perdus elle ne permet pas de garantir la qualité de service. Notre méthode de calcul de temps avant la congestion et les paquets qui peuvent être rejeter si on applique pas une gestion de congestion. Elle permet de prévenir les congestions en amont et d'éviter les pertes de paquets.

Conclusion :

Cette étape de test nous a permis de voir l'intérêt du MPLS dans les réseaux IP par l'implémentation du MPLS-TE qui permet de réduire la charge dans les liens, et le MPLS-VPN qui permet de garantir la sécurité dans la transmission des données et a la fin garantir la QOS .
Les tests sur notre application nous ont donnée la possibilité de faire une comparaison entre notre approche et les travaux qu'on déjà été effectués dans le domaine de congestion dans les réseaux a fin de garantir une Qualité de Service .

Conclusion générale

L'objectif de ce projet de fin d'étude est d'améliorer la qualité de service ainsi la sécurité dans les réseaux d'entreprises, donc nous avons commencé notre travail par l'étude des différents protocoles qui ont lieu pour garantir une certaine qualité de service ainsi une sécurité lors de la transmission des données, cette étude nous a permet de choisir le protocole MPLS comme une solution qui répond a nos besoins . Pour cela, nous avons fait le tour des concepts relatifs à ce dernier et présenté les applications qu'il permet de le réaliser, nous nous sommes penchés sur les plus importantes des applications de MPLS à savoir la qualité de service et la prise en charge du "Traffic Engineering" et la sécurité via VPN.

les mécanismes d'ingénierie de trafic généralement utilisés pour lutter contre les congestions mais toute fois il présentent certaines lacunes. Pour cella nous avons passé a étudier les mécanismes de lutte contre la cogestion dans les réseaux, pour le Trafic Engineering Ils se basent sur des niveaux d'alertes fixes et se contentent d'éviter la congestion en limitant l'utilisation des liens. Certains mécanismes permettent d'intervenir une fois que la congestion s'est manifestée, mais cela entraîne une dégradation de la qualité de service. Pour cela nous avons développé une approche qui permet en quelque sorte de prévenir la congestion sans besoin de supprimer des paquets ou bien de limiter l'utilisation des liens .

Nous avons effectué le test de l'approche sur le réseau WAN de SONATRACH après l'implémentation du MPLS , nous avons réussis a implémenté une qualité de service et nous avons arrivé a créer un réseau performant et sécurisé .

Comme notre approche développée permet de prévenir la congestion et de déclencher différents types d'alarmes .Nous proposons comme un travail complémentaire à ce projet d'implémenter un autre module qui va réagir d'après le type d'alerte d'appliquer des méthodes pour éviter au maximum la congestion .

Annexe

[AN01] :IETF : L'Internet Engineering Task Force, abrégée IETF, littéralement traduit de l'anglais en « Détachement d'ingénierie d'Internet » est un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards Internet. L'IETF produit la plupart des nouveaux standards d'Internet.

[AN02] :Interop : est une plante annuelle foire commerciale pour les technologies de l'information organisé par UBM TechWeb . Elle a lieu à quatre endroits différents à différents moments de l'année:Bombay (Inde), New York (NY, USA), Tokyo (Japon) et Las Vegas (NV, USA

[AN03] : VPN :Virtual Private Network est une technique permettant a un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant des infrastructure publiques (Internet). Ce type de liaison est apparu suite a un besoin croissant des entreprises de relier les différents sites et ce de façon simple et économique.

[AN04] :LCP : **Link Control Protocol** (LCP) est un protocole intégré au PPP

Dans une communication PPP, l'émetteur et le récepteur envoient des paquets LCP pour déterminer des informations spécifiques à la transmission de données. Le LCP vérifie l'identité de l'élément connecté et l'accepte ou le refuse, il détermine la taille des paquets acceptables pour la transmission, recherche les erreurs dans la configuration et peut interrompre la communication en cas d'erreur. Les données ne peuvent pas être transmises sur un réseau tant que la connexion n'est pas acceptée par LCP.

[AN05] :NSP : **Network Control Protocol** (NCP) est un protocole réseau intégré à PPP pour négocier les options concernant la couche 3 du réseau : le plus souvent IP (et, plus rarement IPX de Novell NetWare, ou AppleTalk ;

[AN06] :BSD : ***Berkeley Software Distribution***, abrégé en BSD, désigne en informatique une famille desystèmes d'exploitation Unix, développés à l'Université de Californie (Berkeley) entre 1977 et 1995 par un groupe de programmeurs qui comprend notamment Bill Joy, Marshall Kirk McKusicket Kenneth Thompson.

[AN07] :GRE : **Generic Routing Encapsulation** (GRE ou Encapsulation Générique de Routage) est un protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau dans n'importe quel paquet de la couche réseau. Le paquet d'origine est le payload (information utile) du paquet final. Par exemple, les serveurs de tunnel qui chiffrent les données peuvent utiliser GRE à travers Internet pour sécuriser les Réseaux privés virtuels.

[AN08] :LAC(L2TPAccessConcentrateur) :Il sert à fournir un moyen physique pour se con necter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et co nstruit le tunnel vers les LNS. Il se trouve obligatoirement dans l'infrastructure du FAI de cha que utilisateur du VPN. Cela est donc très lourd (et cher) à mettre en place dans la mesure où i l faut louer une place dans un serveur de connexion du FAI ;

[AN09] :LNS :serveur réseau L2TP, il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel. Il se trouve généralement dans l'entreprise o u le service auquel appartient l'utilisateur distant.

[AN10] :UDP : Le ***User Datagram Protocol*** (UDP, en français **protocole de datagramme utilisateur**) est un des principauxprotocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport de la pile de protocole TCP/IP : dans l'adaptation approximative de cette dernière au modèle OSI, il appartiendrait à la couche 4, comme TCP.

[AN11] :PSK : En cryptographie , une **clé pré-partagée** ou **PSK** est un secret partagé qui était auparavant partagée entre les deux parties à l'aide de certains canal sécurisé avant qu'il ne doit être utilisé. Pour construire une clé de secret partagé, la fonction de dérivation de clé doit être utilisée. Ces systèmes utilisent presque toujours de clés symétriques algorithmes cryptographiques. Le terme PSK est utilisé en Wi-Fi cryptage telles que WEP ou WPA , où les deux points d'accès sans fil (AP) et tous les clients *partagent* la même clé.

[AN12] :RSA : Le **chiffrement RSA** (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

[AN13] :ARIS : **(Architecture of Integrated Information Systems)** is a unique and internationally renowned method for optimizing business processes and implementing application systems.

[AN14] :Frame Relay : Le **relayage de trames** (ou **FR**, pour l'anglais ***Frame Relay***) est un protocole à commutation de paquets situé au niveau de la couche de liaison (niveau 2) du modèle OSI, utilisé pour les échanges intersites (WAN) il a été inventé par Eric Scace, ingénieur chez Sprint International

[AN15]:TCP: **Transmission Control Protocol** (littéralement, « protocole de contrôle de transmissions ») abrégé **TCP**, est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793[1] de l'IETF. Dans le modèle Internet, aussi appelé modèle TCP/IP, TCP est situé au niveau de la couche transport (entre la couche réseau et la couche session). Les applications transmettent des flux de données sur une connexion réseau, et TCP découpe le flux d'octets en *segments*, dont la taille dépend de la MTU du réseau sous-jacent (couche liaison de données).

[AN16] : IGP : Un **Interior Gateway Protocol** (**IGP**) est un protocole de routage utilisé dans les systèmes autonomes.

Le rôle d'un IGP est:

- d'établir les routes optimales entre un point du réseau et toutes les destinations disponibles d'un système autonome,
- d'éviter les boucles,
- en cas de modification de topologie (déconnexion d'un lien physique, arrêt d'un routeur), d'assurer la *convergence* du réseau (c'est-à-dire le rétablissement de la connectivité optimale sans boucle) dans les plus brefs délais.

[AN17] :BGP : **Border Gateway Protocol** (**BGP**) est un protocole d'échange de route utilisé notamment sur le réseau Internet. Son objectif est d'échanger des informations d'accessibilité de réseaux (appelés *préfixes*) entre *Autonomous Systems* (AS) car il a été conçu pour prendre en charge de très grands volumes de données et dispose de possibilités étendues de choix de la meilleure route.

[AN18] :MPEG : **MPEG**, sigle de **Moving Picture Experts Group**, est le groupe de travail SC 29/WG 11 du comité technique mixte JTC 1 de l'ISO et de la CEI pour les technologies de l'information. Ce groupe d'experts est chargé du développement de normes internationales pour la compression, la décompression, le traitement et le codage de la vidéo, de l'audio et de leur combinaison, de façon à satisfaire une large gamme d'applications.

[AN19] :ALL : Atm Adaptation Layer adapté aux applications vidéo et audio à débit constant, comme le transport de la voix.

[AN20] :3DES :Le ***Triple DES*** (aussi appelé **3DES**) est un algorithme de chiffrement symétrique par bloc, enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64bits, avec 2 ou 3 clés DES différentes.

[AN21] :NAT : En réseau informatique, on dit qu'un routeur fait du ***Network Address Translation*** (NAT) (« traduction d'adresse réseau »[1]) lorsqu'il fait correspondre lesadresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.

[AN22] : Le champ DSCP :Differentiated Services Code Point un champ dans le paquet IP est contient 6 bits

[AN23]: PAT :Port Address Translation

[AN24]:ACL: **Access Control List** (**ACL**) — *liste de contrôle d'accès* en français — désigne deux choses en sécurité informatique :

- un système permettant de faire une gestion plus fine des droits d'accès aux fichiers que ne le permet la méthode employée par les systèmes UNIX.
- en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.

Les références

[1] :TER Réseaux Haut débit ATM(Asynchronous Transfer Protocol) Fonctionnement mémoire par Oliver Grudet et Serge Kimbébé –université Montpellier II année 2004-2005

[2] : la documentation cisco CCNA le niveau 3

[3] : la partie Histoire de ATM du livre actes du septième Colloque sur l'histoire de l'informatique et des transmissions par Sylvie RItzenthaler année 1998

[4] : ATM sur FUNIX: site web :http://www.funix.org/fr/reseau/mainreseau.php?ref=wan/atm&page=menu année 2004

[5] :glossaire ATM sur dans d'Audits-conseils-Maintenance-Formations Informatiques sur le site web : http://ad-network-informatique.fr/?page_id=14 année 2012 .

[6] : Réseaux ATM :principes, intégration avec IP dans le site de Mathieu du lien : http://mathieu147.11vm-serv.net/cmsmadesimple/index.php?page=introduction-aux-reseaux-atm –l'année de publication 2004 .

[7] :Asynchronous Transfer Mode sur Wikipédia sur le site web : http://fr.wikipedia.org/wiki/Asynchronous_Transfer_Mode -avec une derniere modification le 09-03-2013 .

[8] :Le modèle RSVP du site WEB :http://manu.lochin.net/qos/qoshtml/node6.html –date de publication 12-09-2001 par Emmanuel Lochin

[9] :Int Serv et RSVP sur le site WEB http://www.httr.ups-tlse.fr/pedagogie/cours/tcp-ip/rsvp/ la date de publication 08-12-2001 université Paul Sabtier par André Aoun

[10] : IntServ sur Wikipedia : http://fr.wikipedia.org/wiki/Intserv dernière date de modification le 26-03-2013

[11]: Documentation sur le MPLS par Benbella Benduduh et jean Marc Fourcade sur le lien :http://www.frameip.com/mpls/ -création du document en 2001- .

[12]: VoixPress "Qualité de service sur IP " sur le site : http://www.voxpress.info créer en 2009

[13] : Documentation :Module de maitrise polyvalente Internet et MultiMedia cours sur la qualité de service par Friendman Timur transparents grace a Pascal Anelli avec modifications a l'université Pierre er Marie Curie le 10fevrier 2003 .

[14] :QOS IP :modeles IntServ/DiffServ sur le site : http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/NatchiaKouao-Benlahcen/index.htm realisé par Jean Sebastien Natchla Kouao –Abdelkader Benlahcen

[15] : DiffServ sur Wikipédia sur le site web http://fr.wikipedia.org/wiki/Differentiated_services derniere modification le 15 mars 2013

[16] :Documentation sur Etude du service DiffServ par Sylvain Francois et Anne-lise Renord et jeremy Rovaris en 2003 sur l'addition Esial

[17] : Etude du protocole DiffServ sur guill.net sur le lien : http://www.guill.net/index.php?cat=3&pro=3&wan=6 en 1999 par Tod Elenner

[18] : le protocole PPP et SLIP sur le site comment ça marche le lien :http://www.commentcamarche.net/contents/529-les-protocoles-ppp-et-slip publié le janvier 2004

[19] : article sur :Les différents protocoles utilisés pour le VPN IP sur le site : http://wapiti.telecom-ille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2000ttv01/Bacon_Chappuis/Les%20protocoles%20de%20tunneling.htm publié en 2009

[20] :Le protocole PPP sur le site Guill ;net le lien web : http://www.guill.net/index.php?cat=3&pro=3&wan=4 publié en 1993 par Anthony Fradera

[21] : article sur le protocole de liaison de données PPP sur le site web http://www.labouret.net/ppp/ publié par Ghrislaine Labouret en 17 avril 1998

[22] : etude du protocole PPP :un document publié dans le site :http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2003ttnfa04/elmoumouhi-fourny/Etude_du_protocole_%20PPP.htm par Jean-Christophe Lator en 17 juin 1996

[23] : Tunneling PPTP sur : http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2000ttv01/Bacon_Chappuis/Tunneling%20PPTP.htm par Amma Bounouna en 1999

[24] : Le blog du VPN contien un document sur la comparatif des protocoles PPTP et OpenVPN sur : https://www.vpnblog.net/comparatif-des-protocoles-pptp-et-openpvn/ la date de publication est en 2009

[25] : VPN sur GIGANEWS le lien :http://fr.giganews.com/vyprvpn/compare-vpn-protocols.html publié en 2009

[26] : Documentation sécurité Gnu/Linux sur :http://www.sharevb.net/IMG/pdf/PPTP.pdf par Share VB en mars 2007 .

[27] : Comprendre Point to Point Tunneling Protocol sue le site Microsoft TechNet le lien :http://technet.microsoft.com/fr-fr/library/dd379317.aspx derniere modification mars 2010

[28] :Documentation sur les VPN par Xavier Lassere,Tomàq Klein et Sebf http://www.frameip.com/vpn/#3.1_-_Rappels_sur_Ppp dernier modification par l'auteur Xavier Lasserre en 15 fevrier 2004

[29] : Un exposé présenté par Rabearivony Justin en décembre 2006 continué par Guillaume Desgeorge en 2000

[30] : VPN gratuit français :le Blog de VPN et comparatifs entre les protocoles PPTP,L2TP et OpenVPN publié par JORIS Onfri en 28 -1262012 son lien est :http://www.sfpaintgallery.com/node/5

[31] :Layer 2 tunneling Protocol sur Wikipédia dans le site :http://fr.wikipedia.org/wiki/Layer_2_Tunneling_Protocol derniere modification remonte en 14 mars 2013

[32] : Virtual Private Network L2TP sur la page web : http://www-igm.univ-mlv.fr/~dr/XPOSE2007/cchamp01_VPN/L2TP.html publié par Etienne Duris le responnsable de la filiere informatique en 2000

[33] : Documentaionsur L2TP faite par Par-Sebf sur le lien :http://www.frameip.com/l2tp-pppoe-ppp-ethernet/ la date de creation de document le 07 decembre 2004

[34] : Mémoire presenté par Willam Landry pour l'obtention du diplôme Master en informatique option administration reseau en 2009 sur le théme de « mise en place d'une architecture VPN MPLS avec gestion du temps de connexion et de la bande passante utilisateur

[35] : Securité SOA niveau transport sur le lien web :http://soaj2ee.blogspirit.com/archive/2005/12/14/securite-soa-niveau-transport.html dans le nom l'architecture orientés Services et J2EE par Ahmed Alami en 14-12-2005

[36] : VPN :sur le lien :http://www.frameip.com/vpn/ par Thomas Klein ET Sebf la date de creation et le 15 janvier 2007

[37] :un exposé realisé par Ben Haddou Mina et Duquenne Wilfried et Clercq Sylven en 14 Décembre 2004 sur le titre de « Réalisation d'un client serveur d'échange de paquets entre deux sous réseaux reliés par un VPN .

[38] : Documentation faite par Guillon Smuel et Roben David et FI/EP en 2005 dur le titre RSVP-TE d'édition Telecom Lille

[39] : Poly JL Langlois sur MPLS –GMPLS sur le lien : http://www.licm.fr/IMG/pdf/chapitreMPLS-GMPLS.pdf

[40] : Multi Protocol Label Switching sur le site web :http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2001/Benduduh-Fourcade/introduction-MissionMPLS/introduction-MissionMPLS.htm par Bendella Bneduduch et Jean Marc Fourcade d'édition :Telecom Lille en 2009

[41] :MPLS sur la page web: http://www.frameip.com/mpls/ par Bneduduch et Jean Marc Fourcade le document a crée en 2001

[42] : Introduction a MPLS sur :http://www.guill.net/index.php?cat=3&pro=3&wan=5 dans Guill.net crée en 2005

[43] : VPN sur :http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2001ttv02/Roudel_Maroc/index.htm par Philippe Roundel et Alain Maroc en Janvier 2002 d'edition Telecom LILLE

[44] : mémoire réalisé par Amine Amine étudiante a l'université de Bechar pour le grade de Technicien supérieur de maintenance de réseaux en 2011 sur le thème « Mise en œuvre d'un cœur de réseau IP/MPLS »

[45] :Multi Label Protocol Label Switching sur la page web : http://www-igm.univ-mlv.fr/~dr/XPOSE2006/marot/architecture.html par Yazzid Kahroub

[46] : Thèses présenté par Mohamed Yazid Saidi –l'université de Rennes- pour l'obtention du grade Docteur en informatique le 28 novembre 2008 sur le théme « Méthode de contrôle distribué du placement de LSP de secours pour la protection des communications unicast et multicast dans un réseau MPLS

[47] : exposé sur MPLS présenté par Antoine Versini en 13 Février 2004 d'edition T-Online

[48] : un article sur MPLS par François Spies de l'université de Franche-Comté en 2009

[49] : Quelques éléments de sécurité des réseaux privés virtuels MPLS/VPN en 10-10-2008

Sur le lien : http://www.unixgarden.com/index.php/misc/quelques-elements-de-securite-des-reseaux-prives-virtuels-mplsvpn

[50] : Avantages des VPN BGP MPLS surréseaux privé Virtuels VPN BGP /MPLS,le lien http://www.brimbelle.org/mattieu/projects/bgpmpls/avantages.htm en 2008 par Mattieu Baptiste et Fabien Viencent-Option RIO-Telecom.LILLE 1

[51] : Thèses présenté par Zamouche Fres Mounir pour l'obtention du diplôme Magister en Informatique, le thème : « Conception d'un serveur de politiques QOS via le système MAUDE » a l'université de Constantine en 2009

[52]: Thèse présenté a l'université de Bordeaux I'école doctorale de mathématiques et d'informatique par Bader Benmmar le 12 ai 2006 avec le thème « La gestion dynamique de la qualité de service dans les réseaux IP mobiles

[53] : Un rapport de recherche par David FUIN et Eric Garcia en 2004 sue « Qualité de service dans les réseaux Actifs »

[54] : Mémoire d'habilitation a Diriger de recherché sur le thème « Architecture des réseaux pour le contrôle de la QOS par Oliver Dugeon en décembre 2008 pour l'obtention du diplôme Ingénieur de recherche a Orange Labs .

[55] : un rapport final dur les réseaux IP :Tarification des services de télécommunication en 2003 dans le bureau de développement des télécommunications dans l'union Internationale des télécommunications .

[56] :Mémoire de DEA a l'université de Franche Comté sur le titre « QOS dans les réseaux actifs » présenté par David Fuin, Eric Garcia et Hervé en 2004 .

[57] :thèse présenté par Antoine Mnhule pour obtenir le grade de docteur d'université en informatique sur le thème « Apprentissage de la qualité de service dans les réseaux multiservices :applications au routage optimal sous contraintes » -novembre 2005-

[58] :thème pour l'obtention du diplôme Master informatique 2011 a université Avignon avec le thème « simulateur Interactif de QOS »

[59] : DiffSERV sur Guill.net la derniere modification le 25 janvier 2007 sur la page : http://www.guill.net/index.php?cat=3&pro=3&wan=6

[60] : thèse présenté devant l'université de Rennes 1 pour obtenir le grade de docteur de l'université de Rennes 1 Mention informatique par Yazid Mohaned Saidi titre de la thèse « Méthodes de contrôles distribué du placement de LSP de secours pour protection des communications unicast et multicast dans un réseau MPLS » en 2008

[61] : these pour obtenir le titre de Docteur en sciences de l'université de Nice –Sophia Antipolis presenté par Marie(Emilie Voge sur le titre « Optimisation des réseaux de télécommunications :Réseaux multi niveaux ,Tolérance aux pannes et surveillance du trafic

[62] : Rapport de fin d'étude pour l'obtention du diplôme Ingénieur sur le titre « Analyse des performances de MPLS en terme de TE dans un réseau Multiservices » présenté par Oussama Foudhaili en 2004 .

[63]; Ellen W. Zegura Samrat Bhattacharjee, Kenneth L. Calvert. Congestion control and caching in canes. *ICC'98, Atlanta, GA*, 1998.

[64];Projet sur la QOS et les reseaux IP fait par Samir Mohamed et Genardo Rubino et Martin Varela

[65] : Omar Cherkaoui Mauro Fonseca, Nazim Agoulmine. Active networks as a flexible approach to deploy qos policy based management. *HP Openview University Association 8th Annual Workshop, HP-OVUA, Berlin, Germany*, 2001

D. Alexander, W. Arbaugh, A. Keromytis, S. Muir, and J. Smith. Secure quality of service handling : Sqosh, 2000.

[66]: Florian Baumgartner. *Quality of Service Support by Active Networks*. PhD thesis, Institute if Computer Science and Applied Mathematics, University of Berne, Februar 2002.

[67]: Florian Baumgartner and Torsten Braun. Quality of service and active networking on virtual router topologies. *Active Networks, Second International Working Conference, IWAN 2000, Tokyo, Japan, October 16-18, 2000, Proceedings*, 1942, 2000.

[68] : Rima Kilany Eric Horlait, Nicolas Rouhana. An implementation of differentiated services using active networks. *IEEE Workshop on Networking, Beyrouth, Liban*, 1999.

[69]: Giuseppe Di Fatta, Salvatore Gaglio, Giuseppe Lo Re, and Marco Ortolani. Adaptative routing in active networks. *IEEE Third Conference on Open Architecture and Network Programming, OpenArch 2000, Tel Aviv*, March 2000.

[70] : Ian W. Marshall and Chris Roadknight. Provision of quality of service for active services. *Computer Networks (Amsterdam, Netherlands : 1999)*, 36(1) :75–85, June 2001.

[71] : Documentation sur l'introduction au routage dynamique avec OSPF par Philippe Latu en 2001

[72]: Rapport sur Eigrp and OSPF comparaison par Scott Hogg en mars 2002 .

[73]: tutoriel GNS 3 –Installation et configuration par Cisco

[74] :tutoriel sur Wireshark sur Depnmanik.com