REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
Faculté de Génie Electrique et Informatique
Département d'Electronique

Mémoire de fin d'étude

En vue de l'obtention du diplôme de Master en Electronique.
OPTION : Réseaux et Télécommunications.

THEME

Mise En Œuvre D'un Cœur D'un Réseau IP/MPLS : Cas ATM Mobilis

Réalisé par :

- M^lle^ AOUSSAT Sarah Zahoua
- M^lle^ CHERRAK Lilia

Dirigé par :

Mr ACHOUR Hakim

Encadré par :

Mr ZIER Abdenour

Promotion: 2012-2013

Dédicaces

Je dédie ce modeste travail

À La mémoire de mon très cher père et à ma très chère maman que Dieu me la protège

À Mes très chères frères et sœurs

À Mes aimables nouveaux et nièces

À Mon binôme et tous mes amis

LILIA

DEDICACES

Je dédie ce modeste travail à mes chers parents et sœurs

que DIEU me les garde

À ma famille, mes amis et toutes les personnes qui m'ont

soutenue et qui ont été toujours là pour moi

À mes cousins et mon binôme

SARAH -ZAHOUA

REMERCIMENTS

Nous rendons grâce à DIEU, de nous avoir accordé le courage et la patience jusqu'à l'aboutissement de nos études et l'accomplissement de ce modeste travail.

Nous tenons à adresser nos vifs remerciements à tous ceux qui, de près ou de loin, ont contribué à l'élaboration de ce présent mémoire et au bon déroulement de notre stage pratique.

Nos remerciements sont adressés tout particulièrement à notre promoteur ***Mr ACHOUR*** *qui nous a beaucoup aidées.*

Nos remerciements les plus sincères vont en faveur du personnel de la Direction générale ***d'ATM Mobilis*** *particulièrement* ***Mr ZIER*** *notre encadreur de nous avoir accueillies en tant que stagiaires, et au personnel de la direction des systèmes Réseaux et Informatique pour leurs aide et assistance tout au long de notre stage.*

LISTE DES FIGURES

Liste des Abréviations

[A] **AAL**: ATM Adaptation Layer

ATM: Asynchronous Transfer Mode

AS :Autonomous System

[B] BGP:Border Gateway Protocol

BICC :Bearer Independant Call Control

[C] CE:Customer Edge (router)

CIDR: Classless Inter-Domain Routing

CoS: ClassesOF services

CLP:Cell Loss Priority.

CR-LDP:Constraint-based Routing over Label Distribution Protocol

CR-LDP LSP:Constraint-based Routing over Label Distribution Protocol Label Switched Path

CR-LSP:Constraint-based Routing - LSP

CSCF:Call Session Control Function

CSPF:Constrained Shortest Path First

[D] DiffServ : Differential Services

[E] eBGP :exterior Border Gateway Protocol

EIGRP :Enhanced Interior Gateway Routing Protocol

ELSR : Edge Label Switching Router

ER-LSR :Explicit Routing – LSP

ERO :Explicite Route Object

[F] FEC : Forwarding Equivalence Class

FIB:Forwarding Information Base

FR:Frame Relay

FTP:File Transfer Protocol

[G] GFC :Generic Flow Control.

GMPLS: Generalized MPLS

[I] iBGP :interior Border Gateway Protocol

IETF: Internet Engineering Task Force

IGP : Interior Gateway Protocol

IntServ: Integrated Services

IP: Internet Protocol

IPv4:Internet Protocol version 4

IPv6 :Internet Protocol version 6

IOS ..... ;

IS-IS: Intermediate System-to-Intermediate System

[L]LDP:Label Distribution Protocol

LER: Label Edge Router

LFIB : Label Forwarding Information Base

LIB: Label Information Base

LSP: Label Switched Path

LSP-TE: Label Switched Path – Traffic Engineering

LSR: Label Switch Router

[M] MAC: Medium Access Control

MCU: Multipoint Contrôler Unit

MGC: Media Gateway Controller

MGW: Media Gateway

MGCP: Media Gateway Control Protocol

MP-BGP: Multi Protocol Border Gateway Protocol

MPLS: Multi Protocol Label Switching

MPLS-TE: Multi Protocol Label Switching - Traffic Engineering

MPLS TE LSP: Multi Protocol Label Switching - Traffic Engineering- Label Switched Path

[N] NGN: Next Generation Networks

[O] OSI: Open Systems Interconnection

OSPF: Open Shortest Path First

[P] P: Provider (router)

PDU: Protocole Data Unit

PE: Provider Edge (router)

PPP: Point-to-Point Protocol

PT: Payload Type

[Q] QoS: Quality of Service

[R] RD: Route Distinguisher

RIP: Routing Information Protocol

RSVP: Resource Réservation Protocol

RSVP TE: Resource ReSerVation Protocol - Traffic Engineering

R T: Route Target

RTC: Réseau Téléphonique Commuté

[S] SIGTRAN: Signalling Transport

SI: Session Initiation Protocol

SIP-T: SIP pour la téléphonie

SNA: Systems Network Architecture

SPF: Shortest Path First

[T] TC: Transmission Convergence

TCP: Transmission Control Protocol

TDM: Time Division Multiplexing

TDP: Tag Distribution Protocol

TE : Traffic Engineering

ToS: Type of Service

[U] UDP: User Datagram Protocol

UIT : Union Internationale des télécommunications

[V] VC: Virtual Channel

VCI: Virtual Channel Identifier

VoATM: Voice over ATM

VoIP: Voice over IP

VPI : Virtual Path Identifier

VPN: Virtual Private Network

VRF: VPN Routing and Forwarding

WAN: Wireless Area Network.

SOMMAIRE

Historique :

ATM MOBILIS a été créée le 3 Août 2003 sous forme d'entreprise publique économique/société par action (EPE/SPA). Il s'agit d'une filiale d'Algérie Télécom dont les actions sont détenues à 100% par Algérie Télécom.

Elle est immatriculée au registre de commerce et ses organes sociaux (Assemblée Générale et conseil d'administration) ont été installés. ATM MOBILIS est la raison sociale de la société, le nom MOBILIS a été choisi comme marque commerciale.

Son objet est l'installation et l'exploitation de réseaux de téléphonie mobile, développement, vente de services de téléphonie mobile, maintenance et montage d'équipements de téléphonie mobile.

Statut juridique :

Dénomination Siège : Son siège est situé à quartier des affaires BAB EZZOUAR, Alger. Avec un effectif de 4100 employés en décembre 2012, elle a pour principal objet l'exploitation des services de la téléphonie mobile.

Capacité technique et offre de MOBILIS :

Mobilis exploite un réseau qui couvre 48 Wilayas par plus de 2900 Stations de base. Ses offres actuelles sont :

- des offres postpayées et prépayées.

- la fonction Roaming international avec les opérations des pays les plus importants pour le client Algérien.

- des services complémentaires (SMS, Messagerie Vocale, Data- Fax, double appel...).

Mobilis en Chiffres clefs :

- Part de marché : 36%
- Couverture : 97,6 %
- Effectifs : 4100
- Distributeurs : 5

- Réseau commercial (points de vente) : 6000

Les structures organisationnelles de MOBILIS :

Les structures des entreprises varient en fonction de la taille de l'entreprise, son historique, son domaine d'activité et la personnalité de ses dirigeants. Si les choix différents dans l'attachement des différents services aux différentes directions, les rôles exerces et les missions remplies restent les mêmes.

L'organigramme de Mobilis se présente comme suit :

***Trois grandes divisions :**

- La Division Réseau et Service (DVRS) ;
- La Division Commerciale et Marketing (DVCM) ;
- La Division Affaire Générales (DVAG).

***Des directions rattachées directement au PDG :**

- Direction de la marque et de la communication ;
- Direction de la stratégie, programmation et performance ;
- Direction des finances et de la comptabilité ;
- Direction du système d'information.

*** Directions régionales :** au nombre de huit (8) rattachées elles aussi au PDG, et qui sont :

Alger, Chlef, Oran, Setif, Constantine, Annaba, Bechar, Ouargla.

- **La Direction Générale :**

La direction générale est dirigée par un président directeur général qui est assisté par des conseillers dans les différents domaines d`activités à savoir, la technique, ressources humaines, finance, juridique, et affaires générales.

Les Divisions Mobilis :

Afin de pouvoir mener les politiques complexes coordonnées au niveau des directions, tout en garantissant une prise en charge opérationnelle de bon niveau par les structures attachées, Mobilis a opté à la mise en place de divisions managerielles regroupent l´autorité et le savoir faire, et dont les rôles à tenir et à découdre.

La Division Réseau et Service (DVRS):

La responsabilité de la DVRS est de manager la cohérence des quatre Directions opérationnelles qui portent ces 4 fonctions :

- Ingénierie
- Transmission
- Déploiement des infrastructures
- Maintenance des infrastructures

La Division Commerciale et Marketing (DVCM) :

La fonction de la DVCM est de manager en cohérence les 3 directions opérationnelles qui concourent à l'exploitation du marché Grand Public, qui portent les 3 fonctions suivantes :

- Ventes/Distribution
- Marketing
- Relation Clients
- Marque et Communication

Elle assure aussi le management global de la Direction du marché Entreprises, pour valider ses choix, et cherche quand cela est opportun, à optimiser, minimiser les moyens entre marché Grand Public et Marché Entreprises

La division est directement responsable de la part de marché sur chaque marché et segment, et de la rentabilité atteinte sur chaque Marché.

La Division Affaire Générales (DVAG)

La division des affaires générales (DVAG) assure le management d'un ensemble de directions au charge de fonctions supports dont certaines ont un contenu management important qui conditionne la Performance générale de l'ensemble des autres divisions et directions : DRH,DFO,DDQ**La direction des finances et comptabilité :**

Elle est reliée directement au PDG et est constituée des sous directions comptabilité, budget, finance.

Le cas pratique sera traité au niveau de la sous direction des finances, département finance qui se charge des contrats et des lettres de crédit, et le service roaming chargé du transfert libre.

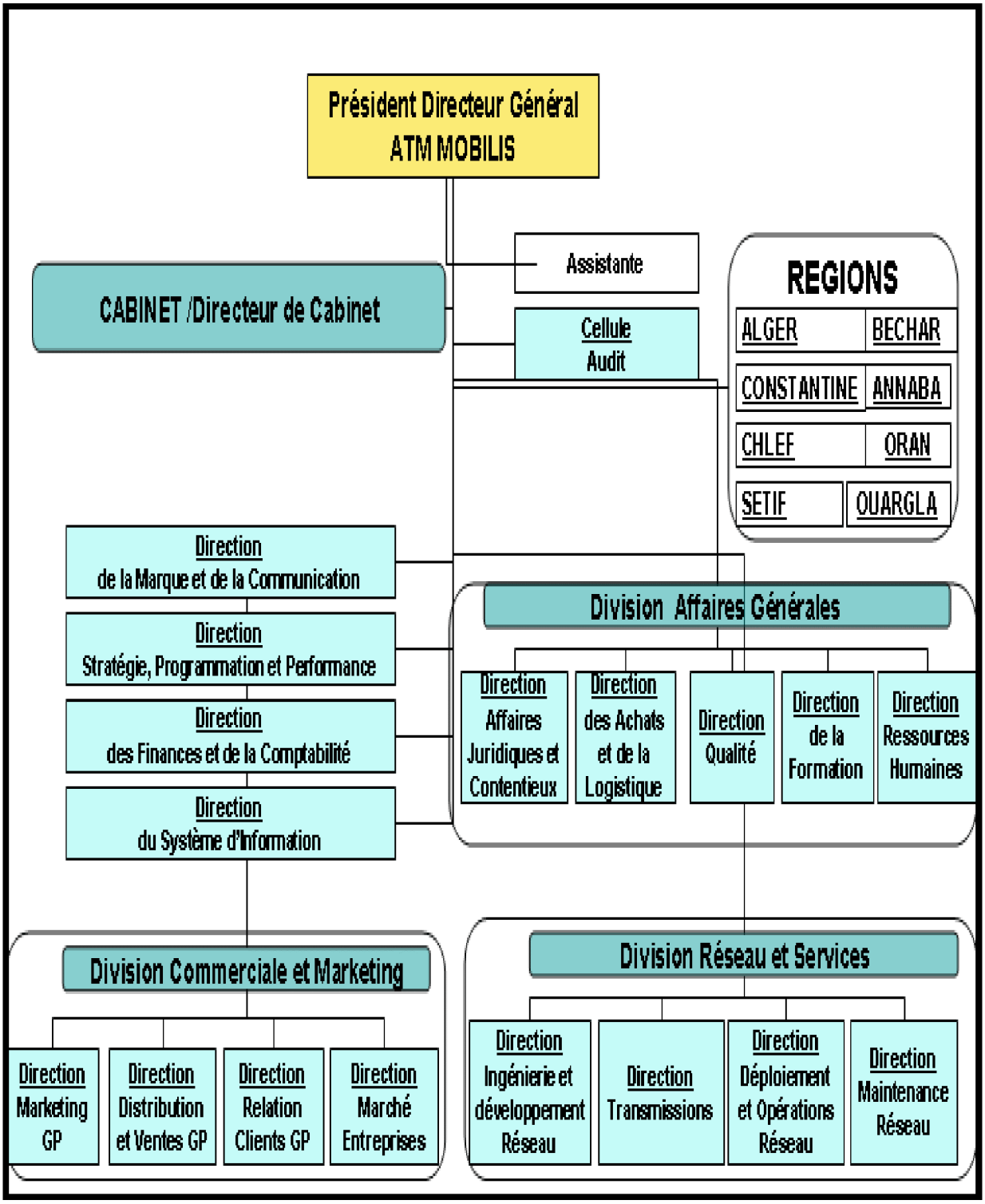


Figure : L'organigramme général de MOBILIS

L'informatique, et plus particulièrement les réseaux, ont beaucoup évolué durant ces dix dernières années. Les flux d'informations ont considérablement progressé et il est désormais possible de s'échanger des données conséquentes de tous types ainsi que de faire transiter de la voix sur des réseaux informatiques.

Ce qui a fait d'IP un protocole presque universel. Le succès de ce dernier repose sur sa grande simplicité puisqu'il se base sur le modèle *Best Effort*. Toutefois, ce même point qui a fait sa force, constitue actuellement sa faiblesse le modèle *Best Effort* a montré ses limites face aux nouveaux besoins des applications, puisque la demande s'est diversifiée (data, voix, vidéo, etc.) et les services sont de plus en plus gourmands en ressources. Les nouvelles applications exigent aujourd'hui de complexifier les réseaux et de prendre en compte les spécifications propres à chacune d'elles pour qu'elles puissent fonctionner correctement. En, d'autres termes, il est primordial d'instaurer la notion de la Qualité de Service (QoS) dans les réseaux télécom. La réponse à la question de QoS a été pour longtemps ATM"Asynchronous Transfer Mode". Car l'aspect non connecté d'IP rend difficile d'envisager de lui intégrer des services temps réel. d'un autre côté, les réseaux IP ont pris une ampleur tellement grande qu'on ne peut plus envisager de créer une architecture nouvelle répondant aux besoins de QoS. Et même l'association IP/ATM a montré ses limites. La solution est alors de définir des mécanismes complémentaires au fonctionnement de IP de base, permettant de prendre en compte les exigences propres de chaque type de service. Ceci quitte à introduire une complexité supplémentaire au fonctionnement d'IP.

C'est là que MPLS (Multi Protocol Label Switching) s'est imposé comme une solution leader. MPLS a réussi à conjuguer la simplicité d'IP avec l'efficacité d'ATM dans la gestion du multiservice.

MPLS fait également partie d'un mouvement d'ensemble vers les NGN (Next Generation Networks) dont le but est de réaliser la convergence voix/données dans une perspective générale de "tout IP" (EoIP : Everything over IP). MPLS est donc une solution prometteuse parce qu'elle permet d'intégrer très facilement de nouvelles technologies dans un cœur de réseau existant.

L'architecture MPLS est issue de plusieurs années de recherches, effectuées par différents acteurs du monde des réseaux informatiques, dans le but d'optimiser ces réseaux. En effet, le MPLS simplifie et améliore le transfert de paquets IP et apporte aux opérateurs une capacité accrue de gérer le trafic et d'éviter les congestions ou les goulets d'étranglement. Alors que cette récente technologie est proposée par de nombreux opérateurs, les clients commencent à migrer leurs réseaux existants vers ce type d'architecture fiable et sécurisée.

Dans le cadre de notre mémoire de fin d'études, il nous a été demandé de développer et mettre en œuvre un cœur de réseau basé sur une plateforme IP/MPLS pour la société ATM Mobilis. La mise en œuvre se fera dans un premier lieu, par une implémentation de la plateforme IP/MPLS sous GNS3. Aussi, nous avons partagé notre mémoire en 5 Chapitres. Après une introduction aux réseaux de nouvelle génération (NGN), le deuxième chapitre sera consacré aux différents protocoles de commutation existants et aux exigences qui ont poussés à l'évolution vers une dorsale IP/MPLS. Le troisième chapitre quand à lui, est une présentation des concepts de base de la technologie MPLS et leur mécanisme de fonctionnement. Le quatrième chapitre portera sur les applications offertes par MPLS. Enfin, le cinquième chapitre est dédié à l'élaboration et implémentation de la plateforme IP/MPLS sous GNS3.

Introduction:

De nos jours, on constate que le trafic de données prend le pas sur le trafic vocal et la tendance est l'augmentation de la bande passante, ce qui a permis aux operateurs possèdent ces deux types de réseaux à utiliser cet argument pour commencer à les unifier. D'ou la convergence entre la voix, données, vidéo.

Conséquence : la migration des réseaux actuels vers NGN.

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

Ce premier chapitre est consacré à la présentation des réseaux de nouvelle génération. Nous sommes intéressées à l'architecture des réseaux NGN, aux différents éléments qui le composent ainsi qu'aux différents protocoles en concurrence.

I-1 Définition NGN:

Le réseau NGN est défini par l'union internationale des télécommunications(UIT) comme un réseau en mode paquet, en mesure d'assurer des services de télécommunication et d'utiliser de multiples technologies de transport à large bande a qualité de service imposée et dans lequel les fonctions liées aux services sont indépendantes des technologies sous jacentes liée au transport.

I-2 Converger vers le NGN:

Dans certaines parties du monde, le trafic de données prend rapidement le pas sur le trafic vocal et la tendance est nettement à l'augmentation en bande passante pour les données, tandis que la voix peut se satisfaire d'une bande passante de 64 kbit/s, voire moindre. Les opérateurs possédant les deux types de réseaux (réseau voix et réseau de données) utilisent cet argument pour commencer à les unifier. Il est clair d'après les limites du réseau TDM (Time Division Multiplexing) que le réseau de données survivra alors que le réseau TDM quittera la scène .Facteur non moins important : le nouveau besoin chez les usagers d'une variété encore plus grande d'applications et de services sophistiqués (Push-to-talk, conférence audio et vidéo, messagerie unifiée, chat) dont la plupart n'étaient même pas envisagés lors de la conception des réseaux actuels.

Pour les opérateurs, l'accès et le transport ne sont plus assez lucratifs et, pour rester compétitif, il leur faudra donc offrir aux usagers toute une gamme de services utiles, faciles à utiliser et rémunérateurs. Par conséquent, les NGN seront axés sur les services, et fourniront tous les moyens nécessaires pour en offrir de nouveaux et adapter les existants pour augmenter les recettes.

Les causes de convergence des réseaux Next Generation Networks (NGN):

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

I-3 Caractéristiques des NGN :

Les principales caractéristiques des réseaux NGN (Next Génération Networks) résident dans l'utilisation d'un réseau unique de transport en mode paquet (IP, ATM,…) et de la séparation des couches de transport des flux et de contrôle des communications sont implémentées dans un même équipement.

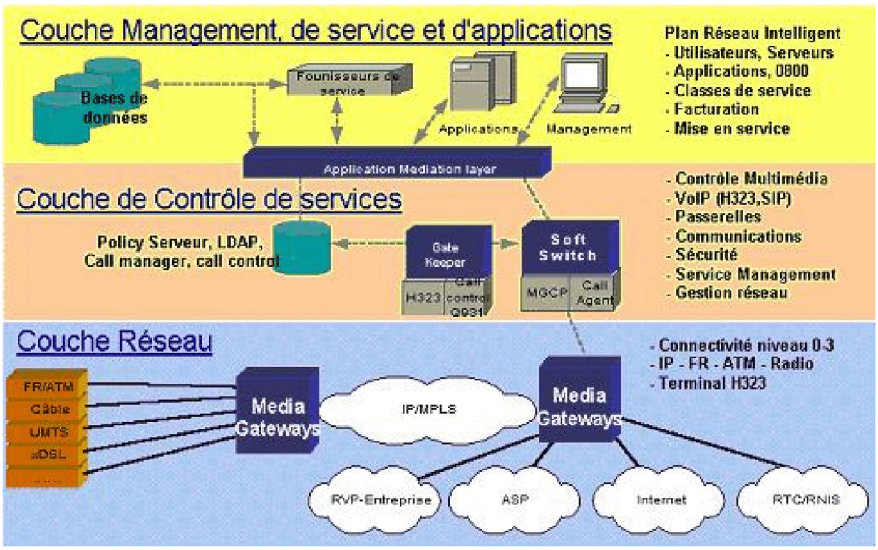


Figure I-1 : Modèle NGN

Une des caractéristiques principales du modèle NGN est de dissocier les services des réseaux physiques. Chaque élément fonctionnel d'une couche peut être offert séparément et peut évoluer indépendamment.

Les éléments fonctionnels qui constituaient un commutateur classique ont été séparés suivant leur fonction primaire en couches différentes :

• une couche avec les fonctions de transport
• une couche avec les fonctions de contrôle de service
• une couche de management, service et application.

Les éléments fonctionnels communiquent via des interfaces ouvertes qui peuvent être des protocoles normalisés.

I-4 Types de NGN :

Il existe trois types de réseau NGN : NGN class 4, NGN Class 5 et NGN Multimédia.

Les NGN Class 4 et Class 5 sont des architectures de réseau offrant uniquement les

Services de téléphonie .Il s'agit donc de NGN téléphonie .Dans le RTC (Réseau Téléphonique Commuté), un commutateur class4 est un centre de transit. Un commutateur Class5 est un commutateur d'accès aussi

appelé centre à autonomie d'acheminement. Le NGN class4 (respectivement. NGNclass5) émule donc le réseau téléphonique au niveau transit (respectivement. au niveau accès) en transportant la voix sur un mode paquet.

Le NGN Multimédia est une architecture offrant les services multimédia (messagerie vocale/vidéo, conférence audio/vidéo, Ring-back tone voix/vidéo) puisque l'usager a un terminal IP multimédia. Cette solution est plus intéressante que les précédentes puisqu'elle permet à l'opérateur d'innover en termes de services par rapport à une solution NGN .

La Class 4 NGN permet :

- Le remplacement des centres de transit téléphoniques (Class 4 Switch).
- La croissance du trafic téléphonique en transit.

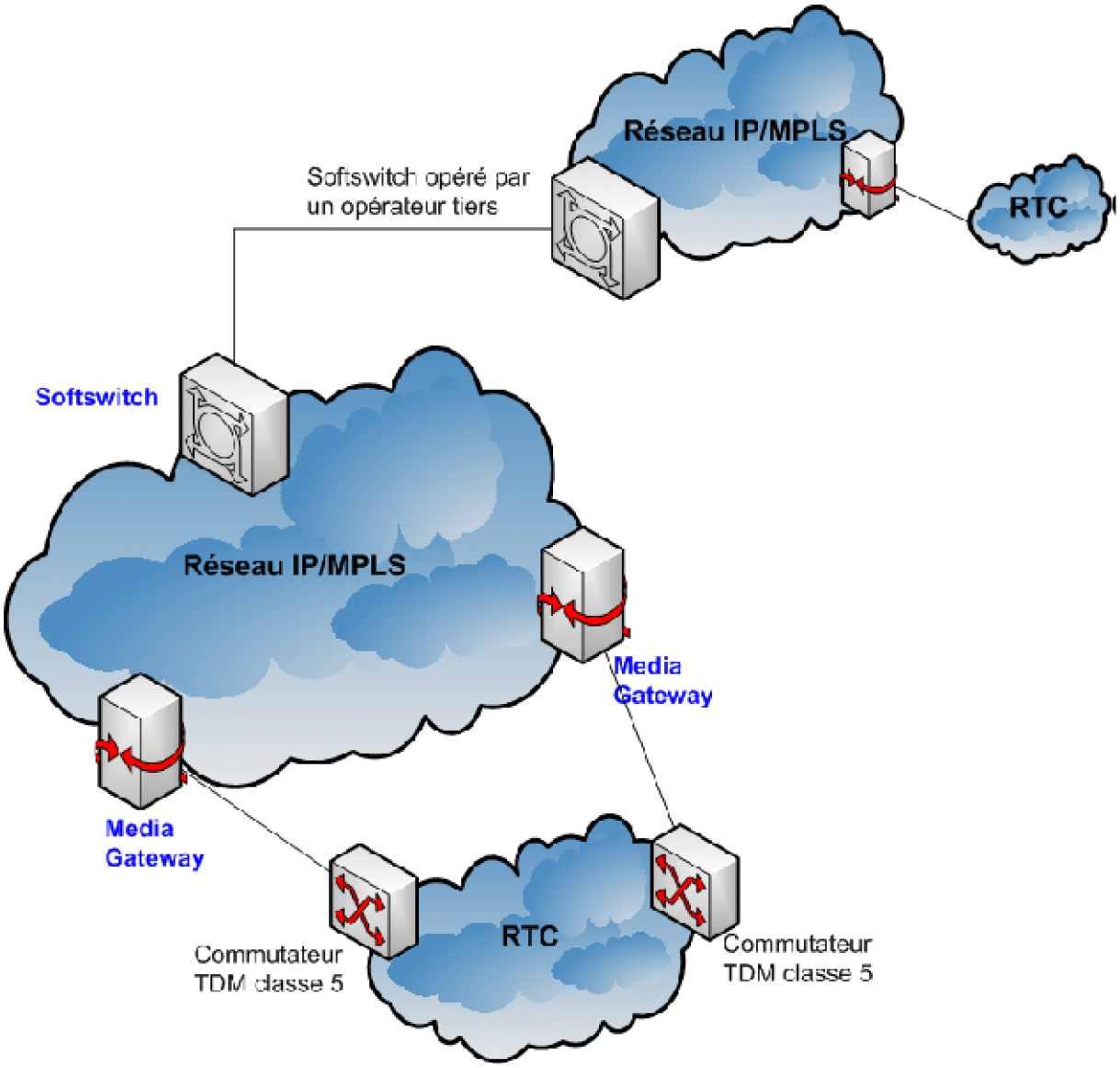


Figure I-2 : Architecture d'une solution NGN de classe 4

La Class 5 NGN permet :

- Le remplacement des centres téléphoniques d'accès(Class5Switch)
- La croissance du trafic téléphonique à l'accès
- La voix sur DSL/ Voix sur le câble

Le MultiMedia NGN permet d'offrir des services multimédia à des usagers disposant d'un accès large bande tel que xDSL, câble, Wifi/WiMax, EDGE/UMTS, etc.

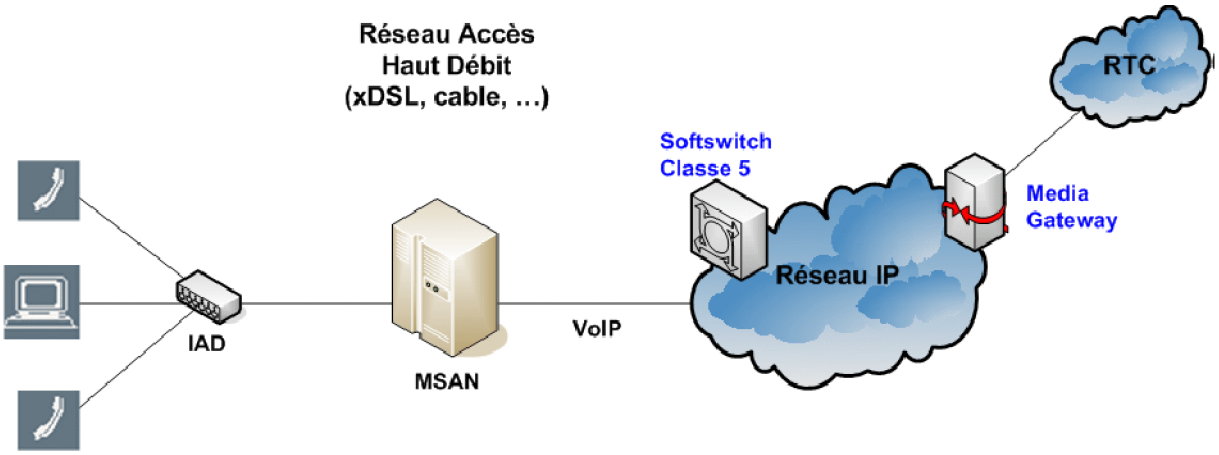


Figure I-3: Architecture d'un réseau NGN de classe 5

I-5 Avantages du NGN :

Grâce au NGN, l'opérateur dispose d'un réseau multiservice permettant d'interfacer n'importe quel type d'accès (Boucle locale, PABX, Commutateur d'accès téléphonique, accès ADSL (Asymmetric Digital Subscriber Line;), accès mobile GSM(Global System for Mobile Communications) ou UMTS(Universal Mobile Telecommunication System), téléphone IP(Internet protocol) etc.).

Cette nouvelle topologie offre les avantages suivants :

- L'opérateur n'aura plus à terme qu'à exploiter un seul réseau multiservice.
- Elle utilise le transport comme l'IP ou l'ATM ignorant les limites des réseaux TDM (Time Division Multiplexing) à 64 kbit/s. En effet le TDM perd son efficacité dès lorsque l'on souhaite introduire des services asymétriques, sporadiques ou à débit binaire variable.
- C'est une topologie ouverte qui peut transporter aussi bien les services téléphoniques que les services de multimédia (vidéo, données temps réel).
- Elle dissocie la partie support du réseau de la partie contrôle, leur permettant d'évoluer séparément et brisant la structure de communication monolithique. En effet, la couche transport peut être modifiée sans impact sur les couches contrôle et application.
- Elle utilise des interfaces ouvertes entre tous les éléments, permettant à l'opérateur d'acheter les meilleurs produits pour chaque partie de son réseau.

I-6 Architecture de NGN en couches:

Le passage à une architecture de type NGN est notamment caractérisé par la séparation des fonctions de commutation physique et de contrôle d'appel. L'architecture NGN introduit un modèle en couches, qui scinde les fonctions et équipements responsables du transport du trafic et du contrôle. Il est possible de définir un modèle architectural basé sur cinq couches successives (cf. Figure 4) :

I-6-1 la couche d'accès :

Elle regroupe les fonctions et équipements permettant de gérer l'accès des équipements utilisateurs au réseau, selon la technologie d'accès (téléphonie commutée, DSL, câble). Cette couche inclut par exemple les équipements DSLAM fournissant l'accès DSL.

I-6-2 la couche de transport :

Elle est responsable de l'acheminement du trafic voix ou données dans le cœur de réseau, selon le protocole utilisé. L'équipement important à ce niveau dans une architecture NGN est le Media Gateway (MGW) et des Signalling Gateway(SGW) gèrent respectivement l'adaptation des protocoles de transport aux différents types de réseaux physiques disponibles (RTC, IP, ATM, …) et la signalisation aux interfaces avec les autres ensembles réseaux ou les réseaux tiers interconnectés.

I-6-3 La couche de contrôle :

Elle gère l'ensemble des fonctions de contrôle des services en général, et de contrôle d'appel en particulier pour le service voix. L'équipement important à ce niveau dans une architecture NGN est le serveur d'appel, plus communément appelé « softswitch », qui fournit, dans le cas de services vocaux, l'équivalent de la fonction de commutation dans un réseau NGN. Dans le standard IMS défini par le 3GPP, les fonctionnalités et interfaces du softswitch sont normalisées, et l'équipement est appelé CSCF (Call Session Control Function).

I-6-4 La couche d'exécution des services :

Elle regroupe l'ensemble des fonctions permettant la fourniture de services dans un réseau NGN. En termes d'équipements, Cette couche regroupe deux types d'équipement : les serveurs d'application (ou application servers) et le service contrôle point« enablers », qui sont des fonctionnalités, comme la gestion de l'information de présence de l'utilisateur, susceptibles d'être utilisées par plusieurs applications. Cette couche inclut généralement des

serveurs d'application SIP, car SIP (Session Initiation Protocol) est utilisé dans une architecture NGN pour gérer des sessions multimédias en général, et des services de voix sur IP en particulier.

I-6-5 La couche applications :

Cette couche applications regroupe l'environnement de création de services, qui peut être ouvert à des fournisseurs de services tiers. Le développement d'applications s'appuie sur les serveurs d'application et le service contrôle point de la couche d'exécution des services.

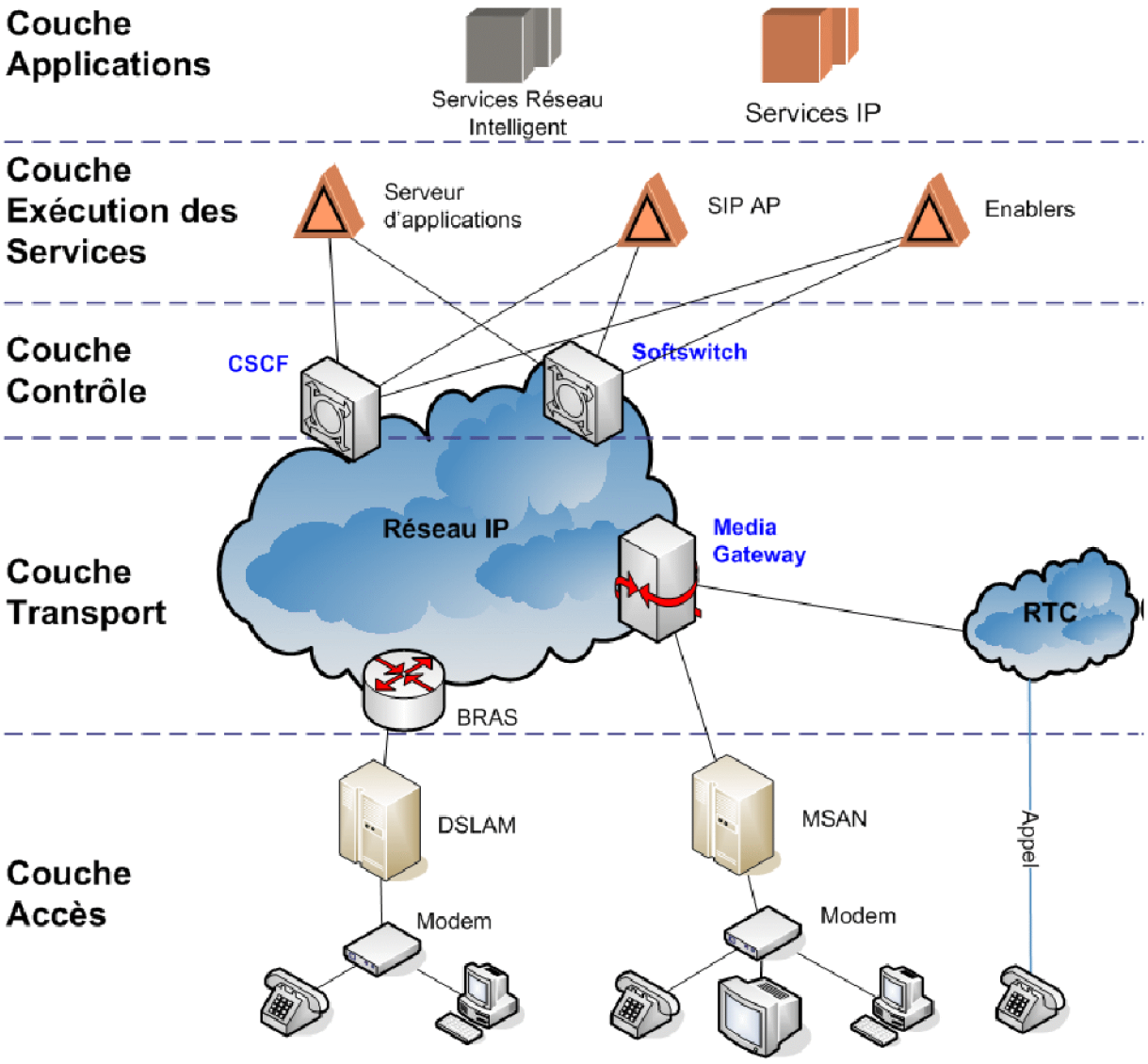


Figure I - 4 : Architecture générale d'un réseau NGN

I-7 Les principaux équipements du réseau NGN :

I-7-1 Rôle des media Gateway dans une architecture NGN :

Les media Gateway constituent un des éléments essentiels déployés dans un réseau NGN. Un media Gateway peut par exemple se positionner entre le réseau de commutation circuit et le réseau de commutation de paquets. Dans ce cas, les media Gateway transforment le trafic circuit TDM en paquets, la plupart du temps IP ou ATM, pour que ce trafic puisse ensuite être géré par le réseau NGN.

En conséquence, plusieurs types de media Gateway sont disponibles sur le marché, en fonction du type de solution voix choisie par l'opérateur et du rôle de ce media Gateway :

- les passerelles VoIP (Voice over IP) : pour convertir des lignes d'accès TDM en flux IP,
- les passerelles VoATM (Voice over ATM) : pour convertir des lignes d'accès TDM en flux ATM,
- les passerelles VoBB pour transformer des flux IP en signaux voix sur un réseau haut-débit câble ou DSL.

I-7-2 La Signalling Gateway (SG):

La fonction Signalling Gateway a pour rôle de convertir la signalisation échangée entre le réseau NGN et le réseau externe interconnecté. Elle assure l'adaptation de la signalisation par rapport au protocole de transport utilisé.

I-7-3 Media Gateway Controller (MGC) ou Softswitch:

Dans l'architecture des réseaux NGN, le serveur d'appel est le nœud central qui supporte l'intelligence de communication. Ce serveur est aussi appelé Softswitch ou Media Gateway Controller (MGC).

Il gère:

- L'échange des messages de signalisation transmise de part et d'autre avec les passerelles de signalisation, et l'interprétation de cette signalisation.
- Le traitement des appels : dialogue avec les terminaux H.323, SIP voire MGCP, communication avec les serveurs d'application pour la fourniture des services.
- Le choix du MG de sortie selon l'adresse du destinataire, le type d'appel, le charge du réseau.

• La réservation des ressources dans le MG et le contrôle des connexions internes au MG (commande des Media Gateways).

I-8 Les familles des protocoles d'un réseau NGN :

L'architecture de NGN est caractérisée par des couches qui sont interconnectées par des interfaces utilisant des protocoles standards. Le réseau TDM est interconnecté avec NGN grâce à des interfaces basées sur des protocoles.

Un protocole est une description formelle de règles et de conventions a suivre dans un échange d'informations que se soit pour acheminer les données jusqu'au destinataire ou pour que ce dernier comprenne comment doit il utiliser les données reçues.

Nous les classerons en trois grandes familles : les protocoles de contrôles d'appels qui regroupent essentiellement H.323 et SIP, les protocoles de media Gateway constitués par MEGACO et MGCP et les protocoles de signalisation entre MGC : BICC, SIP-T, SIGTRAN.

I-8-1 Les protocoles de contrôle d'appel :

Ils permettent l'établissement d'une communication entre deux terminaux et un serveur, les deux principaux protocoles concurrents sont H.323, norme de l'UIT et SIP standard développé à l'IETF (Internet Engineering Task Force) .étudions leur spécifications respectives :

a-H.323 :

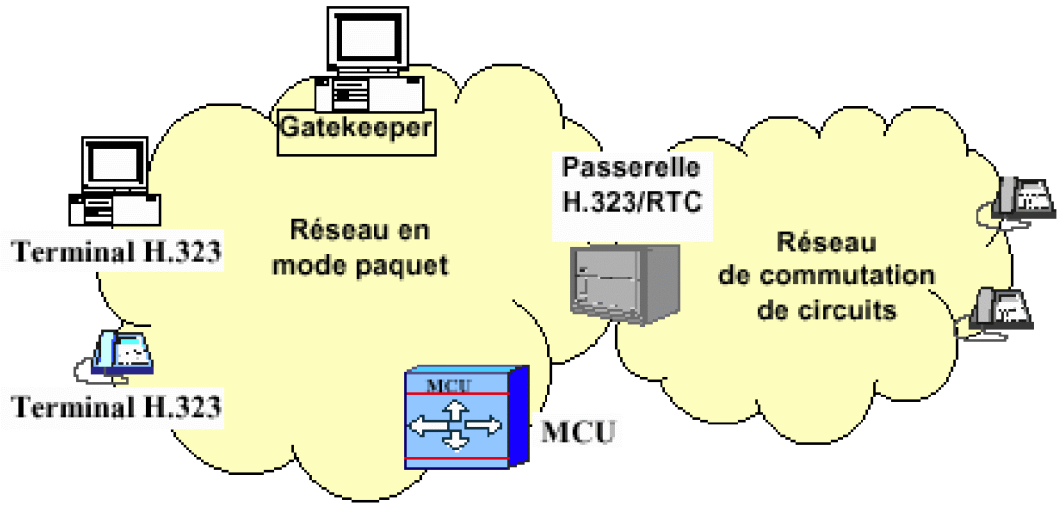


Figure I-5 : Architecture de H323

La recommandation H.323décrit les procédures pour les communications audio et vidéo sur des réseaux en mode paquet sans garantie de service.

Les principales entités nécessaires à la réalisation d'un service de communication multimédia sur des réseaux de donnes sont :

- Les terminaux H.323 qui sont des systèmes multimédia (téléphone, pc) permettent de communiquer en temps réel.
- Le Gatekeeper qui gère les terminaux H.323 (identification et traduction d'adresses) et l'établissement d'appels.
- La passerelle H.323ou Gateway qui permet d'interfacer le réseau IP avec le réseau téléphonique classique.
- L'unité de contrôle MCU (Multipoint Contrôler Unit) qui gère les connexions multipoint (ex. : appels de conférence).

b-SIP :

Le protocole SIP (Session Initiation Protocol) de l'IETF (Internet Engineering Task Force), est un protocole de signalisation applicatif (niveau 7) pour l'établissement, la modification et la terminaison des sessions multimédia sur Internet. Toute opération SIP se compose d'une série de messages (requête/réponse), SIP est un protocole de type Client/serveur.

SIP utilise le protocole SDP (Session Description Protocol) pour définir les attributs d'une session SIP.

Les fonctionnalités de SIP :

• Localisation du ou des participant(s) à la session.

• Etablissement et gestion de la session.

• Gestion de la disponibilité (mise en attente, transfert).

• Gestion des capacités (configuration, négociation des paramètres de la session, hétérogénéité des terminaux).

I-8 -2 Les protocoles de signalisation entre les softswitch :

L'interconnexion des réseaux de données avec les réseaux existants TDM utilisant la signalisation SS7, à nécessité le développement du protocole dédié a l'interconnexion des réseaux et aux transports de la signalisation SS7 sur les réseaux en mode paquet.

Ces protocoles permettant la gestion du plan contrôle, ce sont essentiellement :

- BICC (Bearer Independant Call Control), SIP-T (SIP pour la téléphonie) et H.323, au niveau du cœur de réseau.
- SIGTRAN (Signalling Transport), à l'interconnexion avec les réseaux de signalisation SS7, généralement via des passerelles de signalisation ou Signalling.

I-8-3 Les protocoles de commande de Media Gateway :

Les protocoles de commande de Media Gateway sont issus de la séparation entre les couches Transport et Contrôle et permet au Softswitch ou Media Gateway Controller de gérer les passerelles de transport ou Media Gateway. MGCP (Media Gateway Control Protocol) de l'IETF et H.248/MEGACO, développé conjointement par l'UIT et l'IETF, sont actuellement les protocoles prédominants.

I-8-3-1 Le Media Gateway Control Protocol (MGCP):

C'est un protocole défini par l'IETF, a été conçu pour des réseaux de téléphonie IP utilisant des passerelles VoIP. Il gère la communication entre les Media Gateway et les Media Gateway Controller. Ce protocole traite la signalisation et le contrôle des appels, d'une part, et les flux média d'autre part.

I-8-3-2 Le protocole alternatif : MEGACO/H.248 :

Le groupe de travail MEGACO (Media Gateway Control) a été constitué en 1998 pour compléter les travaux sur le protocole MGCP au sein de l'IETF. Depuis 1999, l'UIT et l'IETF travaillent conjointement sur le développement du protocole MEGACO/H.248 ; c'est un standard permettant la communication entre les Media Gateway Controller (MGC) et les Media Gateway (MG). Il est dérivé de MGCP et possède des améliorations par rapport à celui-ci :

- Support de services multimédia et de vidéoconférence.
- Possibilité d'utiliser UDP ou TCP.

- Utilise le codage en mode texte ou binaire.

Figure I-6: les familles de protocoles d'un réseau NGN

I-9 Les services offerts par le NGN :

Les NGN offrent les capacités en termes d'infrastructure de protocole et de gestion, de créer et déployer de nouveaux services multimédia sur des réseaux en mode paquet.

La grande diversité des services est due aux multiples possibilités offertes par les réseaux NGN en terme de :

- Support multimédia (données, texte, audio).
- Mode de commutation, unicast (commutation point à point), broadcast (diffusion).
- Mobilité (services disponibles partout et tout le temps).

I-9-1 La voix sur IP :

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

- La jeunesse des protocoles de signalisation (SIP, H.323, MEGACO) de voix sur IP et la gestion de la qualité de service qui commence seulement maintenant à être nature ne permettaient pas de déployer des services téléphoniques sur IP.
- Le seul fait de transporter de voix classique, les services associes a la voix sur IP n'ont pas encore la maturité nécessaire pour pousser l'évolution vers ces nouveaux réseaux.
- La nécessité d'interconnecter les réseaux IP aux TDM/SS7 implique des couts liés aux équipements d'interconnexion (passerelle) et le prix des terminaux IP (IP phone) annihile l'avantage financier apporté par le transport en IP.
- Les couts des terminaux IP reste encore supérieur à celui des équipements classiques (pas encore d'économies d'échelle suffisante).

Cependant l'évolution de la technologie et des protocoles et l'apparition des services au monde IP devraient permettre l'émergence de la voix sur IP. De plus, l'évolution des réseaux téléphoniques vers la voix sur IP.

I-9-2 La diffusion des contenu multimédia:

La diffusion de contenu multimédia regroupe deux activités ; l'une focalisée sur la mise enforme des contenus multimédia, l'autre centrée sur l'agrégation de ces divers contenus via des portails. Les outils technologiques, tels que le multimédia streaming (gestion d'un flux multimédia en termes de bande passante et de synchronisation des données) et le protocole multicast, doivent permettre de fournir un service de diffusion de contenu aux utilisateurs finaux.

I-9-3 La messagerie unifiée :

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

I-9-4 Le stockage de données :

L'augmentation de capacité des réseaux et la gestion des flux permettent de proposer des services de stockage de données, en tant que sauvegarde de données critiques sur des

sites protégés, mais aussi en tant qu'accès « local » à un contenu (serveur « proxy » ou « cache »).En effet, les volumes de données évoluant de façon exponentielle, la nécessité d'offrir les services à partir des serveurs « locaux » semble indispensable. Cet aspect semble notamment indispensable pour les applications de télévision interactive et de vidéo.

I-9-5 La messagerie instantanée:

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

I-9-6 Les services associés à la géolocalisation :

La possibilité de localiser géographiquement les terminaux mobiles a été rapidement perçue comme une source de revenus supplémentaires. En effet, la géo localisation permet de proposer aux utilisateurs finaux des services très ciblés à haute valeur ajoutée liés au contexte (exemple : horaire, climat) et au lieu. Actuellement plusieurs solutions techniques existent et sont même en cours d'implémentation dans les réseaux d'opérateurs mobiles. Cependant, si ces solutions offrent la capacité de localiser les terminaux mobiles, il n'existe pas encore d'interfaces permettant l'exploitation de ces données par les applications de services, ou de réelle volonté des opérateurs d'ouvrir leurs serveurs de localisation à des fournisseurs de services tiers, afin d'utiliser cette fonction de localisation comme « service capability server » (élément de base servant de support à la réalisation des services).

Conclusion:

L'objectif de se chapitre est de connaitre les principes sur lesquels sont fondés les NGN, les types des réseaux NGN existants ainsi que les différents services réellement pertinents dans ce cadre, sont des étapes nécessaires pour pouvoir comprendre les stratégies d'évolution des réseaux actuels fixes ou mobiles vers une architecture multiservice, le réseau NGN est en cours de déploiement à ATM Mobilis, le réseau NGN sera un système offrant des services multimédia en s'appuyant sur un réseau support mutualisé est caractérisé par plusieurs éléments essentiels.

INTRODUCTION:

Au cours du temps, de nombreux protocoles de communication ont été développés et implémentés, certains ont connu le succès, d'autres non. Durant les années 60 et 70, c'était commun pour les fabricants d'ordinateurs de développer leurs propres protocoles qui utilisaient leurs propres environnements et pas les autres. Pendant les années 70, IBM publia la première spécification d'architecture de communication de données dite ouverte sous le nom de SNA (Systems Network Architecture). C'est aussi dans les années 70 qu'une nouvelle spécification de protocole connue sous le nom de X25 naquit, introduite non pas par un constructeur d'ordinateur mais par une organisation de standardisation.

Dans ce chapitre nous allons décrire quelques technologies, leurs limites et développements, par la suite nous allons expliquer pourquoi on a convergé vers le standards MPLS.

II-1 le protocole X25:

II-1-1 Présentation du X25:

Pour la transmission des données, il existe plusieurs réseaux spécifiques, comme X25. Ces réseaux publics sont basés sur le protocole standard X25 qui règle les transferts de données. X25 est idéal pour relier des réseaux locaux. Il offre des temps d'établissement de liaisons rapides (inférieurs à une seconde), une très bonne qualité de transmission et des vitesses de transfert allant de 300 à 64Kbit/s.
X25 est particulièrement intéressant pour une entreprise dans le cadre de connexions internationales et lorsque les temps de connexions journalières atteignent plusieurs heures. Pour des transferts de durée moyenne, ce service représente une alternative aux modems et lignes téléphoniques automatiques ou louées.

II-1-2 Fonctionnement du X25 :

X25 est basé sur la notion de circuit virtuel. Le circuit virtuel est une relation logique établie par le réseau entre deux abonnés, pour transmettre, avec un haut degré de sécurité, des séquences de données, sans restriction de longueur ou de nature.

Il est appelé circuit virtuel car les circuits physiques empruntés par les paquets de données

d'un abonné, sont partagés par l'ensemble des communications. Les caractéristiques de transmission du circuit virtuel sont :

- possibilité d'échanges simultanés dans les deux sens, de suite de paquets constituant des messages de longueur variable.
- conservation de l'ordre de paquet.
- le contrôle du flux est effectué, ce qui permet à chaque correspondant d'asservir le débit de l'émission des messages.
- le circuit réalise l'adaptation de la longueur des paquets. Chaque correspondant peut utiliser des longueurs de paquets différentes.
- l'accès est multi voies : il permet à une installation connectée à TRANSPAC par une seule liaison physique de communiquer en même temps avec plusieurs correspondants (en utilisant plusieurs circuits virtuels).

Le circuit virtuel peut être commuté ou permanent :
Circuit commuté : il est établi et libéré à la demande de l'un ou l'autre des correspondants.

Circuit permanent : il est établi de manière permanente entre les deux abonnés.

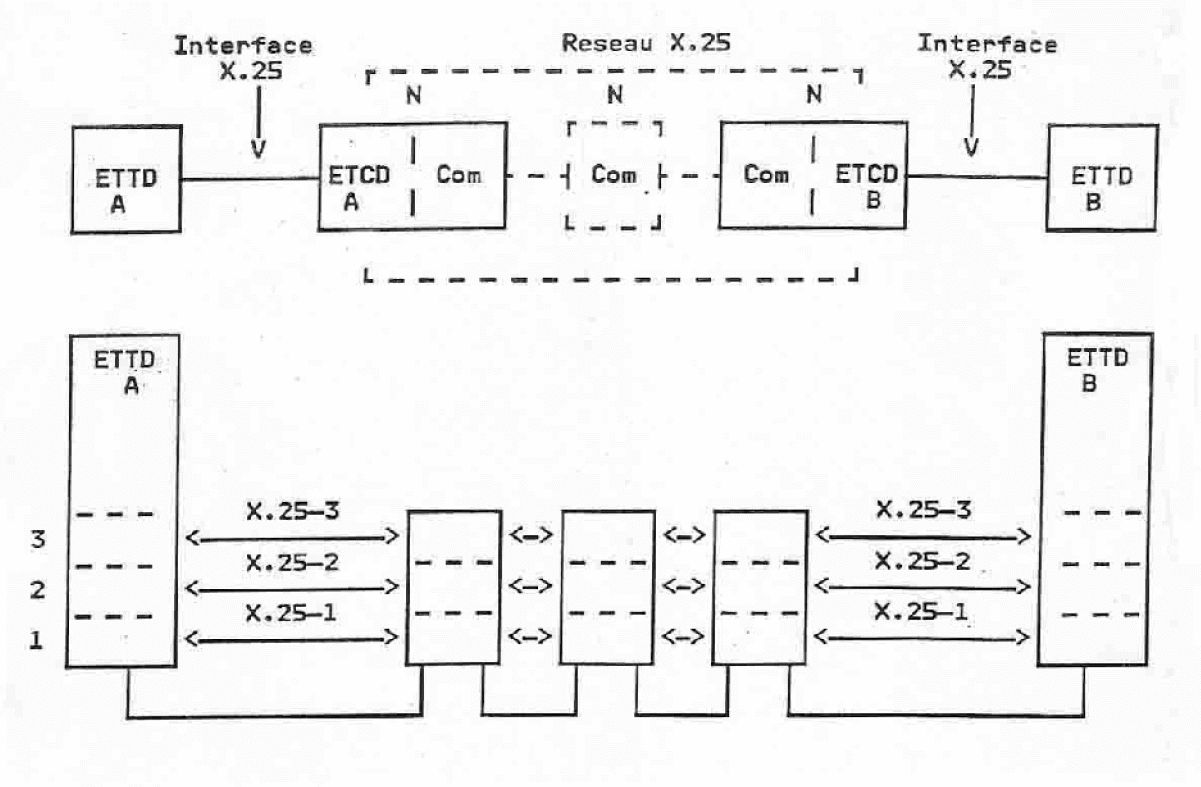


Figure II.1: architecture du protocole X25

II-1-3 Inconvénients x25 :

- Contrôles excessifs pour les lignes numériques actuelles.
- Complexité de la configuration du protocole, trop de paramètres.
- Sa lourdeur limite une bonne commutation purement hardware, commutation logicielle quasi obligatoire. Des performances plus restreint qu'ATM ou FR.

II-2 Commutation de trames (Frame Relay) :

II-2-1 Présentation du protocole frame Relay :

La commutation de trames est une méthode de transmission similaire à X25 et permet d'atteindre des vitesses de transferts de 2 Mbit/s. Alors que les réseaux X25 travaillent avec des longueurs des trames de données fixes, le protocole de commutation de trames utilise des trames de taille variable afin d'utiliser au mieux la bande passante du réseau. Cela permet de réduire la charge sur l'ensemble des branches du réseau. Contrairement à X25, la commutation de trames tourne sur le niveau 1 et 2 du modèle OSI (*Open Systems Interconnection*). De ce fait, elle n'ajoute pas de bits supplémentaires pour le contrôle, ce qui autorise des débits beaucoup plus rapides. Toutefois, cela suppose des terminaux suffisamment intelligents pour effectuer les contrôles d'erreur, lesquels se trouvent donc reportés à des couches supérieurs du modèle.

II-2-2 Fonctionnement Frame Relay :

L'enveloppe du paquet Frame Relay épouse idéalement le format des paquets Ethernet, IP ou SNA. L'effort d'encapsulation est minimum. La suppression du contrôle de flux a également une certaine répercussion sur le délai de transit. En effet, plus légers, les logiciels intégrés aux routeurs et commutateurs Frame Relay réduisent ce délai au sein de l'équipement. Celui-ci se contente de relayer la trame vers le nœud suivant ou sa destination finale.

En cas d'anomalie, les trames erronées sont abandonnées, les trames mal routées connaissent le même sort. Cette volonté de privilégier les performances par rapport à l'intégrité de la connexion table sur des infrastructures numériques fiables et des équipements d'extrémités autonomes, aptes à soulager le réseau d'un contrôle de flux laborieux. Installée aux extrémités, une procédure de transport de bout en bout, comme SNA ou TCP (*Transmission Control Protocol)*, se charge de rapatrier les trames manquantes. Libéré du

contrôle de flux, le protocole Frame Relay se prête plus facilement à l'allocation de bande passante.

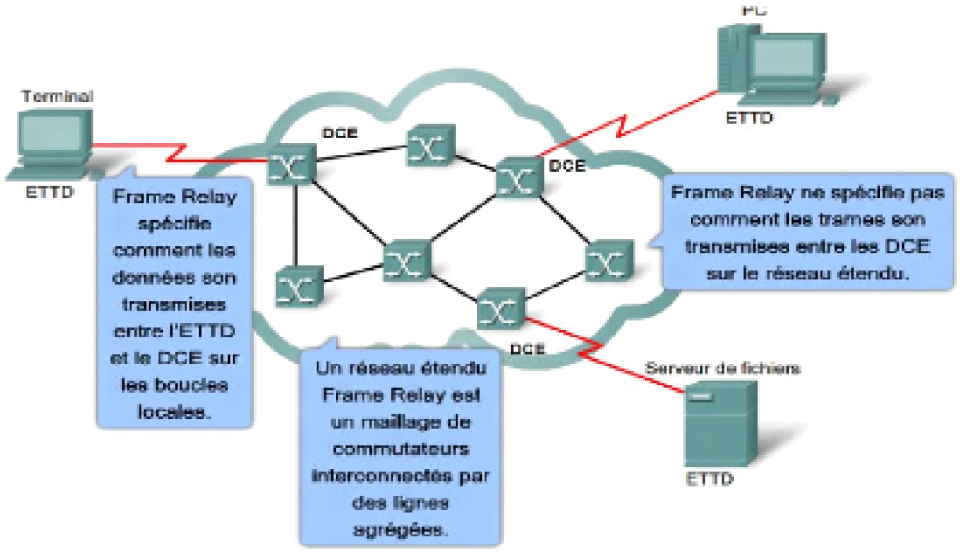


Figure II 2: réseau étendu frame Relay

II-2-3 Inconvénients de frame Relay:

Même si la commutation de trames présente des avantages par rapport à X25, elle n'est pas appropriée pour les applications comme la transmission vocale ou vidéo. Cet inconvénient était jusqu'à présent négligeable, les réseaux pour les transferts de voix ou d'images étant construits séparément. Pourtant, avec l'apparition des applications multimédia sur les réseaux LAN (Layer Area Network) et WAN (Wireless Area Network), l'intégration d'informations audio et vidéo a fait son apparition. Dans ce cas l'utilisation d'ATM est vivement recommandée.

II-3 ATM :

II-3-1 Présentation D'ATM :

ATM est l'abréviation de "Asynchronous Transfer Mode". Dès son développement au début des années '80, le protocole ATM est devenu de plus en plus important. L'accès au réseau ATM est asynchrone, ce qui offre l'indépendance temporelle entre le réseau et l'application. Un réseau ATM peut offrir une gamme de débits de transfert allant de quelques bits par seconde à plusieurs mégabits par seconde. Une grande diversité d'applications est donc réalisable, comme la vidéo, les données, l'audio...

Pour cela, il faut offrir:

- Un **débit** suffisant : Les applications multimédia ont besoin de liens avec des débits en Gigabits/s. Une **qualité de service** (QoS) adaptée aux différents types de trafic :Le trafic temps réel tolère certaines pertes mais pas de retard (comme la voix et la vidéo haute-résolution), tandis (comme le transfert de fichiers). Sans oublier la Bande Passante.

Le flux d'information est divisé en cellules de taille fixe (petits paquets de 53 octets), qui sont assignées aux utilisateurs selon les besoins. Une cellule ATM est composée d'un en-tête (5 octets) et d'un champ d'information (48 octets).

L'ATM est une technique orientée connexion qui permet de créer un VCI (Virtual Channel Identifier) qui contient plusieurs canaux virtuels VPI (Virtual Path Identifier). Le mode connecté procède de telle sorte que les cellules sont transmises en conservant leur séquençage.

II-3-2 Principes d'ATM

En traitant des données de longueur réduite et fixe (cellules), on peut assurer leur commutation au niveau physique (multiplexage). La commutation peut donc être assurée par des systèmes hardware et non plus logiciels, ce qui autorise des débits bien plus importants.

L'architecture ATM est représentée dans la figure suivante :

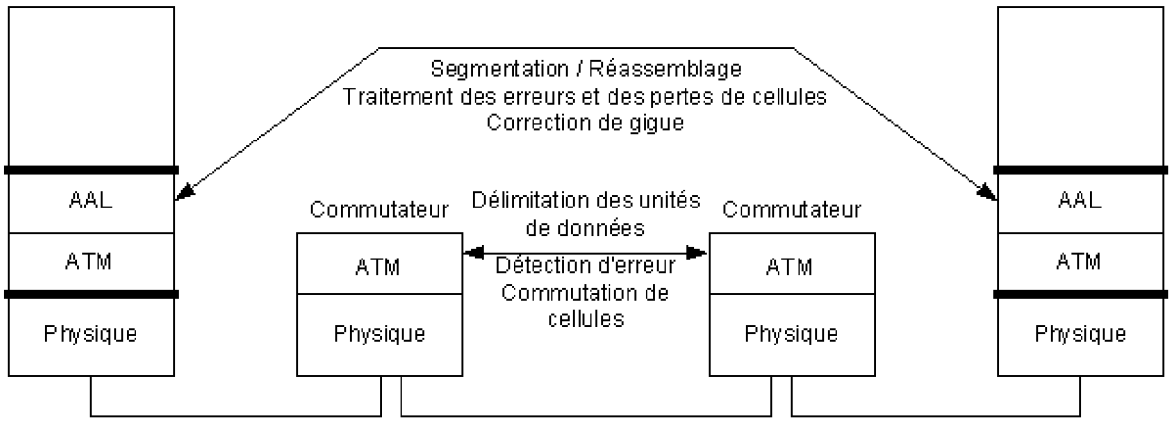


Figure II-3 : Relation entre les différentes couches de l'ATM

II-3-2-1 Les couches d'ATM:

a-La couche physique:

Cette couche est en fait composée de sous-couches:

- la sous-couche TC (Transmission Convergence), qui permet d'adapter les cellules ATM aux trames de transmission du réseau de transport choisi (ceci permet entre autre d'adapter ATM sur le réseau physique d'un opérateur).
- la sous-couche PHY (Physique), qui concerne l'adaptions physique du signal transmis sur les différents média utilisés (fibre optique par exemple).

b-La couche ATM:

Cette couche a pour rôle d'acheminer les données.

Elle doit donc:

- effectuer un contrôle du flux.
- assurer le multiplexage/démultiplexage.
- assurer l'ajout et le retrait de l'en-tête des cellules.
- assurer la translation VPI/VCI assurée à l'intérieur du réseau par le processus d'acheminement des cellules dans les commutateurs.

c- La couche d'adaptation AAL (ATM Adaptation Layer)

À deux fonctions primordiales, qui correspondent aux deux sous-couches AAL :

Une fonction de segmentation et réassemblage (sous-couche SAR) : il s'agit de segmenter et réassembler les PDU (Protocole Data Unit : unité de données usager.) qui ont une taille supérieure à celle d'une cellule. Cette opération modifie donc le format de l'unité de donnée. Des informations de gestion peuvent être ajoutées au champ information lors de cette phase. Ce mécanisme SAR est généralement intégré de façon hardware.

Une fonction de convergence (sous-couche CS) assure l'adaptation des couches supérieures: correction d'erreur, traitement des pertes et gains de cellules, absorption de la gigue, synchronisation.

II-3-3 Détail des cellules (UNI, NNI):

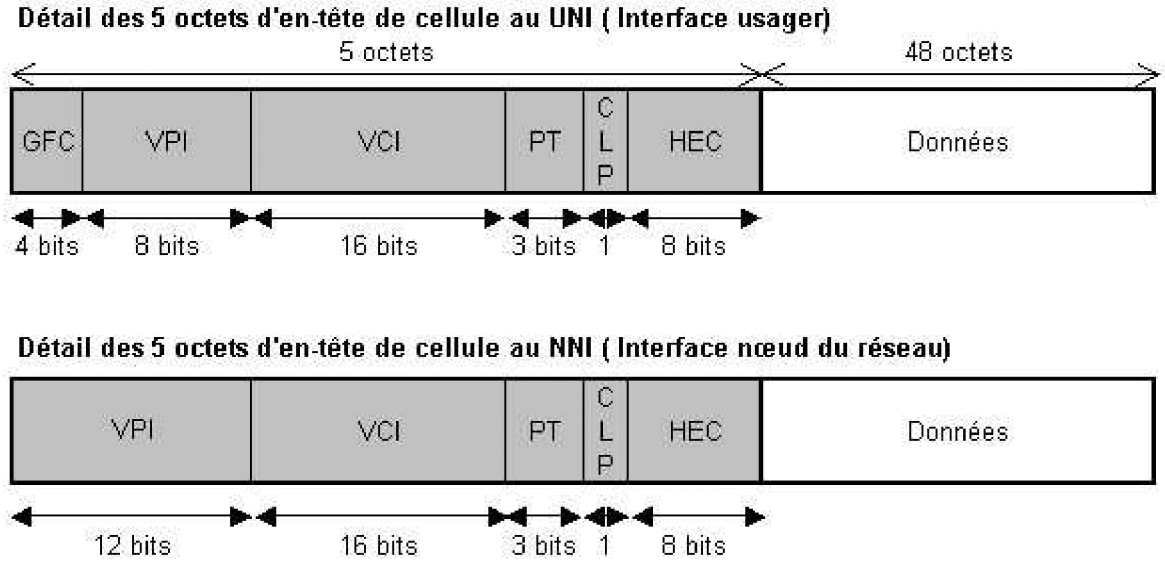


Figure II-4 : Les cellules UNIE et NNI

VPI (Virtual Path Identifier): Identification du conduit virtuel

VCI (Virtual Circuit Identifier) : Identifiant du circuit virtuel

GFC (Generic Flow Control) : Contrôle de flux

PT (Payload Type): Type du contenu transporté par la cellule

CLP (Cell Loss Priority): Priorité à la perte

HEC : Ce champ de contrôle d'erreur est géré par la couche physique.

II-3-4 Mécanisme de commutation de cellules:

Lors de l'établissement de la connexion, un circuit virtuel (***VC*** : Virtual Channel) est établi de bout en bout afin que les cellules puissent toutes suivre le même itinéraire (pour garantir l'intégrité de la séquence des cellules) et il est mémorisé dans les commutateurs ATM. L'entête de chaque cellule contient des informations nécessaires à leur acheminement. Ce sont deux champs indépendants et complémentaires, identifiant à la fois la cellule et la connexion virtuelle à laquelle elle appartient. Il s'agit :

Le **VPI** (Virtual Path Identifier), numéro de conduit virtuel. Le support physique est composé d'un ensemble de conduits virtuels qui eux mêmes sont composés d'un ensemble de circuits virtuels.

Le **VCI** (Virtual Circuit Identifier) qui un numéro de canal virtuel. Ce canal virtuel permettra d'acheminer individuellement les cellules. Lors de l'établissement, un canal virtuel ("contenu" dans un conduit virtuel) est réservé.

Cette double identification permet de voir le support physique comme un ensemble de conduits virtuels contenant plusieurs canaux virtuels.

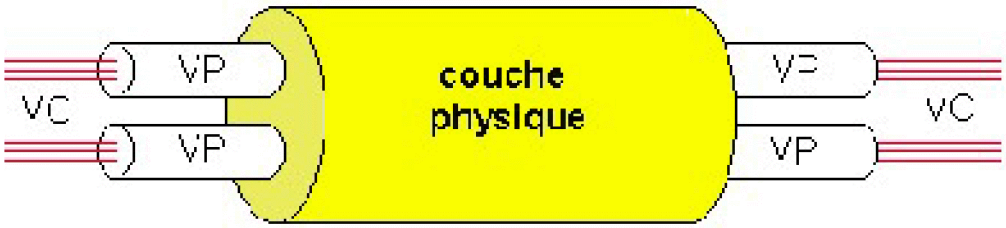


Figure II-5 : Multiplexage de VC dans un VP

L'adressage d'un circuit virtuel ATM (CV) est donc un couple VPI/VCI. Ce système permet d'effectuer un routage très facilement : un circuit virtuel n'est donc qu'une suite de couples VPI/VCI qui permet d'aller de routeur en routeur, jusqu'au destinataire.
En fait, lors de l'établissement de la connexion, chaque routeur du réseau ATM qui compose le circuit virtuel crée une table de routage qui permet de faire transiter les cellules arrivant vers le conduit virtuel adéquat.
On distingue trois phases :
- L'**établissement** de la connexion.
- Le **transfert** de données à travers le canal virtuel établi
- La **libération** de la connexion

II-4 Convergence vers MPLS:

Avant l'apparition de la MPLS, la réponse au problème des performances de routage des réseaux de routeurs consistait à superposer les réseaux IP aux réseaux ATM, ce qui créait une topologie virtuelle dans la couche ATM, dans laquelle tous les routeurs devenaient adjacents et réduisant ainsi au minimum le nombre de sauts IP entre les routeurs.

Toutefois, cette superposition IP/ATM présentait un inconvénient majeur : la nécessité de gérer l'explosion du nombre de connexions de circuit virtuel ATM nécessaires pour assurer un maillage complet des liaisons virtuelles entre les paires de routeurs. En effet, le nombre de circuits virtuels ATM nécessaires augmente comme le carré du nombre de routeurs connectés au nuage ATM.

Avec le remplacement progressif des réseaux IP par les réseaux IP/MPLS, Son rôle principal est de combiner les concepts du routage IP de niveau 3 (couche réseau), et les mécanismes de la commutation de niveau 2 (couche liaison) telles que celles implémentées dans ATM (Asynchronous Transfer Mode) ou Frame Relay. Les réseaux IP/MPLS sont capables de s'adapter aux besoins de forte croissance de l'internet, et de prendre la place de l'ATM en faisant face aux très grandes exigences du trafic professionnel.

De plus, les réseaux IP/MPLS sont prêts pour la convergence des données, de la voix et de la vidéo sur IP. Il n'est donc pas surprenant que l'IP/MPLS soit considéré par la majorité des opérateurs de réseaux comme le réseau cible à long terme.

Conclusion:

Dans ce chapitre nous avons vu les techniques utilisées pour la transmission de données, leurs évolutions, leurs avantages et inconvénients. Ces techniques sont de moins en moins utilisées avec l'arrivée de nouveaux services multimédias qui demandent une large bande passante. D'où la convergence des réseaux actuels vers le MPLS qui donne 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) du modèle OSI.

Introduction :

Le succès d'Internet s'est accompagné d'une augmentation forte du trafic des données dépassant celui de la voix. L'augmentation du trafic et par conséquent du débit des circuits physiques a posé un problème pour l'architecture classique d'un réseau IP. L'extension des tables de routage et le traitement des segments IP limitent la capacité des routeurs classiques. Aussi a-t-on cherché à faire évoluer le routeur vers un commutateur dont l'ATM avait démontré l'intérêt au point de vue performance. MPLS(Multi Protocol Label Switching) a donc été mis en place pour résoudre un certain nombre de problèmes liés à l'accroissement de la taille des réseaux (nombre d'utilisateurs, largeur des bandes passantes, gestion de plusieurs protocoles), donc dans ce cadre qu'est apparu le MPLS , destiné à intégrer les avantages de l'IP et les avantages d'une technologie en mode circuit comme l'ATM (circuits virtuels), afin de répondre aux besoins de fiabilité et de disponibilité.

Le MPLS a été conçu pour transporter des paquets IP, en leur attribuant des numéros d'identification particulièrement courts et faciles à traiter appelés étiquettes (label).

Le but de ce chapitre est de présenter les principaux éléments de l'architecture Multi Protocol Label Switching, (MPLS) et les mécanises de fonctionnent que l'on peut traduire par << commutation d'étiquettes multi protocolaire >>

III-1 PRINCIPES ET CONCEPTS DE MPLS :

III-1-1 Architecture de MPLS :

Un domaine MPLS est composé de deux sortes de routeurs, les LSR (Label Switching Router) et les ELSR (Edge Label Switching Router) où les LER (Label Edge Router) tout court.

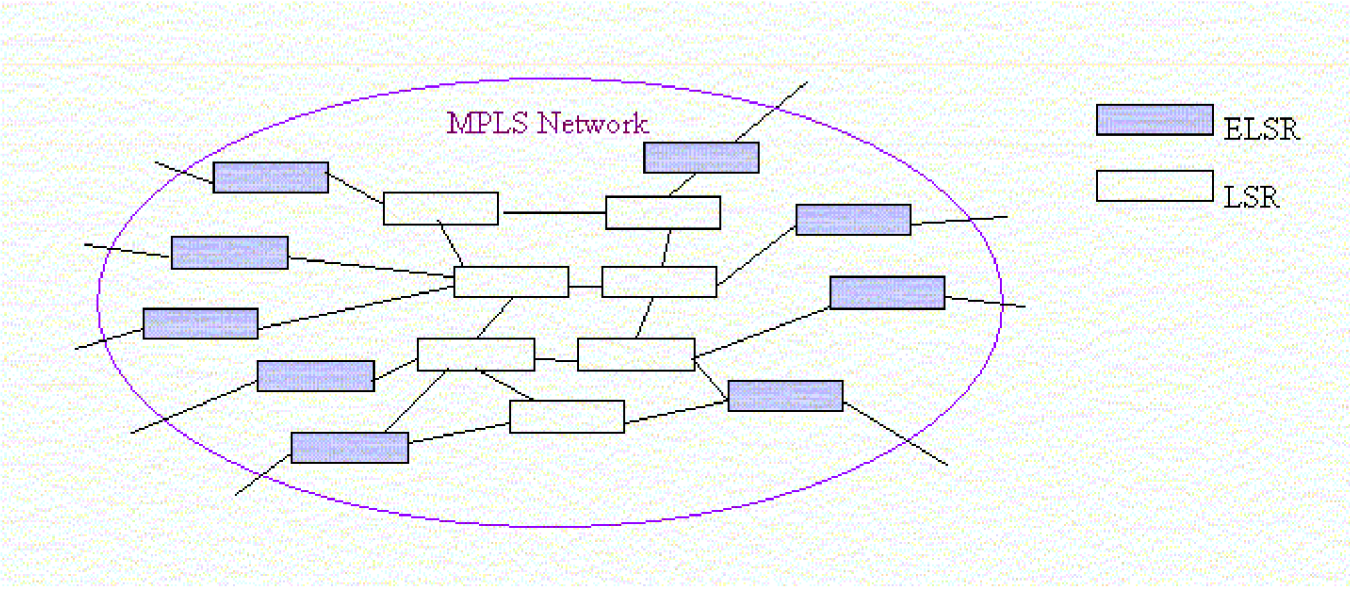


Figure III-1: Architecture d'un réseau MPLS

III-1-1-1 LSR (Label Switch router):

C'est un équipement de type routeur, ou commutateur qui appartient à un domaine MPLS, qui est présent pour lire les labels, gérer les services appropriés et rediriger les paquets en fonction des labels.

III-1-1-2 LER (Label Edge Router) :

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

- **Ingress LER** : c'est un routeur qui gère le trafic qui rentre dans un réseau MPLS.
- **Egress LER** : c'est un routeur qui gère le trafic qui sort d'un réseau MPLS.

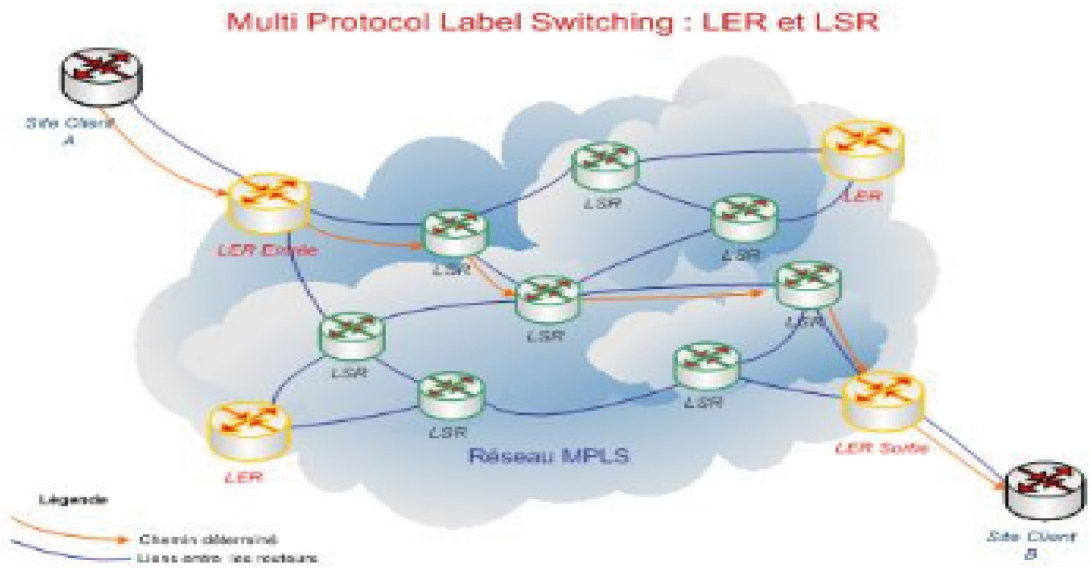


Figure III-2 : les LSR et les LER

III-1-2 Principe de fonctionnement de MPLS :

La mise en œuvre de MPLS repose sur la détermination de caractéristiques communes à un ensemble de paquets et dont dépendra l'acheminement de ces derniers. Cette notion de caractéristiques communes est appelée ***Forwarding Equivalence Class (FEC)***. Une FEC est la représentation d'un ensemble de paquets qui partagent les mêmes caractéristiques pour leur transport.

- Le routage IP classique distingue les paquets en se basant seulement sur les adresses des réseaux de destination (préfixe d'adresse).

- MPLS constitue les FEC selon de nombreux critères : adresse destination, adresse source, application, QoS, etc.

Quand un paquet IP arrive à un Ingress LER, il sera associé à une FEC. Puis, exactement comme dans le cas d'un routage IP classique, un protocole de routage sera mis en œuvre pour découvrir un chemin jusqu'à l'Egress LER (Voir la Figure ci-dessous, les flèches rouges). Mais à la différence d'un routage IP classique cette opération ne se réalise qu'une seule fois. Ensuite, tous les paquets appartenant à la même FEC seront acheminés suivant ce chemin qu'on va appeler ***Label Switched Path (LSP)***. Ainsi on a eu la séparation entre fonction de routage et fonction de commutation : Le routage se fait uniquement à la première étape. Ensuite tous les paquets appartenant à la même FEC subiront une commutation simple à travers ce chemin découvert.

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

L'acheminement des paquets dans le domaine MPLS ne se fait donc pas à base d'adresse IP mais de label (commutation de label).

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

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

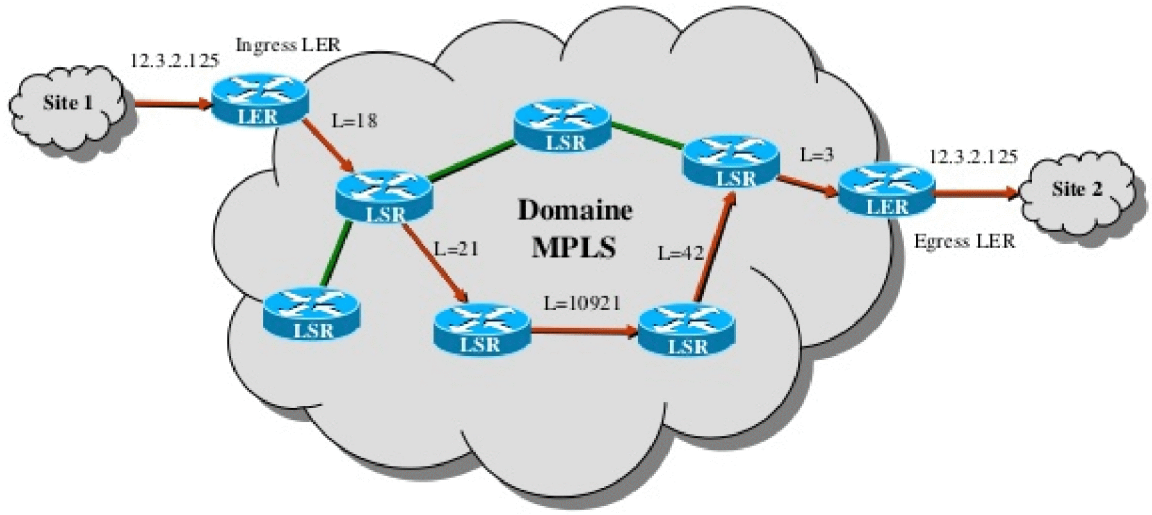


Figure III-3: Exemple d'un réseau MPLS

III-1-3 Pile de labels (label stacking):

Chaque paquet MPLS est susceptible de transporter plusieurs labels, formant ainsi une pile de labels, qui sont empilés et dépilés par les LSR. Cette possibilité d'empiler des labels, désignée sous le terme de Label Stacking, est utilisée par le MPLS

Lorsqu'un LSR commute un paquet, seul le premier label est traité, comme le monter la figure suivante.

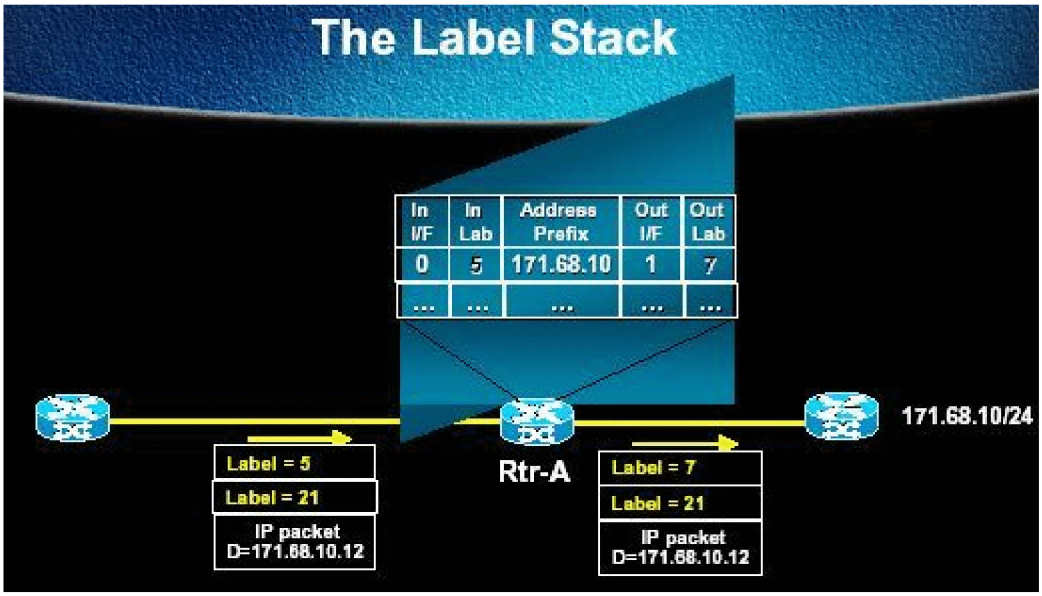


Figure III-4 : Pile de Label

III-1-4 Le LSP (Label Switch Path):

Un LSP (Label Switched Path) est le chemin que le paquet va emprunter lors de son passage dans le réseau MPLS. Ce chemin est établi par le protocole de signalisation LDP et en fonction de sa classe FEC. Il est important de noter qu'un LSP est unidirectionnel, il autorise à un paquet d'être commuté par étiquette d'un point de départ à un point d'arrivée comme le montre la figure suivante :

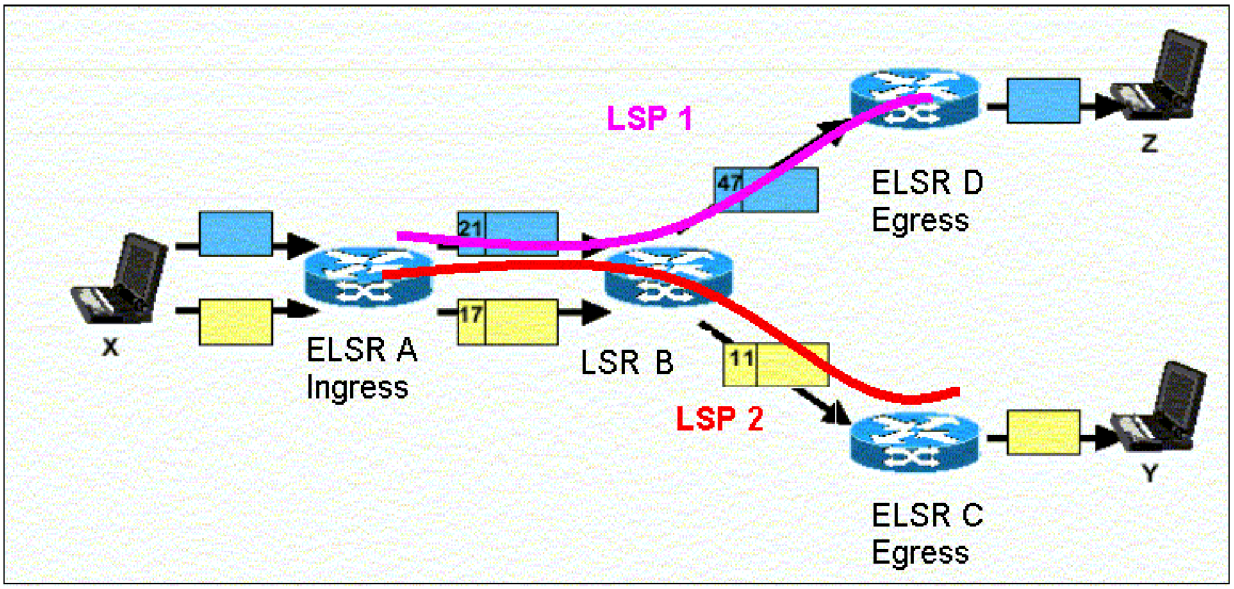


Figure III-5 : le chemin LSP

III-2 Les labels :

III-2-1 Définition :

Un label est un nombre entier inséré dans l'en-tête de couche 2 (Ethernet, PPP, ...) et l'en-tête de couche 3 (IP) du paquet. Ils seront commutés par les routeurs MPLS qui n'auront alors pas la nécessité de consulter l'en-tête de couche 3 ni la table de routage mais seulement les tables de commutation de labels.

III-2-2 Position dans l'en-tête:

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19	20 21 22	23	24 25 26 27 28 29 30 31
LABEL	EXP	S	TTL

Figure III-6: l'en-tête MPLS

LABEL (20 bits) : Contient le label.

EXP (3 bits) : Initialement réservé pour une utilisation expérimentale. Actuellement, la plus part des implémentations utilise ce champ comme indicateur de QoS. Généralement, c'est une

copie du champ PRECEDENCE (PPP) dans l'en-tête IP. En IP, la précédence définit la priorité d'un paquet (0 : priorité supérieure, 7 : priorité inférieure).

S (1 bit) : Indique s'il y a empilement de labels (il est en fait commun d'avoir plus qu'un label attaché à un paquet). Le bit S est à 1 lorsque le label se trouve au sommet de la pile, à 0 sinon.

TTL (8 bits) : Même signification que pour IP. 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

III-2-3 Rôle:

Un label a une signification locale entre deux LSR adjacents et mappe le flux du trafic entre le LSR amont et le LSR aval. A chaque bond le long du LSP (Label Switched Path), un label est utilisé pour chercher les informations de routage (next hop, lien de sortie, encapsulation) et les actions à réaliser sur le label : insérer, changer ou retirer.

III-3 Structures de données des Labels :

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

III-3-1 LIB (Label Information Base):

La première table construite par le routeur MPLS est la table LIB (Label Information Base). Elle est renseignée par le protocole de distribution de label LDP (Label Distribution Protocol) Elle contient pour chaque sous réseau IP la liste des labels affectés par les LSR voisins.

III-3-2 LFIB (Label Forwarding Information Base):

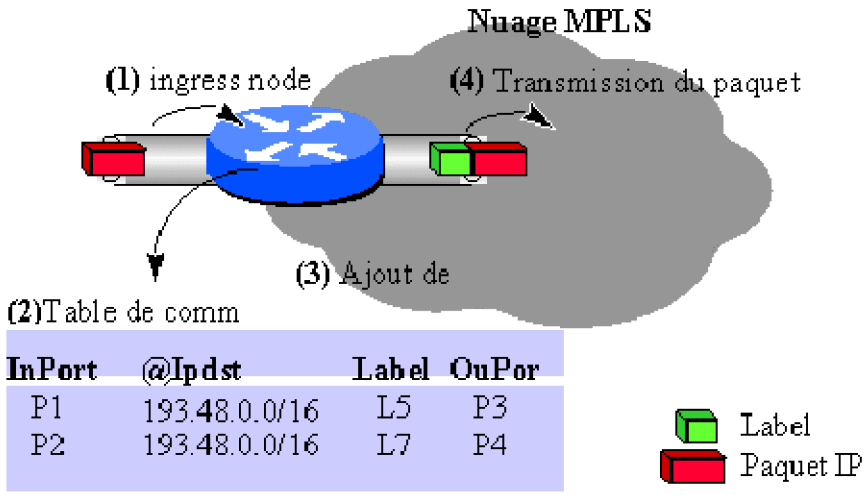
A partir de la table LIB et de la table de routage IP, le routeur construit une table LFIB, qui sera utilisée pour commuter les paquets. Chaque réseau IP est appris par l'OSPF (Open Short Path First), qui détermine le prochain saut ("next-hop") pour atteindre ce réseau. Le LSR choisit ainsi l'entrée de la table LIB qui correspond au réseau IP et sélectionne comme label de sortie le label annoncé par le voisin.

III-3-3 FIB (Forwarding Information Base):

Appartient au plan de donnée, c'est la base de donnée utilisé pour acheminer les paquets non labélisé.

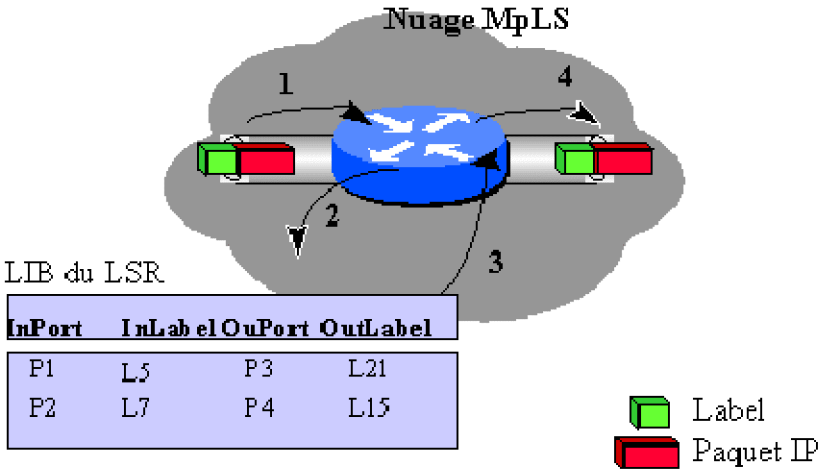
III-4 La commutation de labels :

Lorsqu'un paquet arrive dans un réseau MPLS (1). En fonction de la FEC au quelle appartient le paquet, Ingress node ou Ingress LER (Label Edge Router) consulte sa table de commutation (2) et affecte un label au paquet (3), et le transmet au LSR suivant(4)



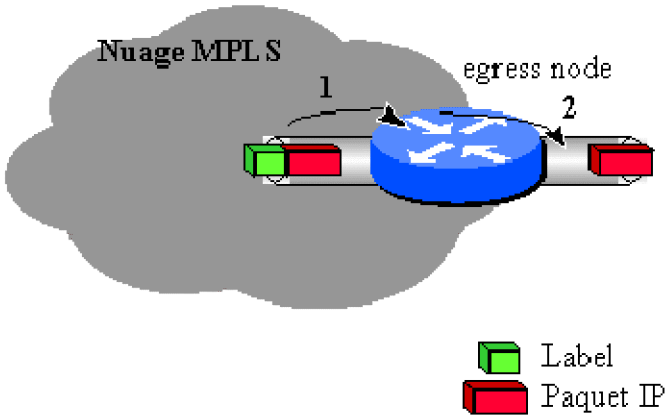
1 - Le paquet IP arrive sur l'ingress node
2 - Le protocole de routage IP détermine, à partir de l'adresse IP de l'eggress node, la FEC, le label et le port de sortie.
3 - Ajout de l'en-tête
4 - Paquet IP + Label envoyé vers le noeud suivant

Lorsque le paquet MPLS arrive sur un LSR (1) interne du nuage MPLS, le protocole de routage fonctionnant sur cet équipement détermine dans la base de données des labels LIB (Label Information Bas), le prochain label à appliquer à ce paquet pour qu'il parvienne jusqu'à sa destination (2). L'équipement procède ensuite à une mise à jour de l'en-tête MPLS (swapping du label et mise à jour du champ TTL, du bit S) (3), avant de l'envoyer au nœud suivant (LSR ou Egress node) (4). Il faut bien noter que sur un LSR interne, le protocole de routage de la couche réseau n'est jamais sollicité.



1 - Paquet IP + Label arrive sur le LSR
2 - Protocole de routage détermine, à partir de la LIB le next-hop LSR ou E-LSR
3 - Mise à jour du label MPLS
4 - Paquet IP + Label envoyé vers le noeud suivant

Enfin, une fois que le paquet MPLS arrive à node (1) ou l'Egress LER, l'équipement lui retire toute trace MPLS (2) et le transmet à la couche réseau



1 - Paquet IP + label arrive sur l'egress node
2 - Retrait du label et transmission du paquet IP à la couche réseau

III-5 Le protocole de distribution de label LDP:

Dans un cœur de réseau MPLS, les paquets IP en transit sont encapsulés dans des paquets MPLS et sont relayés sur la base du label se trouvant dans l'en-tête MPLS. Les LSR (Label Switch Router) d'un nuage MPLS doivent pour cela se mettre d'accord sur le sens à attribuer aux labels, c'est ce que l'on appelle la distribution de label. Il y a plusieurs manières de peupler les tables de commutation MPLS. La première est de le faire manuellement, ce qui n'est réaliste que pour un nombre très limité de classes d'équivalence FEC. Il est aussi possible d'utiliser un protocole entièrement automatique qui construit, sur la base des informations contenues dans les tables de routage IP, les chemins MPLS (les LSP : Label Switched Path)

pour chacune des classes d'équivalence reconnues dans les tables de routage. Avec cette approche, la construction des chemins se fait de proche en proche (Hop by Hop) sur un principe de fonctionnement similaire à celui des protocoles de routage IP. L'utilisation du nouveau protocole de distribution des labels, LDP (Label Distribution Protocol) est un exemple de cette approche.

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. Une connexion LDP peut être établie entre deux LSR directement ou indirectement connectés

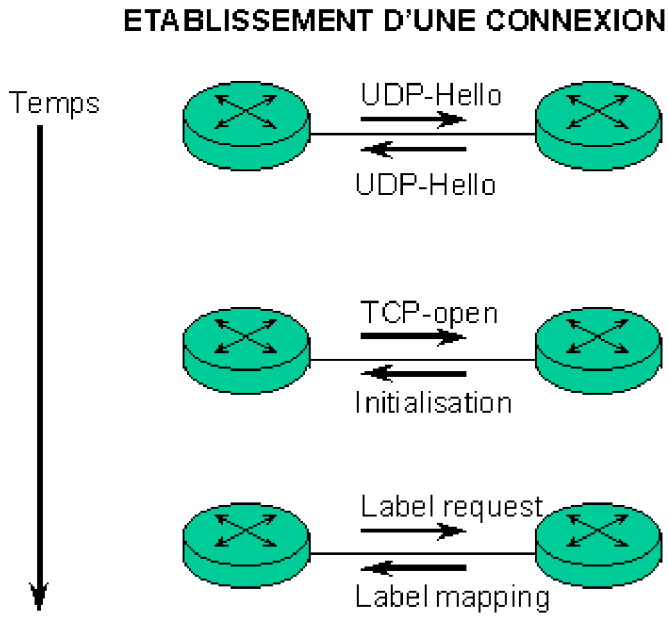


Figure III-7: Etablissement d'une connexion LDP

Label request ou demande de label, est envoyé par le LSR amont pour demander quel label il doit utiliser pour une FEC spécifique. Label mapping, message d'attribution de label à une FEC, peut être émis en réponse au message Label request (distribution en monde non sollicité) ou spontanément après la découverte d'une nouvelle FEC (distribution en mode non sollicité).

LDP est bidirectionnel et permet la découverte dynamique des nœuds adjacents grâce à des messages « Hello » échangés par UDP. Une fois que les deux nœuds se sont découverts, ils établissent une session TCP 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 notifications

III-6 Applications de MPLS :

Les applications les plus courantes du MPLS sont les suivantes :

- L'ingénierie de trafic est activée par des mécanismes MPLS permettant de diriger le trafic via un chemin spécifique, qui n'est pas nécessairement le chemin le moins coûteux. Les administrateurs de réseau peuvent mettre en œuvre des politiques visant à assurer une distribution optimale du trafic et à améliorer l'utilisation globale du réseau.
- La bande passante garantie constitue une amélioration à forte valeur ajoutée par rapport aux mécanismes d'ingénierie de trafic traditionnels. MPLS permet aux fournisseurs de services d'allouer des largeurs de bande passante et des canaux garantis. La bande passante garantie permet également la comptabilité des ressources QoS (qualité de service) de manière à organiser le trafic 'prioritaire' et 'au mieux', tels que la voix et les données.
- Le reroutage rapide 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.
- Les réseaux privés virtuels MPLS simplifient considérablement le déploiement des services par rapport aux VPN IP traditionnels. Lorsque le nombre de routes et de clients augmente, les VPN MPLS peuvent facilement monter en charge, tout en offrant le même niveau de confidentialité que les technologies de niveau 2. Ils peuvent également transporter des adresses IP non-uniques à travers un domaine public.
- La fonction Classe de service (CoS) MPLS assure que le 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.

Conclusion:

Dans ce chapitre, nous avons présenté le mécanisme de fonctionnent de l'architecture MPLS, ainsi que ses éléments les plus importants (LSR, FEC, LSP, ..), leurs différents rôles, les Labels et leurs structures de données.

En effet MPLS est une architecture qui appartient aux réseaux NGN, cette architecture est en cours de déploiement par plusieurs opérateurs comme Algérie Télécom et ATM Mobilis. Dans les chapitres suivants, nous allons détailler les applications de la MPLS.

Introduction:

Les principaux atouts de la technologie MPLS concernent sa capacité à intégrer des solutions de gestion de la qualité de service et d'ingénierie de trafic sur un réseau IP. En effet, les opérateurs ont besoin de contrôler leur réseau plus finement que ce que leur permet le routage IP classique, sans pour autant abandonner la souplesse qu'il apporte. Du fait qu'un chemin virtuel est créé pour transporter les paquets IP, MPLS est un candidat idéal pour supporter des fonctions évoluées d'ingénierie de trafic et ajouter des fonctionnalités de gestion de la qualité de service dans les cœurs de réseau.

IV-1 Traffic Engineering:

L'ingénierie de trafic appliquée aux réseaux MPLS est normalisée sous le nom MPLS-TE (Multi Protocol Label Switching - Traffic Engineering) 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, permet aussi de gérer des services nécessitant différents niveaux de priorités, tel le transport de voix ou de vidéo sur Internet, sans avoir recours à une politique de surdimensionnement des réseaux physiques..

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 technologie MPLS-TE permet également de répondre à des exigences de haute disponibilité et de sécurisation des services notamment temps réels via le mécanisme MPLS-TE Fast-Reroute.

IV-1-1 Fonctionnalités notables proposées par MPLS-TE :

- Création de LSP-TE MPLS unidirectionnels, indépendants du routage IGP et contraints par des critères de métrique, de bande passante requise (fixe ou adaptative), de délai, etc.
- Qualité de service, grâce aux critères de bande passante, priorités d'établissement et de maintien des tunnels et aux chemins préférés (couleurs administratives et affinités).
- Reprise rapide sur incident, sécurisation des LSP-TE (Fast-Reroute).
- Prise en compte des différentes Classes de services (CoS).
- Partage de charge entre plusieurs LSP-TE.

IV-1-2 Les motivations du Traffic Engineering :

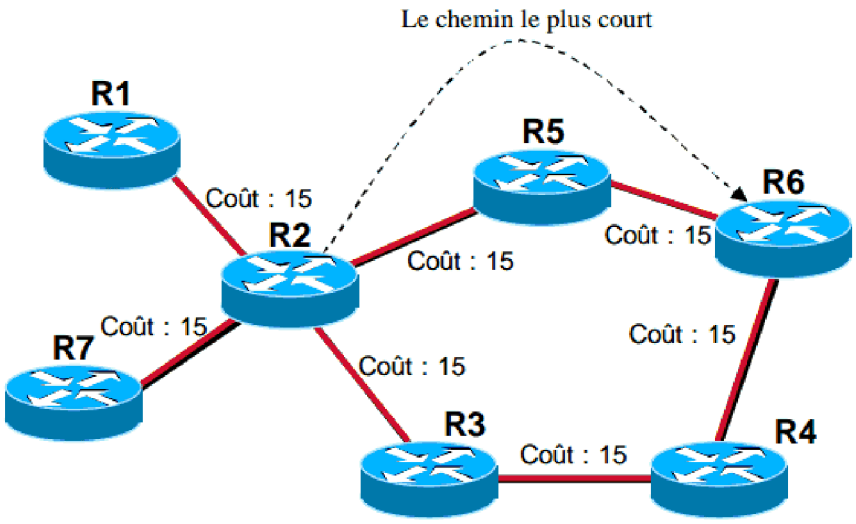


Figure IV-1 : Le routage classique

Dans la figure IV-1 : Il existe deux chemins pour aller de R2 à R6 :

- R2 à R5 à R6
- R2 à R3 à R4 à R6

En IP classique, Le protocole de routage (OSPF, IS-IS, etc.) va se baser sur le critère du plus court chemin. Et puisque tous les liens ont le même coût (15), les paquets venant de R1 ou R7 est qui sont destinés à R6 vont tous suivre le même chemin (R2 à R5 à R6).

Ceci peut conduire à quelques problèmes : supposant que tous les liens de la figure supportent une bande passante de 150Mbps. Et supposant que R1 envoie en moyenne 90Mbps à R6. Le protocole de routage va faire de sorte que ce trafic utilise le plus court chemin, soit R2 à R5 à R6. Si maintenant R7 veut envoyer 100Mbps à R6. La même procédure de routage fera que ce trafic utilisera aussi le chemin le plus court. En final, on aura deux trafics de 190Mbps en total qui veulent tous deux utiliser le chemin le plus court (R2 à R5 à R6), alors que ce chemin ne peut supporter que 150Mbps. Ceci va induire des files d'attente et des pertes de paquets. Cet exemple est un cas explicite de sous utilisation des ressources du réseau vu que réellement, il existe un chemin dans le réseau qui n'est pas exploité et que son utilisation aurait permis de satisfaire les deux trafics.

MPLS TE permet à l'ingress LER de contrôler le chemin que son trafic va emprunter pour atteindre une destination particulière. Ce concept est connu sous le nom de "***Explicit Routing***". Cette méthode est plus flexible que l'acheminement du trafic basé seulement sur l'adresse destination. MPLS TE réserve de la bande passante en construisant les LSP. Ainsi

dans la topologie de la figure IV.2, LSR2 a la possibilité de construire deux LSP (Tunnel1 et tunnel2) relatifs aux chemins :

· LSR2 à LSR5 à LSR6

· LSR2 à LSR3 à LSR4 à LSR6

Les LSP ainsi construits sont appelés ***MPLS TE LSP*** ou ***TE tunnels***.

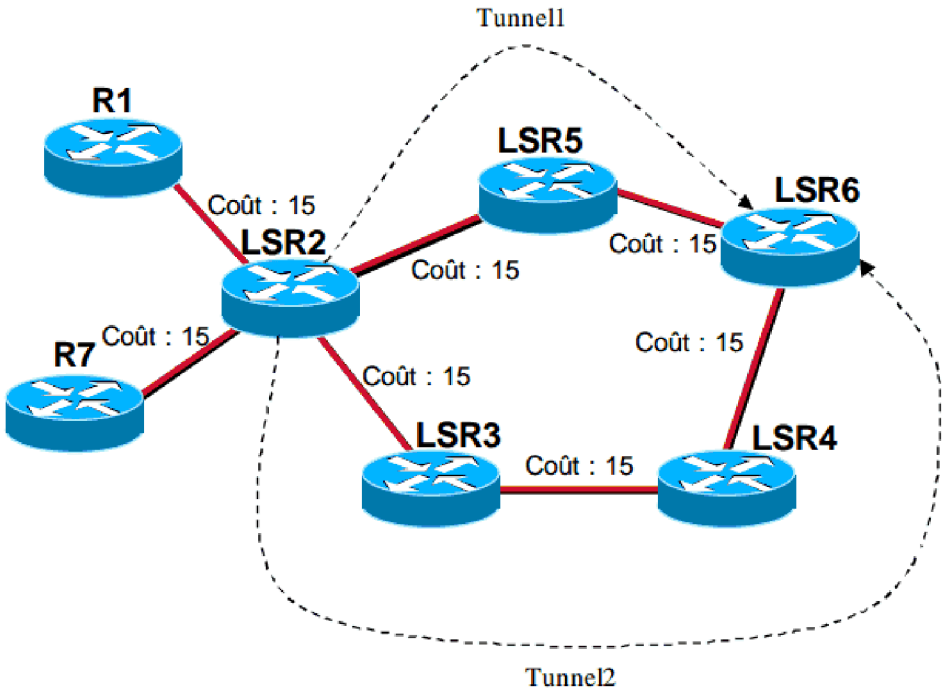


Figure IV-2 : Le Traffic Engineering selon MPLS

La souplesse de l'utilisation des labels dans MPLS TE permet de profiter des avantages suivants :

- Le routage des chemins primaires autour de points de congestion connus dans le réseau (le contournement de la congestion) ;

- Le contrôle précis du re-routage de trafic, en cas d'incident sur le chemin primaire,(on sous-entend par reroutage : la modification du LSP en cas d'erreur (routeur en panne, manque de ressources).

-Un usage optimal de l'ensemble des liens physiques du réseau, en évitant la surcharge de certains liens et la sous-utilisassions d'autres. C'est ce qu'on appelle l'équilibrage des charges ou load balancing.

Le Traffic Engineering permet ainsi d'améliorer statistiquement les paramètres de QoS (taux de perte, délai, gigue, etc.).

Un exemple concret de Traffic Engineering est qu'il est possible de définir plusieurs LSP entre chaque couple de LER. Chaque LSP peut être conçu (grâce aux techniques de traffic Engineering) pour fournir différentes garanties de bande passante ou de performances.

Ainsi, l'ingress LER pourra placer le trafic prioritaire dans un LSP, le trafic de moyenne priorité dans un autre LSP et enfin le trafic best effort dans un troisième LSP.

IV-2 Calcul et établissement des "MPLS TE LSP":

Dans un protocole de routage à état de lien (tel que OSPF ou IS-IS), chaque routeur connaît tous les routeurs du réseau et les liens qui connectent ces routeurs.

Aussi tôt qu'un routeur se fait une idée de la topologie du réseau, il exécute le *"Dijkstra shortest Path First algorithm*" (SPF) pour déterminer le plus court chemin entre lui-même et tous les autres routeurs du réseau (Construction de la table de routage). Etant donné que tous les routeurs exécutent le même calcul sur les mêmes données, chaque routeur aura la même image du réseau, et les paquets seront routés de manière cohérente à chaque saut.

Le processus qui génère un chemin pour un "MPLS TE LSP" est différent du SPF classique, mais pas trop. Il y a deux différences majeures entre le SPF classique, utilisée par les protocoles de routage, et le CSPF (Constrained Shortest Path First), utilisé par MPLS TE :

- Le processus de détermination de chemin n'est pas conçu pour trouver le plus court chemin, mais il tient compte d'autres contraintes ;
- Il y a plus d'une métrique à chaque nœud, au lieu d'une seule comme dans le cas d'OSPF et IS-IS.

MPLS crée les LSP différemment selon qu'on utilise le Traffic Engineering ou non. La création d'un "MPLS LSP", dans le cas non TE, suit les deux étapes suivantes :

- Calcul du "MPLS LSP" : Mise en oeuvre de l'algorithme SPF (OSPF ou IS-IS).
- Etablissement du "MPLS LSP" : Mise en œuvre d'un protocole de distribution de label Topologie-based (LDP).

La création d'un "MPLS TE LSP" suit les deux étapes suivantes :

- Calcul du "MPLS TE LSP" : Mise en œuvre de l'algorithme CSPF ou intervention manuelle de l'administrateur pour imposer une route explicite.
- Etablissement du "MPLS TE LSP" : Mise en œuvre d'un protocole de distribution de label Request-based (RSVP TE, CR-LDP).

Après avoir calculé un chemin avec CSPF, ce chemin doit être signalé à travers le réseau, et ceci pour deux raisons :

- Etablir une chaîne de labels qui représente le chemin.
- Réserver les ressources nécessaires (bande passante) à travers le chemin.

Dans ce qui suit, on va détailler l'étape de l'établissement du "MPLS TE LSP" en examinant de prés le fonctionnement des protocoles de distribution de labels RSVP- TE et CR-LDP. On va se concentrer plus sur RSVP TE vu que l'étude pratique porte sur ce protocole.

IV-3 Resource ReSerVation Protocol - Traffic Engineering (RSVP TE) :

Ce protocole est originalement destiné à être un protocole de signalisation pour IntServ (C'est un modèle de QoS où une machine demande du réseau une QoS donnée pour un flux donné). RSVP avec quelques extensions a été adapté par MPLS pour être un protocole de signalisation qui supporte MPLS TE.

Nous allons, dans cette partie, commencer par illustrer le format général des messages RSVP TE. Pour enfin expliquer avec plus ou moins de détails le fonctionnement de ce protocole.

IV-3-1 Messages RSVP-TE

Le protocole RSVP-TE tourne entre routeurs adjacents. Il repose sur un ensemble de messages constitués d'un en-tête RSVP commun suivi d'un ensemble d'objets RSVP-TE. Ces messages sont transportés directement sur IP ou sur UDP. Par défaut, le rafraîchissement périodique des messages permet de prendre en compte les éventuelles pertes de paquets. Il existe également un mécanisme optionnel d'acquittement et de retransmission permettant de traiter directement les éventuelles pertes de message. Les principaux messages RSVP-TE sont les suivants :

- **Path** : Etablissement et maintenance le LSP-TE dans le sens descendant.
- **Resv** : Etablissement et maintenance le LSP-TE dans le sens montant.
- **PathTear** : Suppression le LSP-TE dans le sens descendant.
- **ResvTear** : Suppression le LSP-TE dans le sens montant.
- **PathErr** : Indication d'erreur dans le sens montant.
- **ResvErr** : Indication d'erreur dans le sens descendant.
- **ResvConf** : Confirmation l'établissement d'un tunnel dans le sens descendant.
- **Srefresh** : Rafraîchissement d'un ensemble de sessions RSVP-TE.
- **Hello** : Maintient l'adjacence entre deux voisins RSVP-TE, permet de détecter la perte d'un voisin. Cette procédure est optionnelle.

IV-3-2 Le fonctionnement de RSVP TE :

RSVP TE est un mécanisme de signalisation utilisé pour réserver des ressources à travers un réseau. RSVP TE n'est pas un protocole de routage. Toute décision de routage est

faite par IGP (Interior Gateway Protocol). Le seul travail de RSVP TE est de signaler et de maintenir la réservation de ressources à travers le réseau.

-RSVP TE a trois fonctions de base :

- L'établissement et la maintenance des chemins (*Path setup and maintenance*).
- La suppression des chemins (*Path teardown*).
- La signalisation des erreurs (*Error signalling*).

RSVP TE est un "*soft-state protocol*". Cela veut dire qu'il a besoin de rafraîchir périodiquement ses réservations dans le réseau. Ceci est différent des "*hard-state protocol*", qui signalent leurs requêtes une seule fois et puis supposent qu'elle reste maintenue jusqu'à sa résiliation explicite. Avec RSVP TE, une requête est résiliée si elle l'est explicitement du réseau par RSVP TE ou si la durée de réservation expire.

IV-3-3 L'établissement et la maintenance des chemins :

Bien que l'établissement et la maintenance des chemins soient des concepts très proches et utilisent les mêmes formats de messages, toutefois, ils différent légèrement. C'est pourquoi, on va les expliquer séparément.

IV-3-3 –1 L'établissement des chemins :

L'établissement d'un LSP-TE par RSVP-TE est effectué en deux temps. Après que l'ingress LER (appelé aussi ***MPLS TE tunnel headend*** ou ***headend***) ait terminé sa procédure CSPF pour un tunnel particulier, il doit signaler le chemin trouvé à travers le réseau. Le headend réalise cette opération en envoyant un Path message au prochain saut (next hop) dans le chemin calculé vers la destination. Message **Path** est envoyé de la source vers la destination, de proche en proche, le long de la route explicite. Ce message **Path** contient les informations suivantes :

- L'adresse de la source et de la destination du LSP.
- Les numéros de tunnel et de LSP.
- La bande passante du LSP.
- Les groupes administratifs à inclure et ceux à exclure.
- Un ensemble de paramètres de classe de service et de sécurisation.
- La route explicite du LSP, codée dans l'objet ERO (Explicite Route Object).

À la réception du message **Path**, chaque routeur de transit instancie un nouvel état RSVP-TE, enregistre les informations reçues dans le message et réalise un contrôle d'admission local pour vérifier que le prochain lien valide les contraintes TE du LSP-TE.

En réponse, le routeur de destination renvoie un message **Resv** de proche en proche vers l'origine du tunnel. Ce message **Resv** réserve la bande passante et distribue les labels, Cela entraîne une mise à jour des tables MPLS en transit et de la table IP sur la tête du tunnel TE.

Le message **Resv** contient les informations suivantes :

- L'adresse de la source et de la destination du LSP.
- Les numéros de tunnel et de LSP.
- La bande passante du LSP.
- Le label alloué localement pour le LSP.

Lorsque le message **Resv** est arrivé sur la tête et que la table de routage IP est mise à jour, le tunnel TE peut être utilisé pour aiguiller du trafic le long du LSP-TE.

La figure ci-dessous détaille les étapes du processus d'établissement d'un LSP-TE avec RSVP-TE, en donnant l'exemple d'une réservation le long du cheminR1->R2->R3->R5->R6->R7.

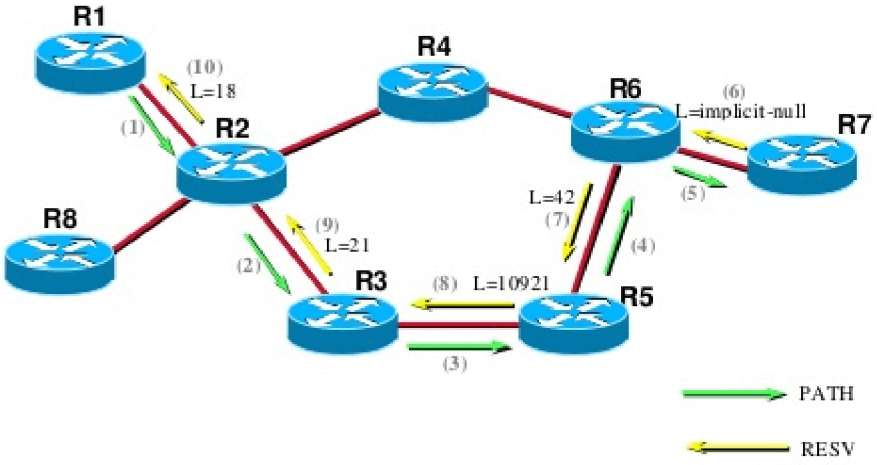


Figure IV-3: Path et Resv messages, lors de l'établissement de chemin

Supposant que R1 a déjà réalisé sa procédure CSPF et a déjà décidé des besoins en bande passante qu'il veut réserver le long du chemin (R1->R2->R3->R5->R6->R7) :

(1) R1 envoie un Path message à R2. R2 vérifie alors le format du message et la disponibilité de la bande passante demandée par R1. S'il y a un Problème, R2 envoie un message d'erreur (PathErr) vers R1.

(2) R2 envoie un Path message à R3qui realise les mêmes vérifications que dans l'étape(1)

(3) R3 envoie un Path message à R5 qui réalise les mêmes vérifications.

(4) R5 envoie un Path message à R6 qui Réalise les mêmes vérifications.

(5) R6 envoie un Path message à R7 qui Réalise les mêmes vérifications.

(6) R7 étant le tunnel TE (tail-end), envoie un Resv message à R6. Ce Resv message contient le Label que R7 veut voir dans les paquets de ce tunnel. Puisque R7 est le tail, il envoie un label « implicit-null».

(7) R6 envoie un **Resv** message à R5 et indique un nouveau label=42.

(8) R5 envoie un **Resv** message à R3 et indique un nouveau label=10921.

(9) R3 envoie un Resv message à R2 et indique un nouveau label=21.

(10) R2 envoie un Resv message à R1 et indique un nouveau label=18. L'établissement du LSP-TE est alors finalisé.

IV-3-3 –2 La maintenance des chemins :

D'un premier coup d'œil, la maintenance des chemins et très similaire à l'établissement des chemins : chaque 30 secondes (Plus ou moins 50%), le headend envoie un Path message par tunnel. Si un routeur envoie quatre Path messages successifs et ne reçoit pas de Resv message correspondant, il considère la réservation supprimée et envoie un message dans le sens inverse indiquant que la réservation est supprimée.

Cependant, il y a une chose importante à comprendre ici. Path et Resv messages sont tous les deux envoyés d'une façon indépendante et asynchrone d'un voisin à un autre. Si on regarde encore une fois la figure IV.3, chaque 30 secondes, R1 envoie un Path message à R2 pour la réservation qu'il a effectuée. Et chaque 30 secondes, R2 envoie un Resv message à R1 pour la même réservation. Cependant, les deux messages ne sont pas connectés. Un Resv message utilisé pour rafraîchir une réservation existante n'est pas envoyée en réponse à un Path message.

IV-3-4 La suppression des chemins :

La suppression des chemins est une procédure assez simple. Si un nœud décide qu'une réservation n'est plus nécessaire dans un réseau, il envoie un PathTear le long du même chemin que le Path message a suivi et un ResvTear le long du même chemin que le Resv message a suivi. ResvTear messages sont envoyés en réponse aux PathTear messages pour signaler que le tunnel tail a supprimé la réservation du réseau.

Exactement comme les messages de rafraîchissement, PathTear messages n'ont pas à traverser la totalité du chemin avant que leur effet ne prend place. Dans la figure IV.3, si R1 envoie un PathTear à R2, R2 répond immédiatement par un ResvTear et puis envoie son propre PathTear au next hop.

IV-3-5 La signalisation des erreurs :

De temps en temps, des problèmes peuvent avoir lieu dans le réseau (Bande passante non disponible, boucle de routage, routeur intermédiaire ne prend pas en charge MPLS, message corrompu, création de label impossible, etc.). Ces erreurs sont signalées par PathErr où ResvErr messages. Une erreur détectée dans un Path message est traitée par un PathErr message, et une erreur détectée dans un Resv message est traitée par un ResvErr message.
Les messages d'erreurs sont envoyés vers la source de l'erreur ; le PathErr est envoyé vers le headend, et un ResvErr est envoyé vers le tail.

IV-4 Constraint-based Routing over Label Distribution Protocol (CR-LDP):

Des modifications ont été apportées au protocole LDP pour permettre la spécification du trafic. Ce protocole a été nommé CR-LDP (Constraint-based Routing over Label Distribution Protocol). L'idée de ce protocole était d'utiliser un protocole de distribution de label déjà existant et de lui ajouter la capacité de gérer le Traffic Engineering.
Sans entrer dans les détails de LDP, CR-LDP ajoute des champs à ceux déjà définis dans LDP, tel que "*peak date rate*" et "*committed data rate*". Le premier indique le débit maximum avec lequel un trafic peut être envoyé via le TE LSP et le deuxième indique le débit garanti par le domaine MPLS pour ce trafic. La gestion des réservations dans CR-LDP est très similaire à celle utilisée dans les réseaux ATM, Alors que RSVP TE utilise plutôt le modèle d'IntServ

IV-4-1 Le fonctionnement de CR-LDP:

On va expliquer d'une façon concise les étapes qui aboutissent à l'établissement d'un CR-LDP LSP. Pour cela, examinant la figure IV.4 :

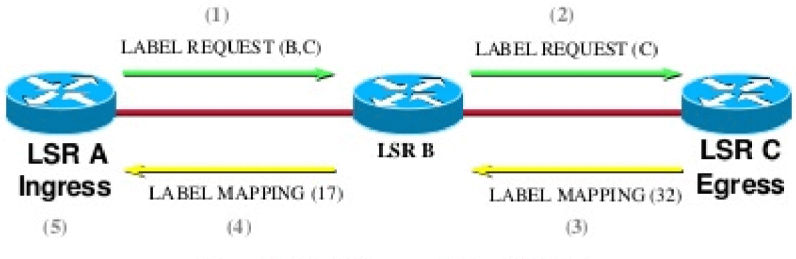


Figure IV.4: Etablissement d'un CR-LDP LSP

(1) Ingress LSR A détermine qu'il a besoin d'établir un nouveau LSP vers LSR C en passant par LSR B. Pour cela, LSR A envoie à LSR B un LABEL_REQUEST message avec l'explicit route (B, C) et le détail des paramètres du trafic nécessaire pour cette nouvelle route.
(2) LSR B reçoit le LABEL_REQUEST message, réserve les ressources demandées, modifie l'explicit route dans le *LABEL_REQUEST message* et fait suivre le message à LSR C. Si

nécessaire, LSR B peut réduire les réservations demandées dans le cas où les paramètres correspondant sont marqués négociables dans le *LABEL_REQUEST* Message.

(3) LSR C détecte que c'est lui l'egress LSR. Il fait les mêmes activités de réservation et de négociation que LSR B. Il alloue un label pour le nouveau LSR et l'envoie à LSR B dans un *LABEL_MAPPING message.* Ce message contient aussi les détails des paramètres finaux du trafic pour ce LSP.

(4) LSR B reçoit le *LABEL_MAPPING message*, il finalise la réservation, alloue un label pour le LSP et met à jour sa table de labels. Ensuite, il envoie le nouveau label à LSR A dans un autre *LABEL_MAPPING message*.

(5) Le même processus se réalise dans LSR A. Mais vu que LSR A est l'ingress LSR, il n'aura pas à allouer un label. Ainsi le nouveau LSR est établi et les données peuvent y transiter.

IV-5 VPN/MPLS

Introduction:

Les VPN/MPLS sont essentiellement implémentés chez les opérateurs afin de fournir des services à leurs clients. Les opérateurs utilisent leur backbone sur MPLS pour créer des VPN, par conséquent le réseau MPLS des opérateurs se trouve partagé où mutualisé avec d'autre client. Du point de vue du client, il a l'impression de bénéficier d'un réseau qui lui est entièrement dédié. C'est-à-dire qu'il a l'impression d'être le seul à utiliser les ressources que l'opérateur lui met à disposition. Ceci est dû à l'étanchéité des VPN/MPLS qui distingue bien les VPN de chaque client et tous ces mécanismes demeurent transparents pour les clients. Finalement, les deux parties sont gagnantes car les clients ont un véritable service IP qui leur offre des VPN fiables à des prix plus intéressants que s'ils devaient créer eux-mêmes leur VPN de couche 2. Les opérateurs eux aussi réduisent leurs coûts du fait de la mutualisation de leurs équipements.

Cette partie aborde les concepts de VPN/MPLS, en particulier avec les notions de routeurs virtuels (VRF) et le protocole MP-BGP, dédié à l'échange de routes VPN.

IV-5 -1Model des VPNS :

IV-5 -1-1 .Overlay model:

Au lancement des VPN/MPLS le modèle Overlay avait été choisi, il consiste à émuler des lignes dédiées entre chaque entité du client sur le réseau MPLS. Il s'agit en fait d'un LSP (Label Switched Path) sur le réseau MPLS qui relie chaque site. La création de ces LSP entre les différents sites de l'entreprise permettra alors de former un VPN IP.

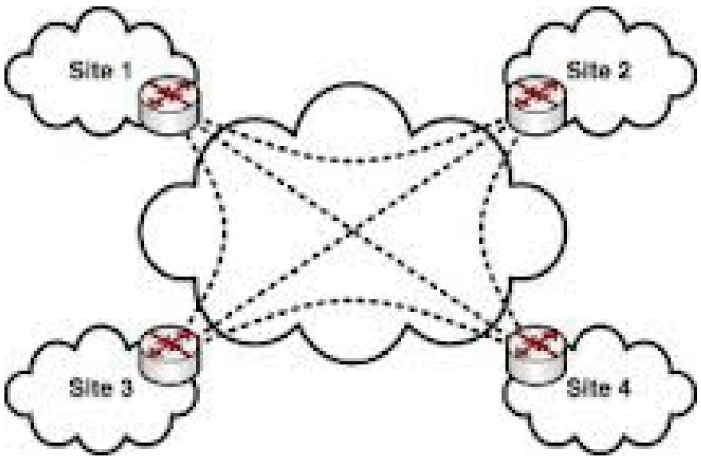


Figure IV-5 overlay model

Ce modèle a cependant un inconvénient car les points d'accès au réseau MPLS se situent dans le réseau du client. En effet, l'ajout de nouveaux sites dans ce VPN nécessite la création de nouveaux LSP. Ce modèle pose ainsi un problème de scalabilité. Si nous avons 5 sites appartenant à un VPN, l'ajout d'un 6ième site requiert la mise en place de 5 nouveaux LSP. Par conséquent, plus le nombre de sites est élevé plus la tache s'avère fastidieuse.

IV-5 -1-2 Peer to peer model:

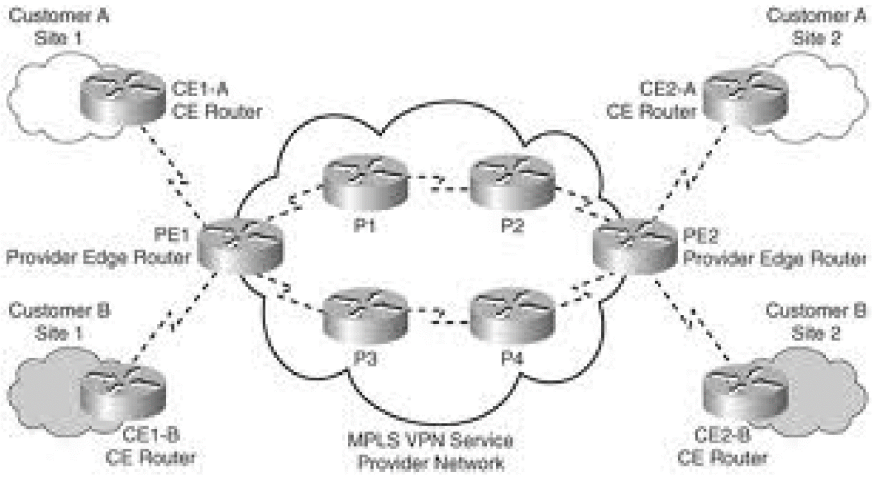


Figure IV-6: peer to peer model

Actuellement ce modèle est largement employé chez les opérateurs car il permet l'ajout de nouveaux sites en changeant la configuration des PE. De plus, du point de vue de l'utilisateur l'interconnexion avec le VPN ne se fait que sur un seul équipement de l'opérateur contrairement au modèle Overlay, il s'agit du PE. Enfin, le routage entres différents sites clients est optimale car le PE connaît sa topologie et peut de ce fait choisir la route adéquate.

De manière générale, la topologie utilisée pour relier les sites dans un VPN avec ce modèle est la topologie entièrement maillée ou «full mesh». Cela implique que tous les sites peuvent se voir ou bien qu'il existe une liaison point à point entre tous les sites du VPN.

IV-5 -2 Routeurs P, PE et CE architecture de VPN/MPLS:

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

IV-5 -2-1 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 ;

IV-5 -2-2 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 :

- Maintient des tables de routage et de forwarding pour chaque VPN.
- Echange des informations VPN avec les autres PE (utilisation de MP-BGP).
- Utilise de LSPs MPLS pour 'forwarder' le trafic VPN.

IV-5 -2-3 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.

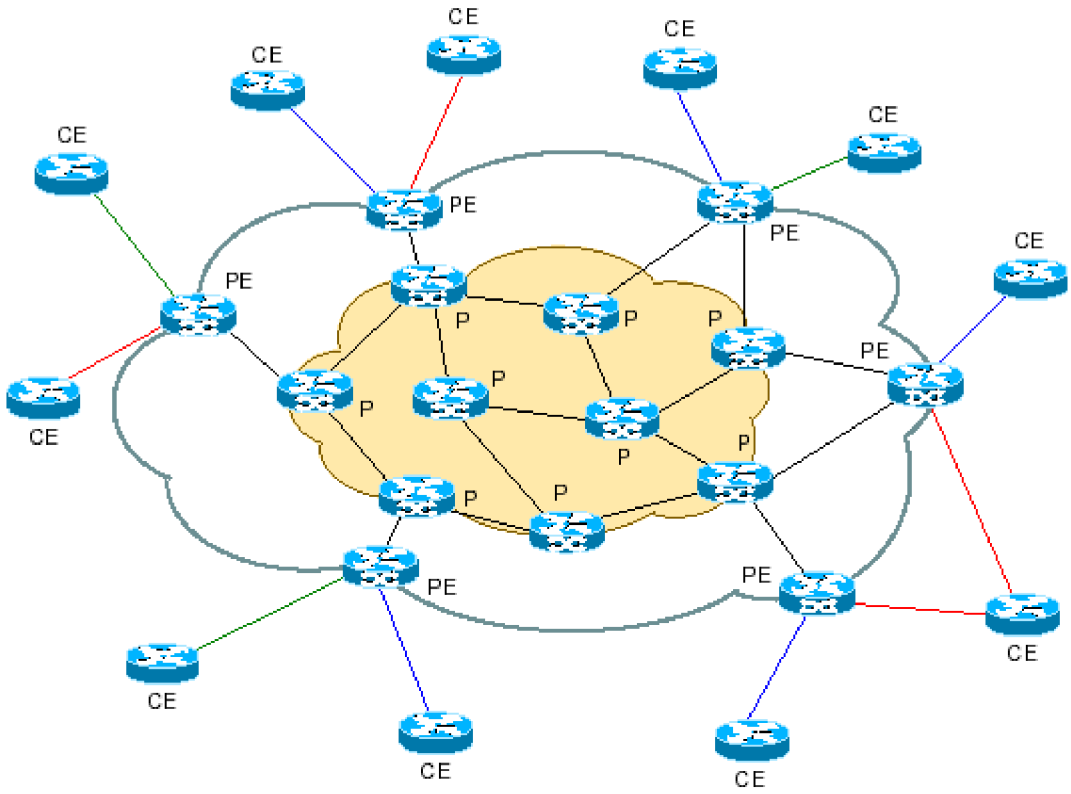


Figure IV-7: Emplacement de ces routeurs dans une architecture MPLS

IV-5 -3 Routeurs virtuels (VRF) :

La notion 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 FEC (*Forwarding Equivalent Class*) spécifiques, indépendantes des autres VRF et de la table de routage globale. Chaque VRF est désignée par un nom 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 interface 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.

Pour construire leurs tables VRF, les PE doivent s'échanger les routes correspondant aux différents VPN. En effet, pour router convenablement les paquets destinés à un PE

nommé PE-1, relié au site CE-1, le routeur PE-2 doit connaître les routes VPN de PE- 1. L'échange des routes VPN s'effectue grâce au protocole MP-BGP. Les configurations des VRF ne comportant que des paramètres relatifs à MP-BGP (notamment pour l'export et l'import des routes). La table FEC permet de déterminer le Next-Hop, l'interface de sortie et les labels utilisés pour atteindre un subnet particulier.

IV-5 -4 Multi-Protocol Border Gateway Protocol (MP-BGP):

Le protocole BGP permet le routage inter domaine. Il est notamment utilisé pour échanger les informations de routage sur Internet afin de relier entre eux les différents fournisseurs de service, représentés par des systèmes autonomes, nommés AS. C'est en effet le seul protocole pouvant supporter un très grand nombre de routes à annoncer, (Actuellement, près de 225000 routes sont contenues dans les tables de routage d'Internet Et qui permet de maintenir une certaine stabilité du routage.

BGP utilise notamment l'agrégation de routes, qui consiste à réunir en un seul préfixe (adresse réseau + masque explicite, par exemple 154.23.64.192/26) différentes adresses réseaux, en utilisant le principe de CIDR (Classless Inter-Domain Routing). Le routage dans BGP fonctionne par l'échange de messages UPDATE qui contiennent trois éléments :

- Les préfixes qui ne sont plus joignable par une route précédemment annoncée.
- Les attributs du chemin traversé depuis les préfixes annoncés, sous la forme d'un vecteur comportant les numéros d'AS traversés (AS_PATH).
- Les préfixes qui sont annoncés.

MP-BGP (Multi Protocol Border Gateway Protocol) : Utilisé pour l'échange de routes VPNv4. MP-BGP, qui n'est qu'une extension de BGP, a ainsi été standardisé pour permettre l'ajout d'informations supplémentaires aux messages UPDATE ; dans le cas des VPN sur MPLS il s'agit d'information sur les routes VPN échangées {Target VPN, VPN-of-origin, site-of-or-igin).

Le MP-BGP adopte une terminologie similaire à BGP concernant la convergence:

- MP-iBGP (Multi Protocol Interior Border Gateway Protocol) **:** convergence entre routeurs d'un même AS (Autonome System).

-**MP-eBGP** (Multi Protocol Exterior Border Gateway Protocol) **:** convergence entre routeurs situés dans 2 AS différents.

IV-5 -4-1 Notion de RD (Route Distinguisher) :

Le RD est employé pour transformer seulement des adresses de 32 bits non-uniques de la version 4 d'IP de client (IPv4) en adresses uniques de 96-bit VPNv4 (également appelées les adresses de VPN IPv4). Les adresses VPNv4 sont échangées seulement entre les routeurs PE, elles ne sont jamais employées entre les routeurs CE. Le protocole BGP doit donc supporter l'échange des préfixes IPv4 traditionnels aussi bien que l'échange des préfixes VPNv4 entre les routeurs PE. Une session de BGP entre les routeurs PE s'appelle par conséquent une session Multi-Protocole BGP (MP-BGP).

IV-5 -4 -2 Notion de RT (Route Target) :

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.

IV-5 -5 Fonctionnement VPN/MPLS :

Durant la conception d'un réseau d'entreprise, les ingénieurs choisissent généralement des plages d'adresses IP privées pour leur réseau LAN (10.0.0.0, 172.16.0.0, 192.168.0.0). Or le réseau MPLS permet l'implémentation de plusieurs VPN clients au sein de son réseau. Il faut par conséquent trouver un moyen de différencier les VPN qui peuvent avoir le même adressage IP. Afin de permettre aux différents sites d'un réseau privé de parler entre eux, il y a une procédure d'échange de routes, entre routeurs CE et PE d'une part, et entre routeurs PE d'autre part. Les CE envoient leurs routes aux PE par du routage statique ou dynamique. De même, les PE envoient les routes provenant des autres sites d'un même VPN aux CE, sur chaque PE, l'information de routage pour chaque VPN est maintenue dans des instances de routages de VPN.ces tables de routage sont appelées VRF. Une VRF donné correspond une ou plusieurs interfaces du client connectées au CE et appartenant au même VPN. Les PE

distribuent les routes reçues des CE et stockées dans les VRF aux autres PE qui connectent des sites du même VPN grâce au protocole MP-BGP.

L'espace d'adressage utilisé par chaque VPN pouvant se chevaucher, il est nécessaire de différencier les routes issues des différents VPN et ainsi éviter toute confusion quant à l'appartenance d'une adresse IP à un VPN donné. Pour y parvenir, les PE utilisent des *route distinguishers* qui sont ajoutés à chaque route VPN reçue d'un routeur CE. Avec cet ajout, il ne peut y avoir confusion avec l'information de contrôle de différents VPN. Il n'est alors plus question d'adresses IPv4 mais d'adresses VPN-IPv4 de 96 bit. Ainsi, les annonces de routes échangées par le protocole MP-BGP ne contiennent que des adresses VPN-IPv4 associées aux étiquettes VPN liées aux routes échangées. Les adresses VPNIPv4 ne sont toutefois utilisées que dans le cœur du réseau. Entre PE et CE, ce sont les adresses IPv4 usuelles qui sont utilisées. Cela cause, entre autres conséquences, que les CE ignorent ce qui se passe dans le cœur du réseau, n'ayant ainsi aucune visibilité sur les autres VPN déployés.

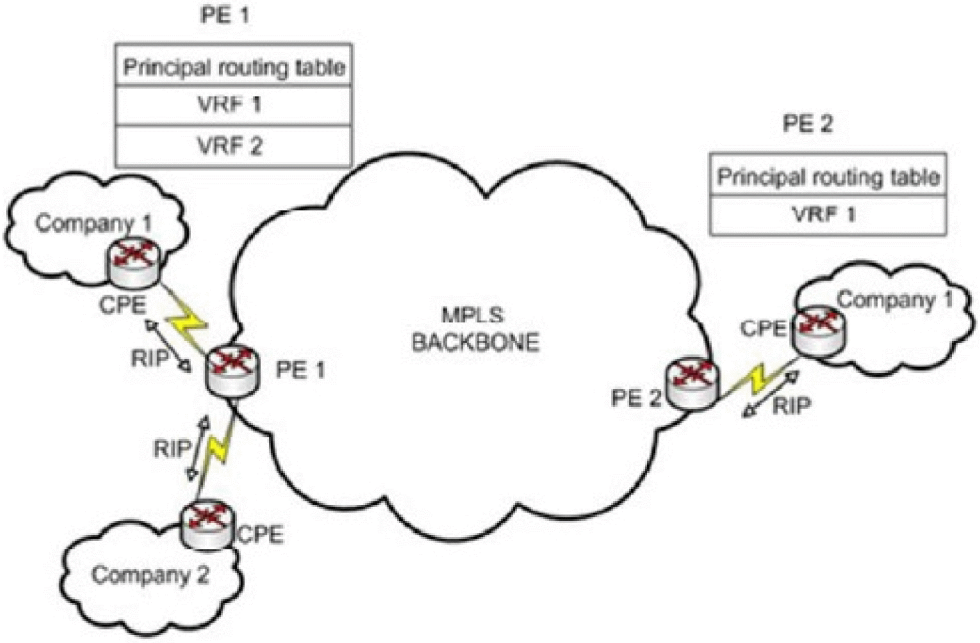


Figure IV-8: Principe de fonctionnement(1)

Sur la figure IV.8 les sites connectés au VPN matérialisant la connexion CE-PE peuvent communiquer avec l'intermédiaire d'une route statique ou encore avec un protocole IGP comme : RIP, OSPF EIGRP pour envoyer leurs informations vers le PE de l'opérateur.

Jusqu'à présent nous avons vu comment les sites clients envoyaient leurs informations vers les PE et comment les PE gérer ces différents VPN. Maintenant nous allons s'intéresser à la communication des sites clients mais du coté backbone MPLS.

Nous avons vu plus haut que les nœuds LSR utilisent un protocole IGP pour connaître leurs voisins dans les réseaux MPLS. Cela leur permettait de renseigner leur table LIB faisant l'association des FEC avec les labels, d'autre part, un protocole de distribution de label est utilisé pour échanger les labels et effectuer des mapping entre les nœuds LSR pour établir un LSP. Mais avec les VPN il y a eu l'introduction du RD (Route Distinguisher) afin de distinguer les différents VPN. Il a été décidé que pour les VPN implémentés sur les réseaux MPLS, le protocole d'échange de label serait le MP-BGP (Multi Protocol Border Gateway Protocol). Des sessions BGP sont établies entre deux PE et non entre un PE et P. Car en effet, entre le PE et les P routeur, le mécanisme qui s'applique est le «label swapping». Les routeurs PE s'échangent au travers de MP-BGP des *Routes Targets,* qui Définissent quelles routes doivent être importées ou exporter pour chaque VRF

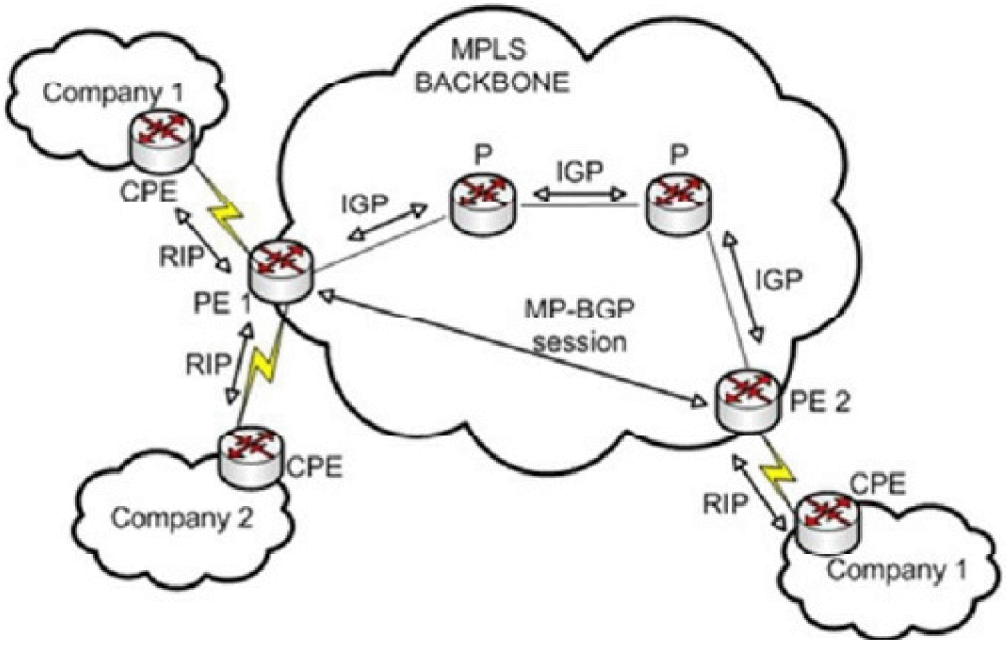


Figure IV-9: Principe de fonctionnement(2)

Lorsqu'un PE apprend une nouvelle route :

- Il insère dans sa VRF et il indique la joindre en EIGRP.

- Ensuite il annonce cette route avec les autres PE en établissant une session BGP en fournissant le label associé pour pouvoir atteindre ce VPN en question.
- Enfin, seul les PE sur lesquels les VRF ont été configurées vont rajouter ces routes dans leur table de routages.

Dès lors qu'il y a un transport de données entre les VPN, les CE envoient les paquets aux PE avec lesquels ils sont connectés. Les PE identifient à quels VPN ces CE font parties, ensuite ils consultent leur VRF et insèrent le label qui est associé au préfixe IP de destination et qui fait également partie de ce VPN. Pour cela, les *PE-ingress* réalisent un empilement d'étiquettes : en premier lieu, ils ajoutent une étiquette définissant le VPN auquel le paquet appartient, puis une seconde étiquette MPLS qui permet de diriger le paquet à travers le réseau MPLS, en étant changée à chaque routeur P traversé, jusqu'aux *PE-egress.* Ces étiquettes sont enlevées par ces derniers et les paquets sont transmis aux routeurs CE de destination comme de simples paquets IP, en fonction de la valeur de l'étiquette VPN. Dans le cas du *penultimate hop popping,* c'est le dernier routeur P traversé avant le routeur *PE-egress* qui enlève l'étiquette MPLS.

IV.6 MPLS-QoS(qualité de service):

Dans le monde les télécommunications, la QoS est un sigle qui signifie Quality of Service en anglais, que l'on traduit par « qualité de service » en français. La Qualité de Service est la capacité à véhiculer dans de bonnes conditions un type de trafic, en termes de disponibilité, débit, délais de transmission, taux de perte de paquet .Son but est ainsi d'optimiser les ressources du réseau et de garantir de bonnes performances aux applications critiques. La qualité de Service dans les réseaux permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par application. Elle permet ainsi aux fournisseurs de services (départements réseaux d'entreprises, opérateurs…) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP. Selon le type de service envisagé, la qualité pourra résider dans le débit (Téléchargement ou diffusion vidéo), le délai (pour les applications interactives ou la téléphonie), la disponibilité (accès à un service partagé) ou encore, le taux de pertes de paquets (pertes sans influence pour de la voix ou de la vidéo, mais critiques pour le Téléchargement). Il existe deux grands modèles pour implémenter la QoS dans un réseau:

-Integrated Services (IntServ)

-Differential Services (DiffServ)

IV-6-1 Le modèle IntServ:

Int-Serv 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 (messages RSVP, classification). IntServ permet donc une forte granularité de QoS par flux et pour cette raison, est plutôt destiné à être implémenté à l'accès.

IntServ définit 2 classes de services:

Guaranteed: garantie de bande passante, délai et pas de perte de trafic.
Controlled Load: fournit différents niveaux de services en best effort.

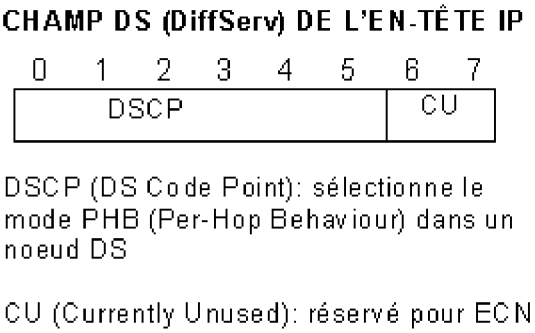
IV-6-2 DiffServ:

Quant à lui, est davantage destiné à être appliqué en cœur de réseau opérateur. Les différents flux, classifiés selon des règles prédéfinies, sont agrégés selon un nombre limité de classes de services, ce qui permet de minimiser la signalisation. DiffServ ne peut pas offrir de QoS de bout en bout et a un comportement Hop By Hop».

Le champ DS (Differenciated Services) aussi appelé CoS ou Exp est utilisé pour spécifier aux différents LSR quel traitement appliquer aux paquets IP (c'est à dire le plus souvent séparation du trafic selon la classe de service). Ce champ DS correspond à l'ancien champ ToS (Type of Service) de l'en-tête IP v4 qui a été renommé.

DiffServ définit 2 classifications de service (Expedited, Assured) qui peuvent être corrélées aux classifications de service IntServ (Guaranteed, Controlled Load).

MPLS est amené à inter fonctionner avec DiffServ, car LDP supporte avant tout de la QoS à faible granularité. Le mapping entre le champ DS de l'en-tête IP et le SHIM header de l'en-tête MPLS reste à définir.



IV.7 Extension MPLS:

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

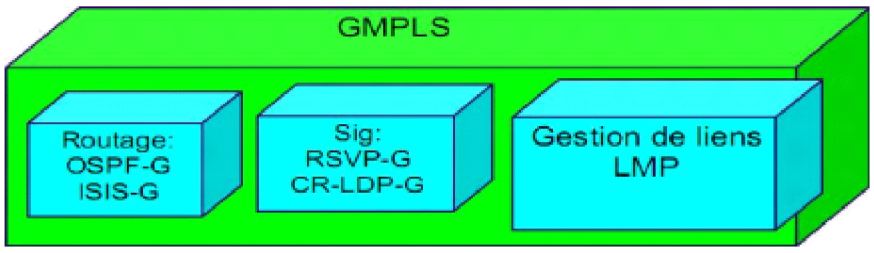


Figure IV-10: Architecteur GMPLS

Conclusion :

Au terme de ce chapitre, nous avons terminé l'étude théorique de la technologie MPLS: nous avons présenté les composantes relatives à l'ingénierie de trafic dans MPLS, et mise en ouvre d'un VPN dans MPLS, ainsi nous avons présenté les différents modèles utilisés pour la gestion de la QoS au niveau des réseaux MPLS.

Pour appliquer les concepts introduits précédemment, nous avons choisi une topologie de réseau qui permet la mise en œuvre d'un cœur de réseau IP /MPLS d'un fournisseur de service et simuler les différentes applications appropriées à MPLS (MPLS-TE, VPNs/MPLS, QOS.....), ainsi que l'implémentation de la « class based tunnel selection ».

Pour cela nous avons élaboré une plateforme sur GNS3 sur laquelle on a appliqué les techniques décrites précédemment, d'où les étapes suivantes :

· Réalisation de la plateforme du backbone avec VPN/MPLS.

· Implémentation de MPLS-TE.

· Implémentation de la «class based tunnel selection(CBTS)».

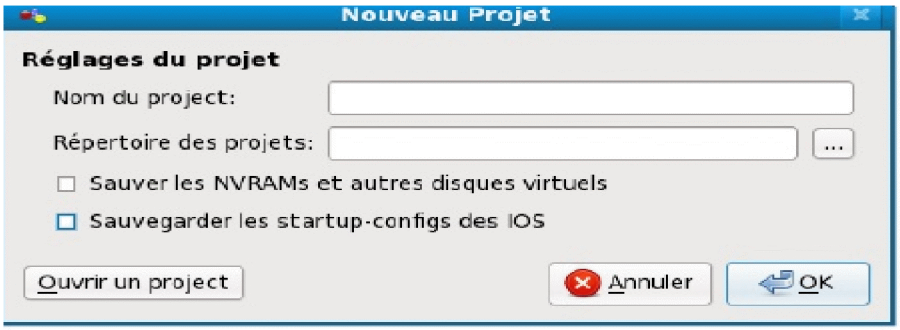
V-1. Logiciels utilisés :

V-1-1 Logiciel GNS3

GNS3 qui nous a permis de réaliser notre plateforme (réseau IP MPLS) est un logiciel d'émulation de routeur Cisco en mode graphique. Ce logiciel permet de simuler matériellement des routeurs 7200, 3600 et 2600... en utilisant les systèmes d'exploitation (IOS) de Cisco. Il fonctionne avec un outil de supervision des routeurs émulés : Dynagen. Ces outils fonctionnent sous Linux et Windows et permettent de simuler des topologies incluant tous les protocoles de l'IOS (RIP, EIGRP, OSPF). Il est aussi possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou de tester les configurations avant d'être déployées dans des routeurs réels. L'annexe A donne un aperçu sur l'utilisation du logiciel GNS3.

Les étapes de création et de configuration de la plateforme IP/MPLS sous GNS3:

Apres avoir créé la plateforme il faut sauvegarder à la fin pour y revenir il faut cocher les deux cases sur la fenêtre « **nouveau Projet** » comme le montre la figure suivante :



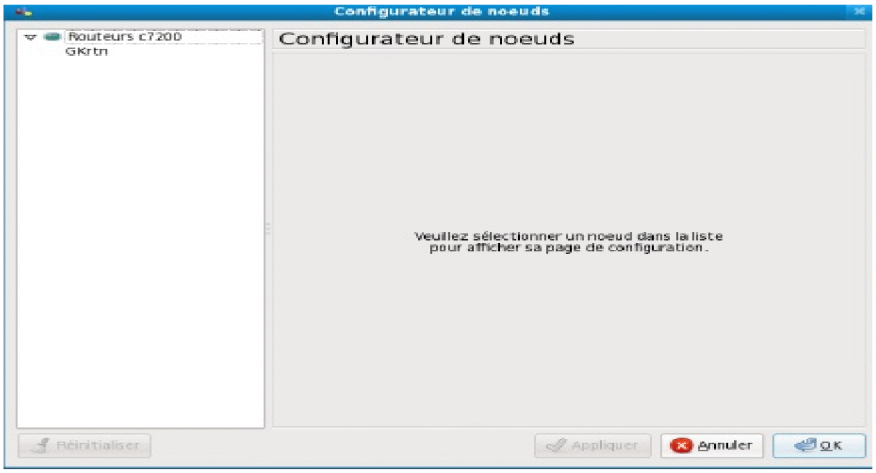
Pour notre cas : les routeurs utilisés sont des routeurs C7200.

On donne un nom à chaque routeur (clique droit sur le routeur et on clique à nouveau sur « changer le nom d'hôte ».

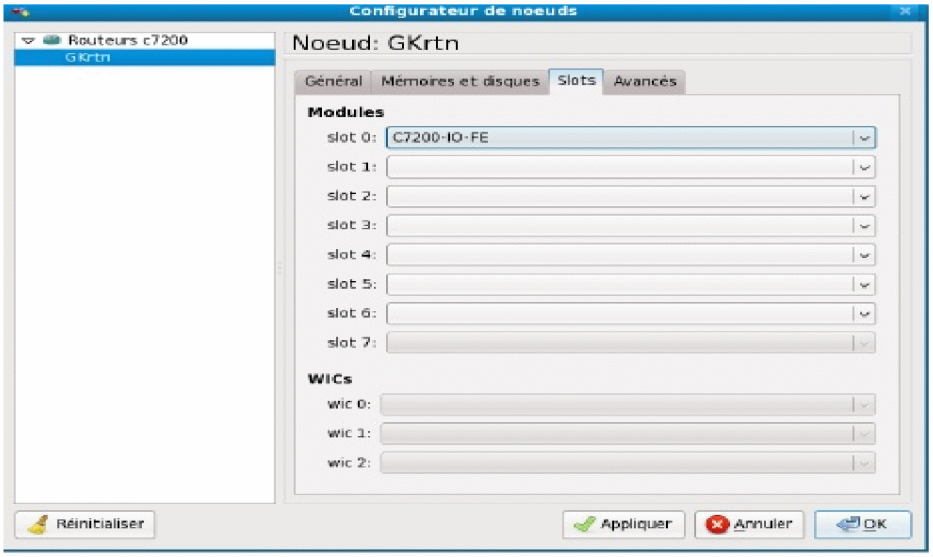
On a ceci

Clic « ok »

Pour avoir la figure suivante qui nous permet de configurer les routeurs (clic droit sur le routeur puis un autre sur configurer)

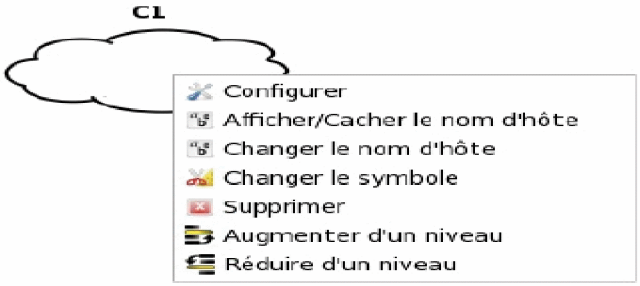


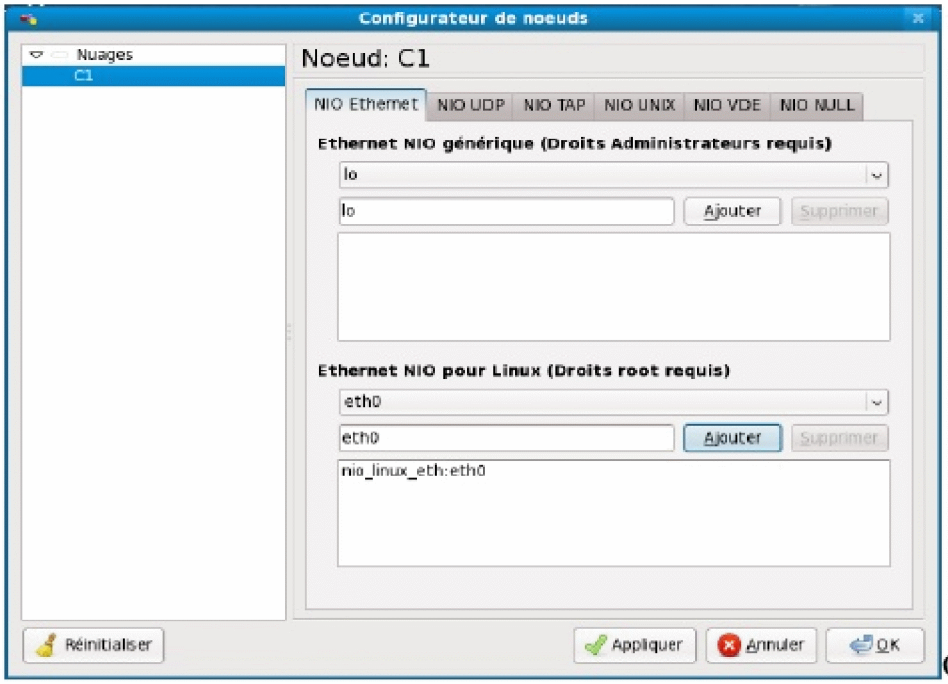
Ajout des slots au routeur pour avoir des interfaces.



Clic « Ok »

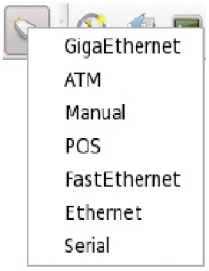
De même pour configurer un nuage (Cloud, clic droit/configurer)





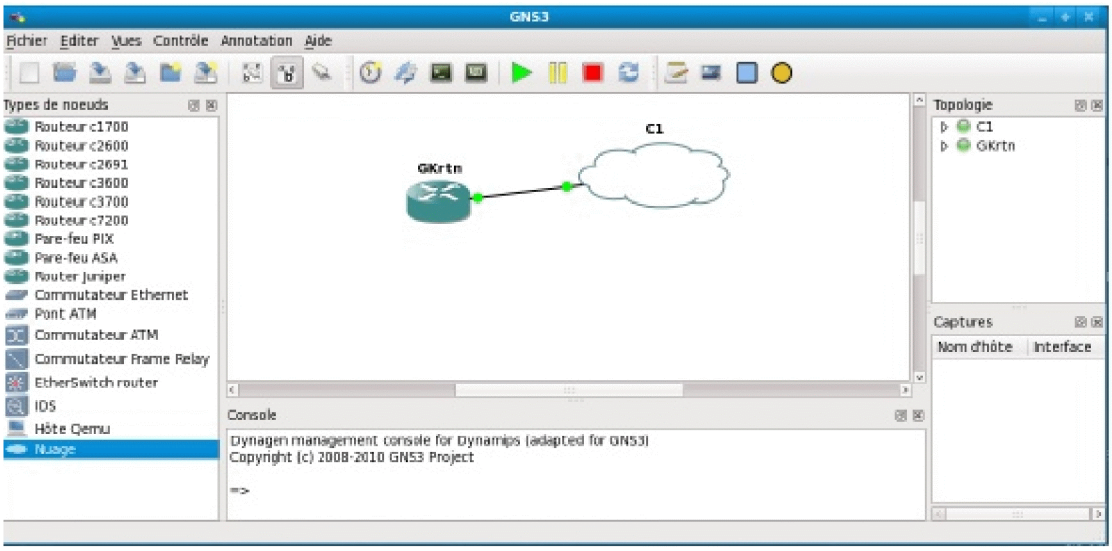
Clic « Ok »

Apres avoir formé la plateforme c'est-à-dire placer les routeurs et les nuages sur la partie centrale et les relier par des câbles (les câbles sont choisis a travers l'icône suivante sur la barre de menu en haut )



Après le choix du câble l'icône devient 

On redémarre les routeurs à travers le bouton suivant  et cela en sélectionnant en premier lieu le routeur qu'on veut démarrer.



Clic droit sur le routeur puis sur console pour configurer le routeur.

V-1-2 Le logiciel VMware Workstation :

Est un logiciels de virtualisation 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.

V-1-3 Installation du serveur FTP (File Transfer Protocol) :

C'est l'un des protocoles parmi les plus anciens et les plus utilisés. Son but est le transfert de manière sécurisée de fichiers entre les ordinateurs hôtes d'un réseau. Ce protocole permet aux utilisateurs d'accéder à des fichiers sur des systèmes distants en utilisant un ensemble standard de commandes simples.

V-2-Logiciel utilisé pour la supervision de la maquette :

V-2-1 Wireshark (anciennement Ethereal) :

Est un logiciel libre d'analyse de protocole, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage.

La force de Wireshark vient de:

- sa facilité d'installation.
- sa simplicité d'utilisation de son interface graphique.
- et son très grand nombre de fonctionnalités.

V-2-2 PRTG (Paessler Router Traffic Grapher) :

Est un logiciel qui supervise l'utilisation de la bande passante et d'autres paramètres réseau, géré via SNMP. Les informations sont présentées sous forme graphique via une interface Web qui permet de visualiser le volume de trafic en fonction du temps ce qui permet d'identifier les points de charge. PRTG tourne sur une machine Windows dans réseau et permet d'enregistrer constamment les paramètres de l'usage du réseau. Les données enregistrées sont par la suite sauvegardées dans une base de données interne pour être consultées ultérieurement. PRTG utilise SNMP pour enregistrer les données de trafic, de charge ou tout autre valeur accessible via SNMP à fin de les présenter sous forme graphique dans le temps sur des périodes plus ou moins longue.

V-3 Analyse des propriétés fonctionnelles d'un routeur :

Nous avons utilisé pour la réalisation de la maquette les routeurs de la gamme 7200 pour les raisons suivantes :

Le routeur Cisco 7200 est un routeur compact haute performance, conçu pour un déploiement à la périphérie du réseau et dans le centre de données, où performances et

services sont essentiels pour faire face aux besoins des entreprises, des administrations et des fournisseurs de services.

Le routeur Cisco 7200 est capable de gérer les applications suivantes :

- Accès haut débit à Internet pour professionnels et particuliers.
- Messagerie électronique.
- Téléphonie IP et FAX IP.
- Services VPN (Virtual Private Networking).
- E-business.

V-4 Mise en pratique des concepts fondamentaux des réseaux :

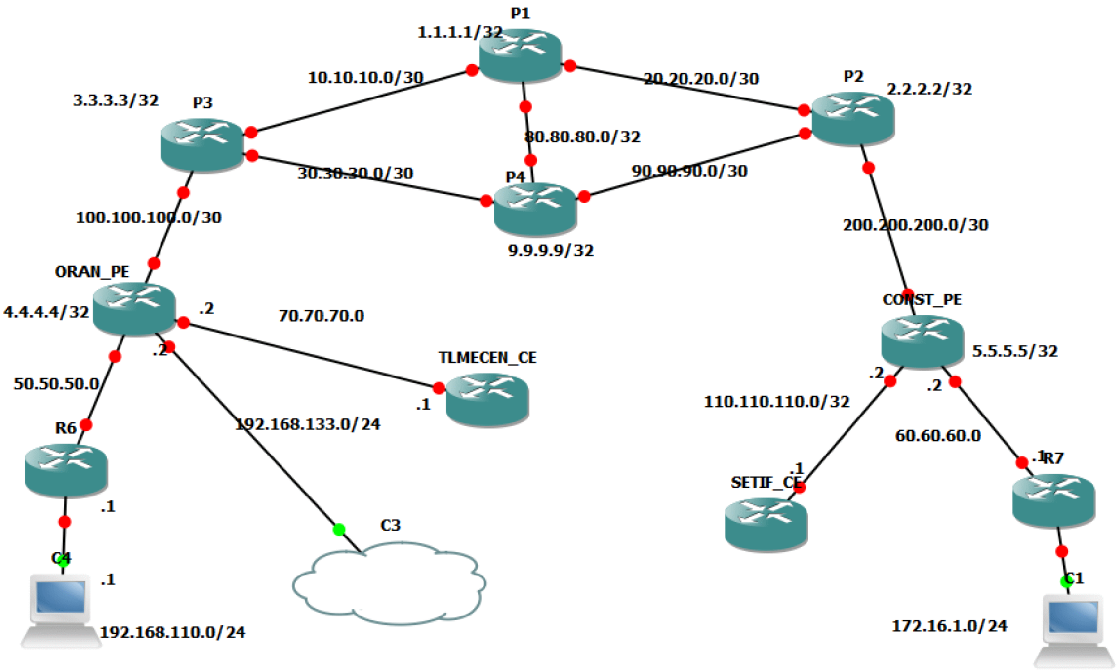
V-4-1 Configuration de la maquette :

Nous avons utilisé pour cette tâche 8 routeurs dont :

- ✓ 4 routeurs représentant le core MPLS (routeurs P) simulant les routeurs P1 ,P2 ,P3, P4
- ✓ 2 routeurs représentant l'edge MPLS (routeurs PE) et simulant les routeurs d'Oran et Constantine.
- ✓ 2 routeurs désignant les deux sites d'un client VPN (des routeurs CE) et simulant P6 et P7.
- ✓ 1 Cloud où est installé le logiciel PRTG avec une adresse de 192.168.133.0/24
- ✓ 2 machines virtuelles, une avec une adresse de 172.16.1.0/24 où a été installé le serveur FTP qui va permettre les transferts de fichiers avec l'autre machine d'où son adresse 192.168.1.0/24.

Les routeurs PE, P et CE utilise la version IOS «c7200- p-mz[1].124-10b.bin» supportant ainsi la technologie MPLS.

La figure suivante représente la topologie utilisée dans la maquette :



V-4-2 Configuration des interfaces des différents routeurs :

Routeur	Interface Loopback 0	Interface	Adresse Ip	Masque
P1	1.1.1.1 /32	G0/0 G1/0 G2/0	10.10.10.2 20.20.20.2 80.80.80.2	255.255.255.252
P2	2.2.2.2 /32	G0/0 G1/0 G2/0	90.90.90.2 20.20.20.1 200.200.200.2	255.255.255.252
P3	3.3.3.3 32	G0/0 G1/0 G2/0	30.30.30.1 10.10.10.1 100.100.100.2	255.255.255.252
P4	9.9.9.9 /32	G0/0 G1/0 G2/0	90.90.90.1 80.80.80.1 30.30.30.2	255.255.255.252
ORAN –PE	4.4.4.4 /32	G0/0 G2/0 G3/0	50.50.50.2 100.100.100.1 192.168.133.1	255.255.255.252 255.255.255.0
CONST-PE	5.5.5.5 /32	G0/0 G1/0	60.60.60.2 200.200.200.1	255.255.255.252
P6		G0/0 G1/0 E0/0	50.50.50.1 192.168.110.1 10.245.245.254.1	255.255.255.252 255.255.255.0
P7		G0/0 G1/0	172.16.1.1 60.60.60.1	255.255.255.0 255.255.255.252

V4-2-1Technologies utilisées :

On a choisi pour cette plateforme les technologies suivantes:

- OSPF pour la communication intra-nuage
- EIGRP en guise de protocole CE-PE.
- MP-BGP pour le VPN
- RSVP pour les tunnels LSP

Pour la configuration du backbone on est amené à suivre les phases suivantes :

V-5 Configuration des VPN/MPLS :

V-5-1 Etape 1 : activation du routage classique :

L'activation du routage classique au niveau du backbone (PE-P et P-P), le protocole de routage utilisé est l'OSPF, le choix de ce protocole est justifier par les raisons suivantes :

- L'OSPF est un protocole de routage d'état des liaisons sans classe qui utilise une hiérarchie de zone pour une convergence rapide.
- L'OSPF échange des paquets HELLO pour établir des contigüités entre les routeurs.
- L'algorithme SPF utilise une mesure de coût pour déterminer le meilleur chemin. Des coûts moindres indiquant un meilleur chemin.
- Utilise une interface de bouclage pour maintenir la cohérence de l'ID du routeur OSPF.

Sur les routeurs PE la configuration est la suivante :

```
ORAN-PE (config-if)#router ospf 1

ORAN-PE (config-router)# network 100.100.100.1 0.0.0.0  area 0

ORAN-PE (config-router)# network 4.4.4.4  0.0.0.0  area 0
```

C'est la même configuration pour le routeur PE de Constantine en adaptant les IPs.

Sur les routeurs Px (P1 à P4) la configuration est la suivante :

```
P1 (config-if)#router ospf 1

P1 (config-router)# network 10.10.10.1 0.0.0.0 area 0

P1 (config-router)# network 20.20.20.2  0.0.0.0 area 0

P1 (config-router)# network 80.80.80.2  0.0.0.0  area 0

P1 (config-router)# network 1.1.1.1  0.0.0.0  area 0
```

Les mêmes étapes seront suivies pour la configuration des routeurs P2, P3 et P4 en adaptant les adresses IPs.

V-2 Etape 2. Activation du MPLS :

Seuls les routeurs PE et P supportent MPLS, donc l'activation est réalisée à ce niveau. Avant de configurer MPLS sur les interfaces des routeurs, il est indispensable d'activer le CEF(Cisco Express Forwarding). Le Cisco Express Forwarding (CEF) est une technologie Couche 3 qui fournit une évolutivité de transfert et d'exécution accrus pour gérer plusieurs flux de trafic de courte durée. L'architecture CEF place seulement les préfixes de routage dans ses tables CEF (la seule information qu'elle requiert pour prendre des décisions de transfert Couche 3) se fondant sur les protocoles de routage pour faire le choix de l'itinéraire. En exécutant une consultation de simple table CEF, le routeur transfert les paquets rapidement et indépendamment du nombre de flux transitant.

Nous avons choisit LDP (*Label Distribution Protocol*) pour distribuer les labels MPLS. Comme les interfaces des routeurs dans notre maquette sont de type série, la configuration est la suivante :

```
P1 (config)#ip cef

P1 (config)#mpls ip

P1 (config-if)#int g0/0

P1 (config-if)#ip cef

P1 (config)#mpls ip

P1 (config)#int g1/0

P1 (config-if)#ip cef

P1 (config)#mpls ip

P1(config)#int g3/0

P1(config-if)#ip cef

P1 (config)#mpls ip
```

Nous introduirons aussi la même configuration pour les routeurs P2, P3, P4 et l'interface qui relie le routeur ORAN-PE avec routeur P1 (ainsi que pour le routeur CONST-PE avec P2).

V-5-3 Etape 3. Mise en place des VRF sur les PE :

L'une des applications les plus importantes du protocole MPLS est de pouvoir créer des réseaux privés virtuels VPN (Virtual Private Network), pour cela nous avons implémenté dans notre maquette un VPN MPLS qui relie deux cites client d'Oran et Constantine.

Pour assurez l'isolation du trafic entre les différents clients, nous avons créé dans les routeurs Edge qui connectent les réseaux des clients, une **VRF** pour chaque client. Pour notre client de démonstration, nous avons défini un VRF avec les paramètres suivants:

Route distinguisher 100 :1

Route target import 100 :1

Route target export 100 :1

Autonomous-system 100

```
Oran- PE #conf t
Enter configuration commands, one per line. End with CNTL/Z.
Oran- PE(config)#ip vrf Oran
Oran- PE(config-vrf)#rd 100 :1
Oran- PE(config-vrf)#route import 100 :1
Oran -PE(config-vrf)#route export 100 :1
Oran -PE(config-vrf)#exit
```

Cette étape est bien entendu à répéter sur PE- Constantine qui accueillera exactement la même configuration.

V-5-4 Etape.4. Configuration des interfaces :

Outre la configuration des IPs, nous devons également effectuer plusieurs actions pour « préparer le terrain »:

- Sur toutes les interfaces des PE directement reliées sur des CE, nous devons assigner à l'interface locale du PE une VRF.

Assignation d'une VRF sur un port de routeur

```
Oran- PE(config)#int g0/0

Oran -PE(config-if)#ip vrf forwarding Oran

Oran- PE(config-if)#ip add 50.50.50.2 255.255.255.252

Oran- PE(config-if)#no sh
```

Avec cette commande *ip vrf forwarding*, on affecte l'interface de la VRF choisie uniquement. Cette opération est à répéter également sur PE-Constantine en adaptant les adresses IPs

V-5-5 Etape 5 Mise en place du protocole CE-PE :

V-5-5 -1 Protocole utilisée est EIGRP :

Le protocole **EIGRP** se trouve entre les routeurs clients et edge (CE-PE) à cause du MPLS- VPN qui offre la possibilité d'utiliser n'import quel protocole de routage dans les sites des clients. Ainsi l'échange des routes entre les routeurs PE est assuré par le protocole MP-BGP.

Caractéristique de EIGRP sont les suivants :

- Mise à jour déclenchées (EIGRP n'a pas de mises à jour régulières).
- Utilisation d'une table topologique pour maintenir toutes les routes reçues des voisins (pas seulement les meilleurs chemins).
- Etablissement de contigüités avec des routeurs voisins par le bais du protocole HELLO EIGRP.
- Prise en charge des masque de sous –réseau de longueur variable et du résumé des routes manuel, permettant ainsi au protocole EIGRP de créer de grands réseaux structurés hiérarchiquement.

Dans un premier temps, la configuration dédiée aux CE est très simple, du fait que le CE n'a aucune notion de MPLS, il va juste établir une adjacence avec le PE auquel il est relié et partager ses routes avec celui-ci.

Cette configuration sera à appliquer aussi sur le routeur P7 en ne changeant que l'adresse IP.

```
P6 (config)#router eigrp 100
P6 (config-router)#network 192.168.110.0
P6 (config-router)#network 10.0.0.0
P6 (config-router)#network 50.50.50.0
P6 (config-router)#no auto-summary
```

Dans le cas de la configuration du PE, un peu plus complexe, nous allons configurer dans le PE une instance d'EIGRP par VRF. Ces commandes s'appliqueront sur PE-Oran et PE-Constantine en adaptent les IPs.

```
Oran -PE(config)#router eigrp 1
Oran -PE(config-router)#address-family ipv4 vrf Oran
Oran- PE(config-router-af)#network 50.50.50.0
Oran- PE(config-router-af)#no auto-summary
Oran- PE(config-router-af)#autonomous-system 100
Oran -PE(config-router-af)#exit
```

V-5-6 Etape 6. Mise en place du protocole MP-BGP :

Pour configurer la liaison VPN IPV4 entre les deux PE que l'on recherche à faire, il nous faut configurer sur les deux routeurs, comme on le ferait en BGP, une relation de voisinage en prenant comme référence les IPs de loopback paramétrées précédemment.

La configuration pour Oran- PE est la suivante :

```
Oran- PE (config)#router bgp 1
Oran- PE (config-router)#neighbor 5.5.5.5 remote-as 1
Oran- PE (config-router)#neighbor 5.5.5.5 update-source Lo0
Oran- PE (config-router)#address-family vpnv4
```

```
Oran- PE (config-router-af)#neighbor 5.5.5.5 activate

Oran- PE (config-router-af)#neighbor 5.5.5.5 send-community both

Oran- PE (config-router-af)#exit

Oran- PE (config-router)#exit
```

Enfin, on active le mécanisme VPN IPV4 de BGP en le configurant également de telle sorte à ce que BGP utilise le champ « community » de ses updates pour pouvoir en faire un champ de communauté étendue (qui servira lors de la négociation des capacités des voisins et des RT qui sont stockés également dans ce champ).

La configuration pour PE-Constanntine est exactement la même en adaptant les IPs:

```
CONST-PE(config)#router bgp 1
CONST-PE (config-router)#neighbor 4.4.4.4 remote-as 1
CONST-PE (config-router)#neighbor 4.4.4.4 update-source Lo0
CONST-PE (config-router)#address-family vpnv4
CONST-PE (config-router-af)#neighbor 4.4.4.4 activate
CONST-PE (config-router-af)#neighbor 4.4.4.4 send-community both
CONST-PE (config-router-af)#exit
CONST-PE (config-router)#exit
```

V-5-7 Etape 7. Gestion de la redistribution respective des préfixes :

Avant de pouvoir tester le bon fonctionnement de notre VPN, il nous manque encore une brique importante de notre architecture. Il faut configurer les PE de telle sorte à ce que la redistribution des routes soit effective mutuellement dans les deux sens entre BGP et EIGRP

Dans le cas où un client rajoute une route sur son CE, la route est automatiquement redistribuée dans BGP et les autres PE seront directement au courant de ce nouveau préfixe sans aucune intervention.

V-5-7-1 Redistribution EIGRP => BGP – configuration:

La configuration suivante permet la redistribution des routes apprises par EIGRP dans BGP. Une configuration similaire est également à appliquer sur PE-Constantine.

```
Oran- PE (config)#router bgp 1
```

```
Oran- PE (config-router)#address-family ipv4 vrf Oran

Oran- PE (config-router-af)#redistribute eigrp 100

Oran- PE (config-router-af)#exit
```

V-5-7-2 Redistribution BGP => EIGRP – configuration:

Après cela, on s'occupera de la redistribution des routes apprises par BGP dans EIGRP. La configuration similaire est également à appliquer sur PE-Constantine.

```
Oran- PE (config)#router eigrp 1
Oran- PE (config-router)#address-family ipv4 vrf Oran
Oran- PE (config-router-af)#redistribute bgp 1 metric 1000000 4000 200 10 1500
Oran- PE (config-router-af)#exit
```

V-5-8 Tests et vérifications :

On se place sur le routeur P6 qui a envie de contacter P7 à travers le VPN MPLS.

Le résultat est le suivant :

```
P6#ping 60.60.60.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 60.60.60.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/64/88 ms

P6#ping 60.60.60.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 60.60.60.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 68/80/88 ms
```

V-6 Configuration des MPLS-TE :

Dans cette section nous allons voir l'objectif de l'utilisation de l'ingénierie de trafic (TE) pour acheminer les données des clients (VPNs), mettre en place les mécanismes d'ingénierie de trafic avec MPLS et montrer comment le trafic des VPNs peut utiliser les tunnels construit par TE.

V-6 -1 Activation de MPLS TE : dans tous les routeurs PE et P, et dans toutes les interfaces qui vont participer à la création des tunnels.

La même configuration est à réaliser pour tous les routeurs PE (Constantine, Oran) et pour les routeurs P2, P3, P4.

```
P1 (config)#mpls traffic-eng tunnels

P1 (config)#router ospf 1

P1 (config-router)#mpls traffic-eng router-id loopback 0

P1 (config-router)#mpls traffic-eng area 0
```

V-6 -2 Configuration du protocole PSVP-TE : Configuration de la réservation de la bande passante dans l'interface MPLS TE par RSVP sur tous les routeurs PE et P sur toutes les interfaces.

```
P1 (config-router)#int G0/0

P1 (config)#mpls traffic-eng tunnels

P1 (config)#ip rsvp bandwith 10000
```

V-6 -3 Création des tunnels LSP : Création des tunnels explicites : nous avons crée deux tunnels 0 et 1.

Configuration du Tunnel 0 :

```
ORAN-PE (config)# interface tunnel 0
ORAN-PE (config-if)# ip unnumbered loopback 0
ORAN-PE (config-if)# tunnel destination 5.5.5.5
ORAN-PE (config-if)# tunnel mode mpls traffic-eng
ORAN-PE (config-if)# tunnel mpls traffic-eng autoroute announce
ORAN-PE (config-if)# tunnel mpls traffic-eng priority 1 1
ORAN-PE (config-if)# tunnel mpls traffic-eng bandwidth 100
ORAN-PE (config-if)# tunnel mpls traffic-eng path-option 1 explicit name LSP0
ORAN-PE (cfg-ip-expl-path)# next-address 100.100.100.2
ORAN-PE (cfg-ip-expl-path)#  next-address 10.10.10.2
ORAN-PE (cfg-ip-expl-path)#  next-address 20.20.20.1
ORAN-PE (cfg-ip-expl-path)# next-address 200.200.200.1
ORAN-PE (cfg-ip-expl-path)#  next-address 5.5.5.5
```

Configuration de tunnel 1 explicite:

```
ORAN-PE (config)# interface tunnel 1
ORAN-PE (config-if)# ip unnumbered loopback 0
ORAN-PE (config-if)# tunnel destination 5.5.5.5
ORAN-PE (config-if)# tunnel mode mpls traffic-eng
ORAN-PE (config-if)# tunnel mpls traffic-eng autoroute announce
ORAN-PE (config-if)# tunnel mpls traffic-eng priority 2 2
ORAN-PE (config-if)# tunnel mpls traffic-eng bandwidth 100
ORAN-PE (config-if)# tunnel mpls traffic-eng path-option 2 explicit name LSP1
ORAN-PE (cfg-ip-expl-path)# next-address 100.100.100.2
ORAN-PE (cfg-ip-expl-path)#  next-address 30.30.30.2
ORAN-PE (cfg-ip-expl-path)#  next-address 90.90.90.2
ORAN-PE (cfg-ip-expl-path)# next-address 200.200.200.1
```

```
ORAN-PE (cfg-ip-expl-path)#  next-address 5.5.5.5
```

V-7 La mise en œuvre sélection du tunnel Class-Based(CBTS) :

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).

V-7-1Configuration du protocole SNMP (protocole simple de gestion de réseau) :

C'est un protocole de communication qui permet aux administrateurs réseaux de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels et tout cela à distance.

La configuration est la suivante :

```
ORAN_PE (config)#snmp-server host 192.168.133.100 public
ORAN_PE (config)#snmp-server community public
ORAN_PE (config)#snmp-server enable traps
```

V-7-2 Création des access list : qui permettent d'autoriser le trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, …).

```
P6 (config)# access-list101 permit ip 192.168.110.100 0.0.0.0 172.16.1.100 0.0.0.

P6 (config)# access-list 102  permit ip 10.245.245.1  0.0.0.0  172.16.1.100 0.0.0.0
```

V-7-2 Création des classes :

Lorsque l'on souhaite mettre en place une qualité de service sur un réseau, une configuration du matériel est nécessaire. Cette configuration se fait alors suivant plusieurs étapes :

- Création de "class-map"
- Création de "policy-map"
- Création de "service policy"

V-7-2-1 Création des "class-map" :

Dans un réseau, il est nécessaire de différencier les types de trafics pour pouvoir gérer leurs priorités. Les "class-map" (littéralement "plan de classes") permettent une classification de ces types de flux.

On a crée deux class-map

1ère class-map:

```
P6 (config)#class-map mobilis
P6 (config-cmap)#match access-group 101
P6 (config-cmap)#description flux- media gateway
```

2ème class-map:

```
P6 (config)#class-map mobilis1
P6 (config-cmap)#match access-group 102
P6 (config-cmap)#description flux-internet
```

V-7-2-2 :Création des "policy-map"

Une "policy-map" permet de définir une action associée à une "class-map", c'est-à-dire, le traitement à lui appliquer comme par exemple une bande passante pour un flux de données.

```
P6 (config)# policy-map mobilis
P6 (config)#class mobilis
P6 (config-cmap)#set precedence 7
P6 (config)#class mobilis1
P6 (config-cmap)#set precedence 5
```

V-7-2-3 :Création des "service-policy"

Les "service policy" permettent d'attacher des politiques à des interfaces du routeur. En fonction du type de trafic, on peut attacher ces politiques soit sur l'interface sortante, soit sur l'interface entrante. On peut ainsi éviter les congestions à l'entrée du routeur en limitant la quantité de paquets sur l'interface entrante. De plus, si l'on souhaite assurer une priorité sur des paquets en direction de l'extérieur, on peut appliquer ces politiques sur l'interface sortante.

La configuration est la suivantes :

```
P6 (config)#int g0/0
P6 (config-if)#service-policy output mobilis
```

Configuration des valeurs exp :

La configuration du routeur ORAN-PE montre que le tunnel 0 transporte un paquet avec MPLS valeur exp 5 et le tunnel 1 avec une valeur exp 7. La valeur exp indique le paquet prioritaire.

```
ORAN_PE (config)#int tunnel 0
ORAN_PE (config-if)#tunnel mpls traffic-eng exp 5
ORAN_PE (config)#int tunnel 1
ORAN_PE (config-if)#tunnel mpls traffic-eng exp 7
```

V-7-3 Configuration Master tunnel :

C'est un tunnel qui permet de gérer les 2 tunnels explicites qu'on a créé (tunnel 0 et tunnel 1)

```
ORAN_PE (config-if)#interface Tunnel10
ORAN_PE (config-if)# description qos master bandle
ORAN_PE (config-if)# ip unnumbered Loopback0
ORAN_PE (config-if)# tunnel mode mpls traffic-eng
ORAN_PE (config-if)# tunnel destination 5.5.5.5
ORAN_PE (config-if)# tunnel mpls traffic-eng autoroute announce
ORAN_PE(config-if)# tunnel mpls traffic-eng path-option 100 dynamic
ORAN_PE(config-if)# tunnel mpls traffic-eng exp-bundle master
ORAN_PE(config-if)# tunnel mpls traffic-eng exp-bundle member Tunnel0
ORAN_PE(config-if)# tunnel mpls traffic-eng exp-bundle member Tunnel1
```

Quelques commandes de Vérification :

Pour le test du bon fonctionnement de la configuration de la plateforme, plusieurs commandes sont disponibles, notamment :

show ip vrf : vérifie l'existence de la table VFR.

show ip vrf interfaces : Vérifies les interfaces actives.

show ip bgp vpnv4 tag: Vérifie le protocole de routage BGP.

sh mpls forwarding-table : vérifie les labels utilisés.

sh ip ospf : vérifie la table de routage ospf.

sh ip route : table mentionnant les routes du routeur

sh mpls traffic-eng tunnel : vérifie des tunnels.

sh mpls traffic-eng tunnel brief : vérifie les interfaces des tunnels.

Conclusion générale :

De nos jours, les quantités de données transportées sur les réseaux et le développement des technologies à contrainte temporelle telles que la VoIP ou les applications vidéo sont de plus en plus importantes et requièrent l'utilisation d'un réseau pouvant respecter ces besoins. De plus le routage IP actuel ne satisfait pas aux contraintes qui sont désormais de l'ordre de la bande passante et du temps de transmission. Le mode "best effort" de l'IP devient alors trop limité pour l'utilisation souhaité. La convergence audio / vidéo / données sollicite ainsi des réseaux à très haut débit.

D'où le développement de nouvelles technologies telles MPLS qui a su prendre une place prépondérante dans les réseaux longue distance des opérateurs. Son but premier, qui était d'optimiser le temps de traitement des paquets au sein du cœur de réseau s'est peu à peu effacé pour laisser placer aux extensions et applications du MPLS. MPLS offre ainsi plusieurs services intéressants à exploiter et ne nécessite pas forcément d'investissement conséquent lors de sa mise en place. La logique modulaire selon laquelle le MPLS a été développé permet de l'étendre avec beaucoup de souplesse, comme en témoigne l'apparition du GMPLS destiné à devenir un standard.

L'objectif premier de notre projet de fin d'étude est l'analyse des performances de MPLS et les applications offertes par se réseau à savoir la prise en charge du "Traffic Engineering" qui permet une meilleure gestion du trafic sur le réseau en se basant sur des mécanismes de classification du trafic et de commutation de label. La nécessité d'optimiser les performances, les ressources ainsi que les flux sur un réseau opérationnel a fait apparaître la notion de TE : « Trafic Engineering ». Sur les réseaux MPLS, l'utilisation du protocole RSVP-TE permet de répondre à ces besoins. Grâce a ses fonctionnalités avancées de gestion, d'optimisation et de routage du trafic, associées à la détection d'erreurs, le protocole RSVP-TE apporte une complémentarité essentielle sur un réseau MPLS avec la Qualité de Service (QoS) et le Traffic Engineering. Nous avons aussi abordé le VPN /MPLS qui est une topologie qui consiste à interconnecter les sites des clients via un réseau opérateur utilisant comme technologie de transport MPLS.

Toujours dans le cadre de notre étude, nous avons aussi contribué à la mise en œuvre du cœur d'un backbone de commutation IP/MPLS dans le réseau de télécommunication national qui constituera désormais le cœur de l'architecture du futur réseau de télécommunication national type NGN en cours de déploiement chez ATM Mobilis.

Annexes

❖ **Présentation du simulateur GNS 3 :**

GNS3 est un simulateur graphique de réseaux qui vous permet de créer des topologies de réseaux complexes et d'en établir des simulations. Ce logiciel, en lien avec Dynamips (simulateur IOS), Dynagen (interface textuelle pour Dynamips) et Pemu (émulateur PIX), est **un excellent outil pour l'administration des réseaux CISCO, les laboratoires réseaux ou les personnes désireuses de s'entraîner avant de passer les certifications** CCNA, CCNP, CCIP ou CCIE. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou de tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment Open Source et multi-plates-formes. Il est possible de le trouver pour Mac OS X, Windows et évidemment pour une distribution Linux.
Remarque importante : l'utilisateur doit fournir ses propres images IOS pour utiliser GNS3.

❖ **Présentation de dynamips**

Dynamips est un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées comme si elles s'exécutaient sur de véritables équipements. Le rôle de Dynamips n'est pas de remplacer de véritables routeurs, mais de permettre la réalisation de maquettes complexes avec de vraies versions d'IOS. Contrairement à certains autres produits, il ne s'agit pas d'une émulation de la ligne de commande IOS et de son fonctionnement, mais d'une émulation complète du « hardware ». Dynamips peut être utilisé à des fins de formation, d'expérimentation, aide au diagnostic, validation de configurations, ...
Dynamips est écrit en langage C, sous licence GPL. Les plateformes hôtes supportées sont de type PC sous Linux, Mac Os X et Windows. Un portage sur d'autres plateformes Unix est également possible.
Les gammes de routeurs émulés sont:
• Cisco7200 (NPE-100 jusqu'à NPE-400, NPE-G2)
• Cisco 3600 (3620, 3640, 3660)
• Cisco 3700 (3725, 3745)

• Cisco 2600 (2610 à 2651XM, 2691)
• Cisco 1700 (1710 à 1760)
Différentes instances de l'émulateur peuvent être interconnectées à travers ces interfaces. Une connexion à un réseau réel est réalisable en Ethernet via une interface physique du serveur hôte. Dynamips fonctionnant uniquement en ligne de commande, des projets connexes non portés par l'UTC ont vu le jour :

-Dynagen est un produit complémentaire écrit en Python s'interfaçant avec Dynamips grâce au mode hyperviseur. Dynagen facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive.

-GNS-3 reprend ces mêmes fonctionnalités sous forme d'interface graphique. Ecrit en Python, il s'appuie sur des modules de Dynagen.

- **Installation de GNS 3**
- **Téléchargement du GNS 3 :**

télécharger le logiciel GNS 3 à partir du site officiel http://www.gns3.net .

Figure 1 : site de téléchargement du GNS3

Figure 1 : site de téléchargement du GNS3

Télécharger le paquet GNS3 v0.7.3 all-in-one. Après l'avoir téléchargé, on lance l'installation comme suit :

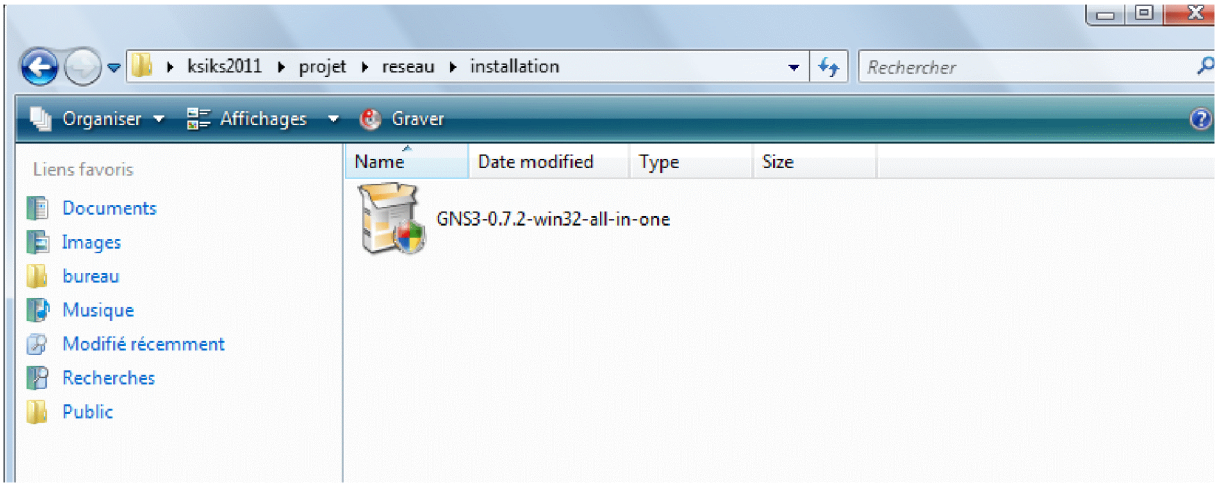


Figure 2 : Le setup du GNS3

Sur la page d'accueil du GNS 3, cliquer sur suivant pour continuer :

Figure 3 : fenêtre 1 de l'installation

Accepter la License et on continue l'installation :

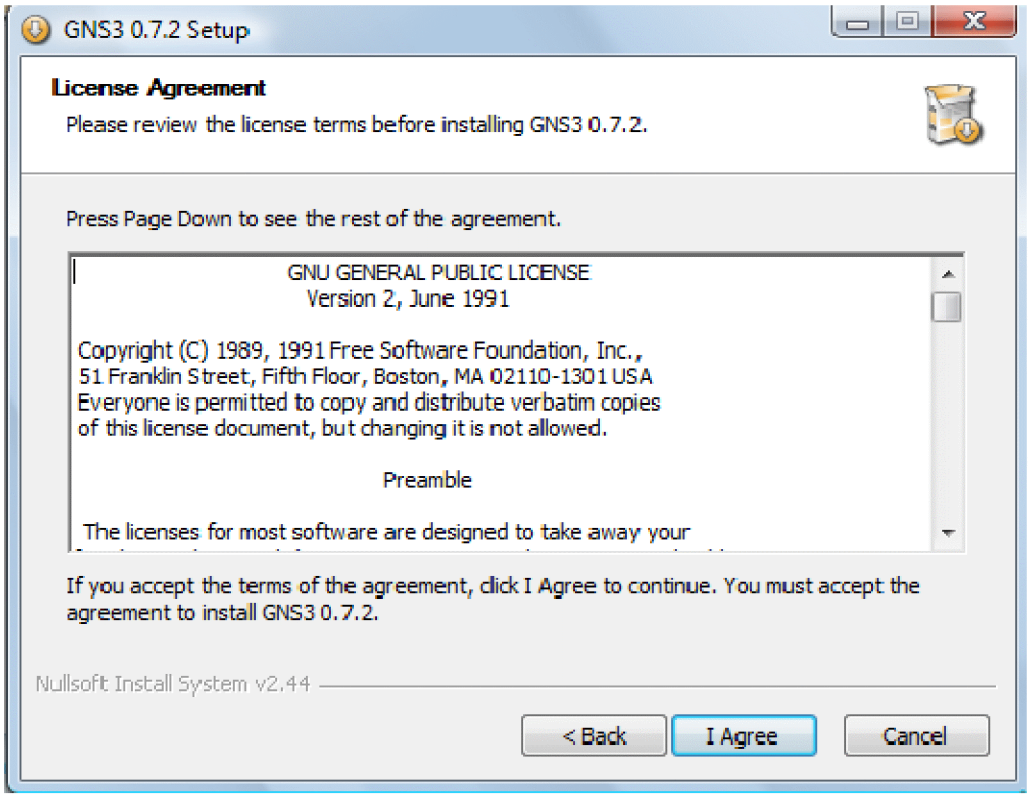


Figure 4 : fenêtre 2 de l'installation du GNS3

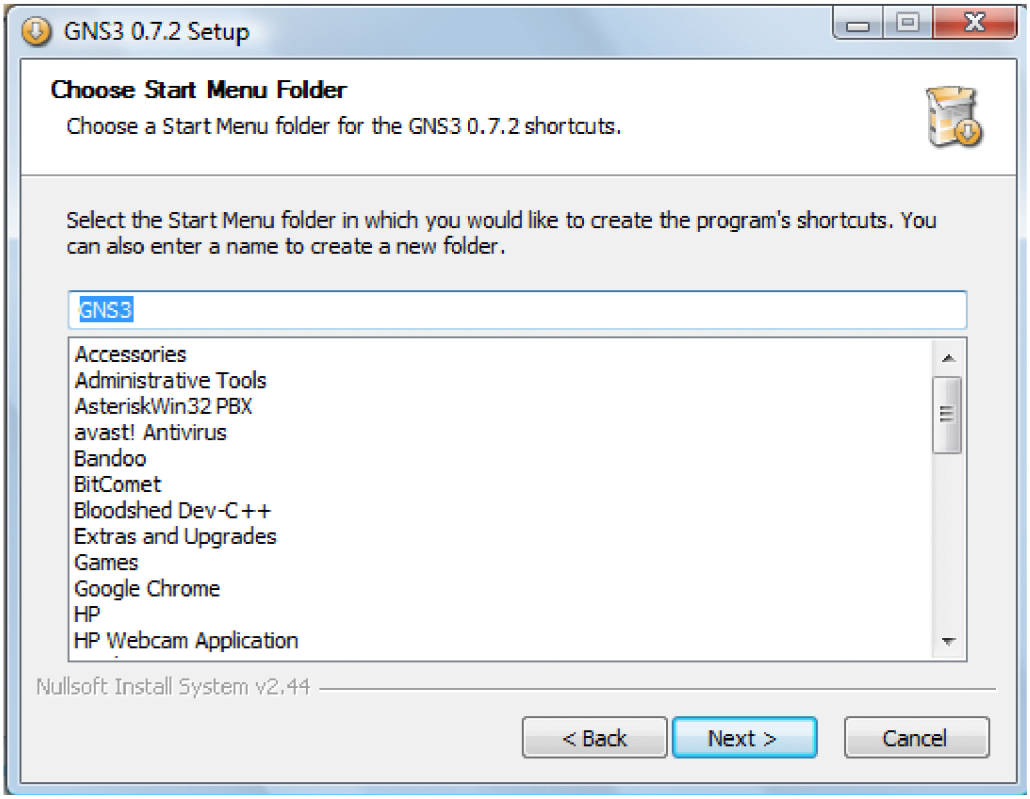


Figure 5 : fenêtre 3 de l'installation du GNS3

Cocher toutes les cases pour installer les éléments nécessaires pour le fonctionnement du GNS 3.

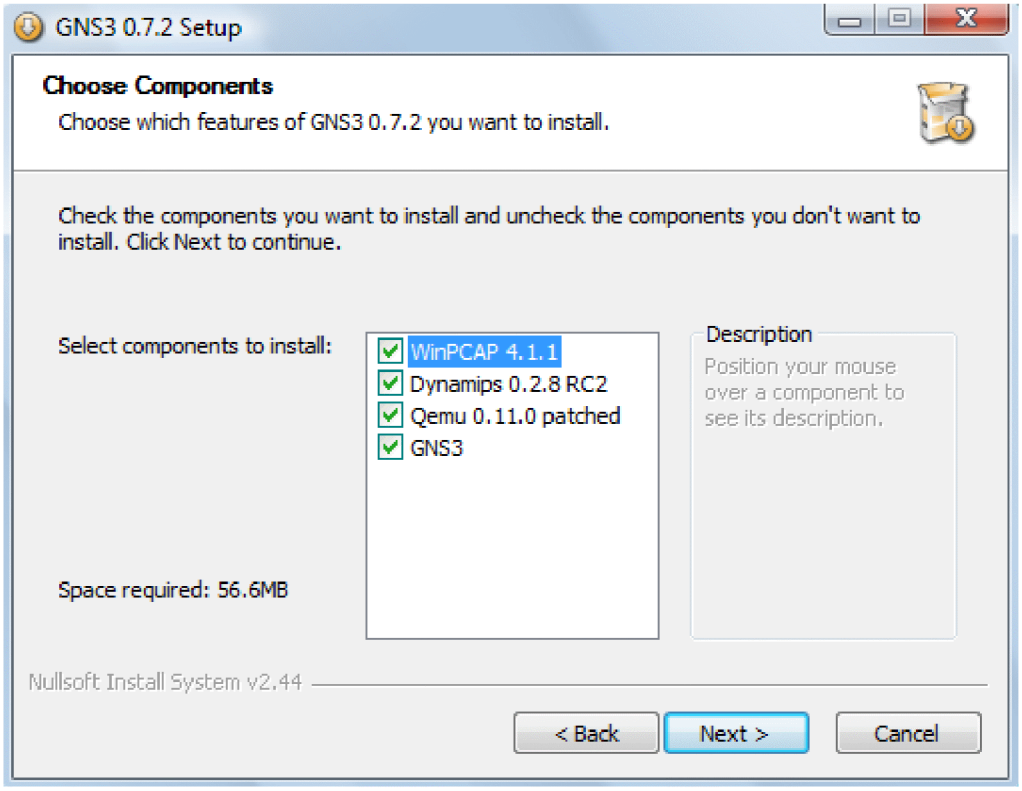


Figure6 : fenêtre 4 de l'installation du GNS3

Choisir un emplacement pour installer le programme.

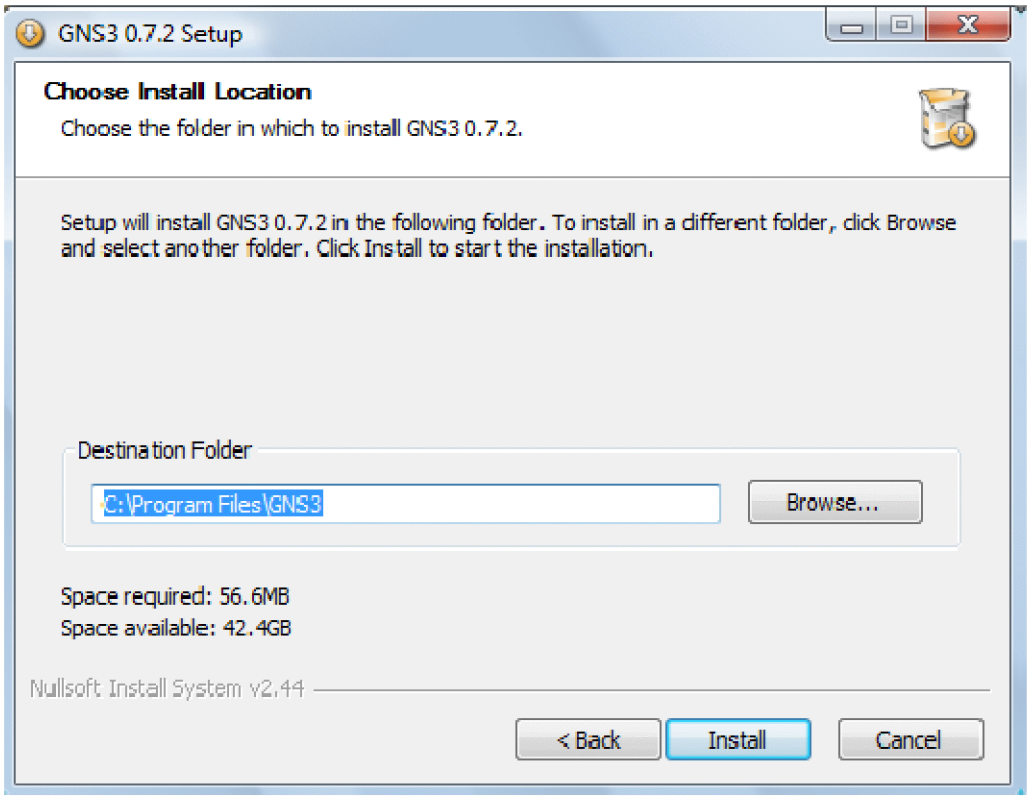


Figure 7 : fenêtre 5 de l'installation du GNS3

❖ **Téléchargement du WinPcap**

WinPcap est l'outil standard industriel pour accéder aux connections entres les couches réseaux (connectivité et sélection de routes entre deux systèmes hôte), disponible sur le système d'exploitation Windows. Grâce à cet outil, vous pouvez capturer les paquets réseaux transmis, manipulant ainsi la pile du protocole réseau. Il offre de précieux outils additionnels tels que des filtres de paquets de bas niveau, un moteur générant des statistiques d'usage réseau et supportant la capture de paquets à distance. Il utilise une combinaison de librairies et de contrôleurs pour accéder facilement aux couches réseau inférieures. C'est un programme efficace, versatile qui est devenu le logiciel préféré de filtrage et de capture de paquets pour la plupart des applications réseau populaires disponibles aujourd'hui tels que les analyseurs de protocole, la surveillance réseau, les systèmes de détection d'intrusion réseau, les mouchards, les générateurs de trafic, les analyseurs de trafic, etc. **C'**est une application essentielle. Sans cela, les meilleurs logiciels de gestion réseau (NMAP) tels que Windump, Ethereal, etc. ne fonctionneront pas.

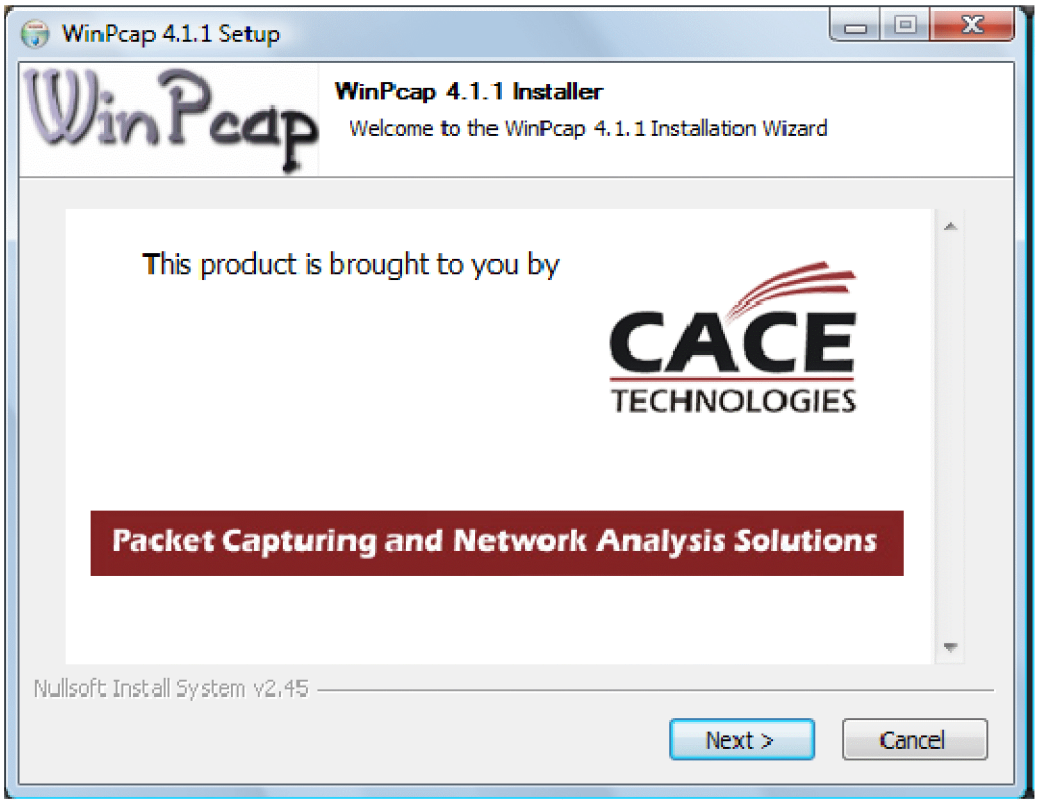


Figure 8 : fenêtre 6 de l'installation du GNS3

Cliquer sur continuer.

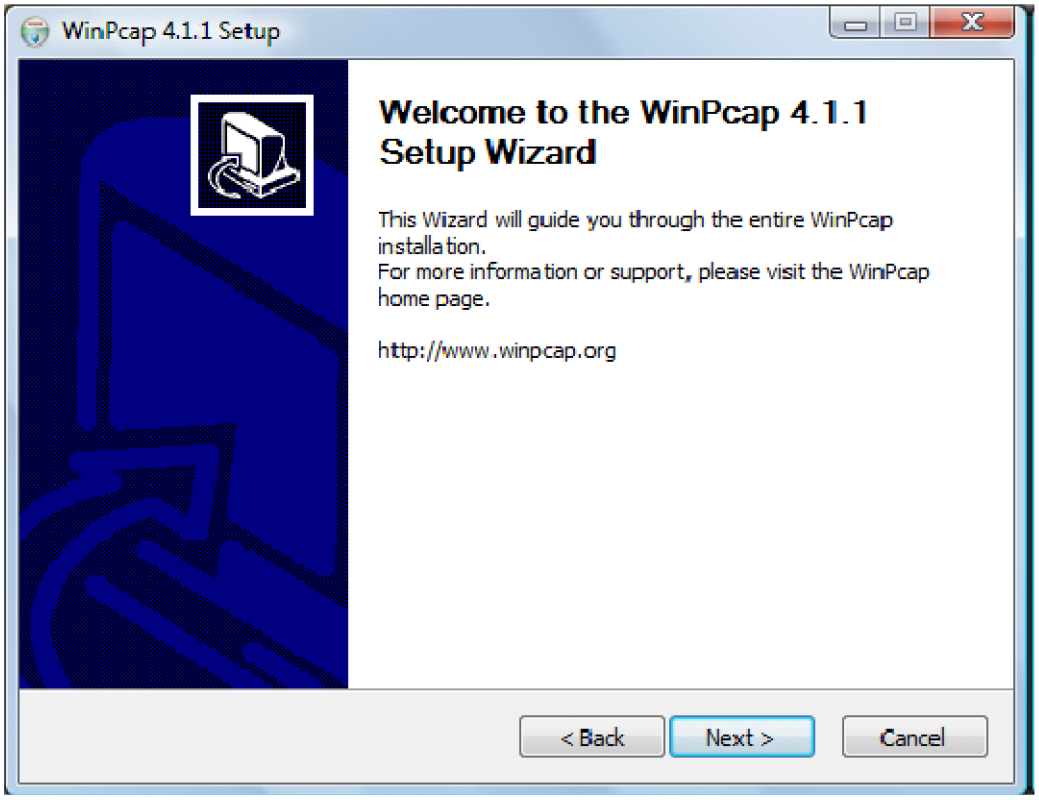


Figure 9: fenêtre 7 de l'installation du GNS3

Accepter la licence et on continue l'installation.

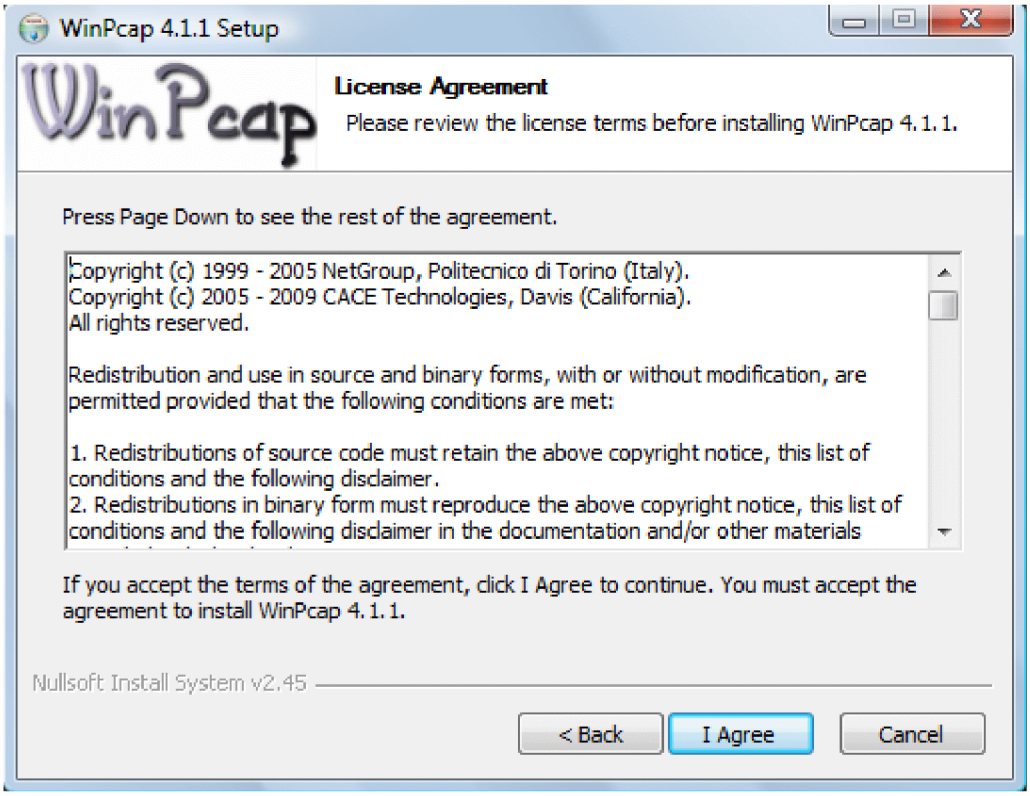


Figure 10: fenêtre 8 de l'installation du GNS3

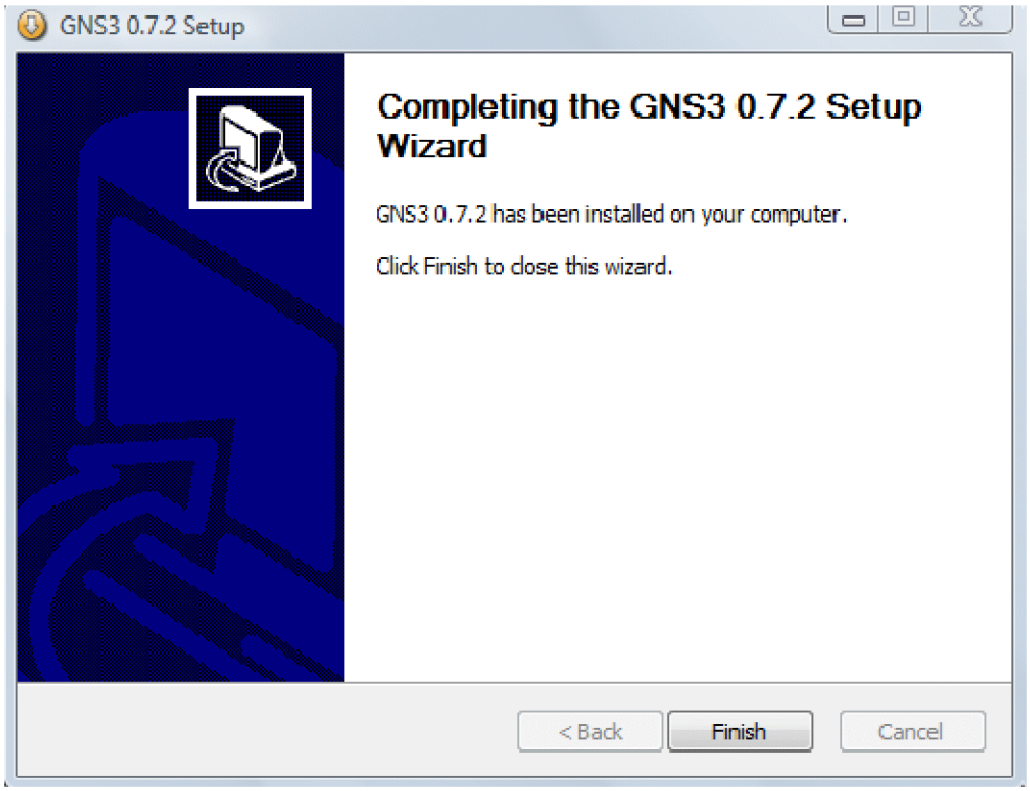


Figure 11: fenêtre 12 de l'installation du GNS3

L'installation est terminée. On peut maintenant lancer GNS.

Tout d'abord, il va falloir configurer et tester le fonctionnement du Dynamips et ajouter des images IOS pour travailler sur GNS 3.

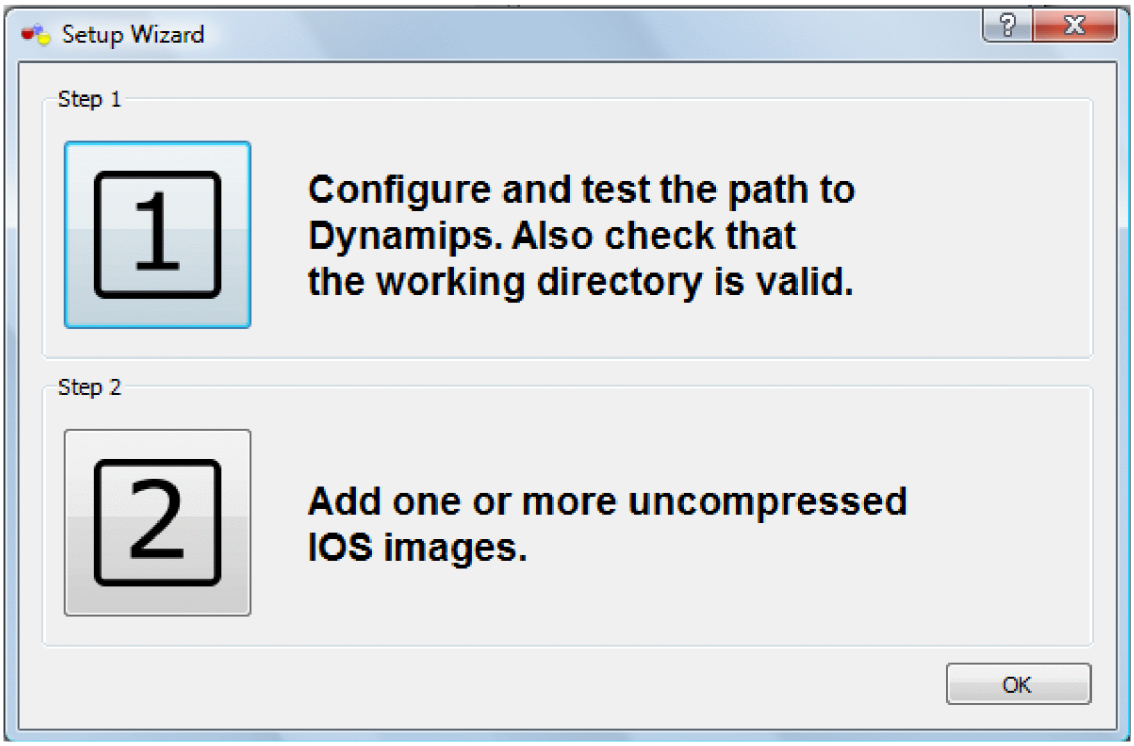


Figure 12: fenêtre d'option pour la configuration de dynamips et insertion IOS

On clique sur 1, et on se retrouve sur la partie préférence. On clique sur Dynamips et on lance le test. On remarque que ça fonctionne.

- **Téléchargement des images IOS** :

A partir du lien http://gns3.blogspot.com/2007/10/ios.html , on peut trouver différentes images IOS comme le montre la capture suivante.

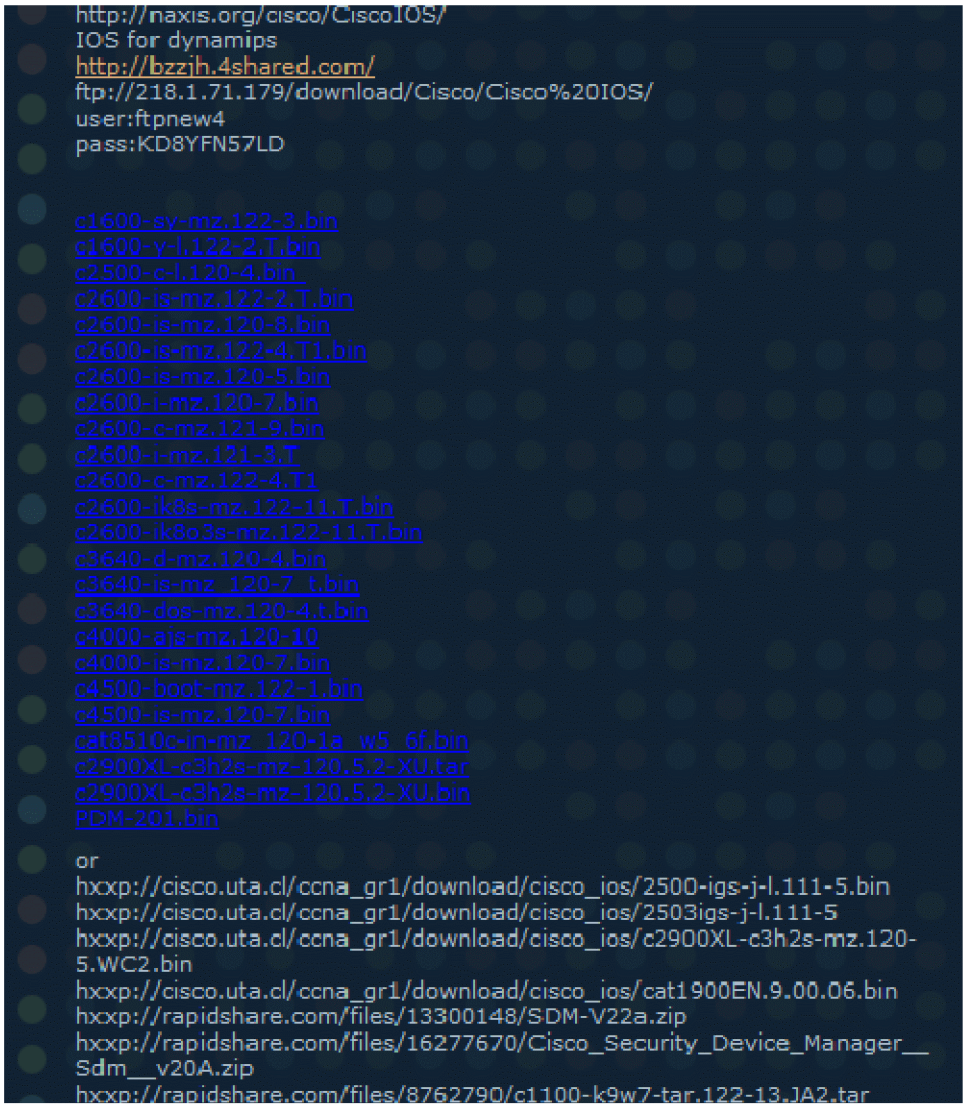


Figure 13 : exemple d'une page web de téléchargement IOS

- **Installation d'une ISO sur un routeur**

chargement de l'IOS :

Sur le logiciel Gns3 pour utiliser un équipement n'importe lequel, il faut incorporer d'abord son image ISO correspondante. On a vu dans la partie précédente comment obtenir ces images et dans cette partie nous verrons comment les utiliser sur le simulateur Gns3.

D'abord il faut créer un répertoire dans le quel, il faudra mettre toutes les images téléchargées et qu'on veut utiliser pour organiser les choses sinon cela est facultatif.

-Dans le menu **Editer** : on clique sur *Images IOS et Hyperviseurs*

Figure 14 : étape 1 de l'insertion d'une image IOS

Apres avoir cliqué on obtient l'interface suivante :

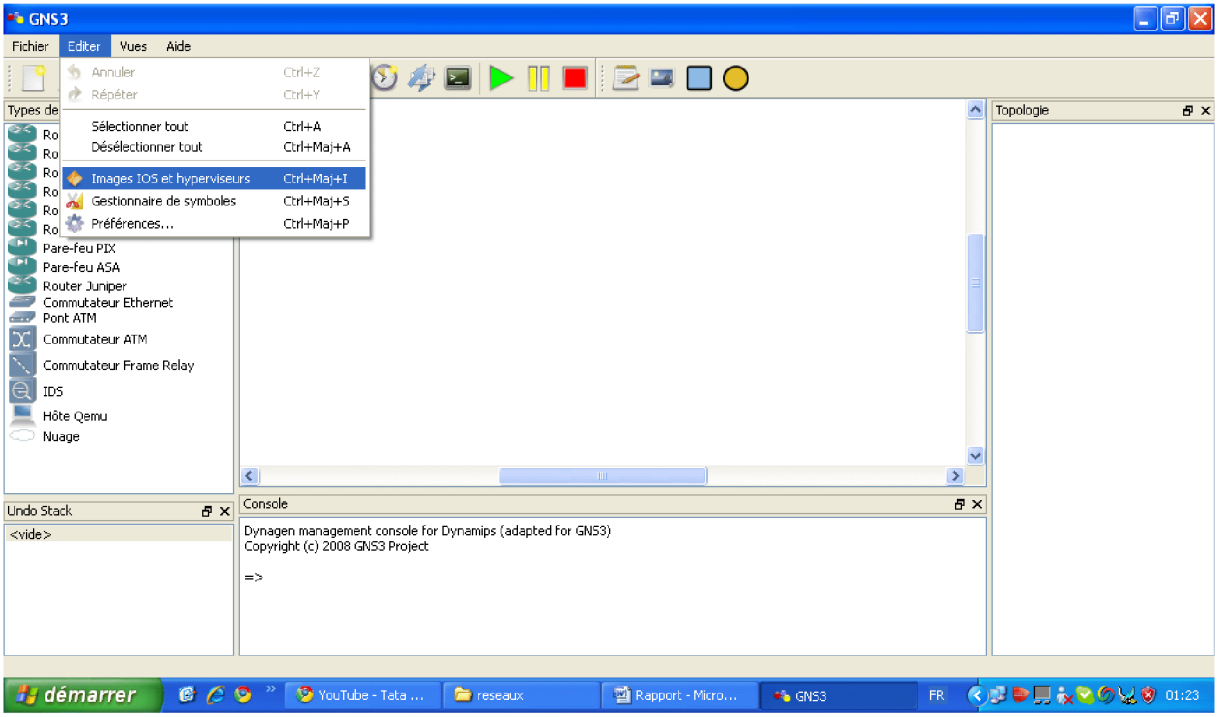


Figure 15 : étape 1 de l'insertion d'une image IOS

Apres avoir cliqué on obtient l'interface suivante :

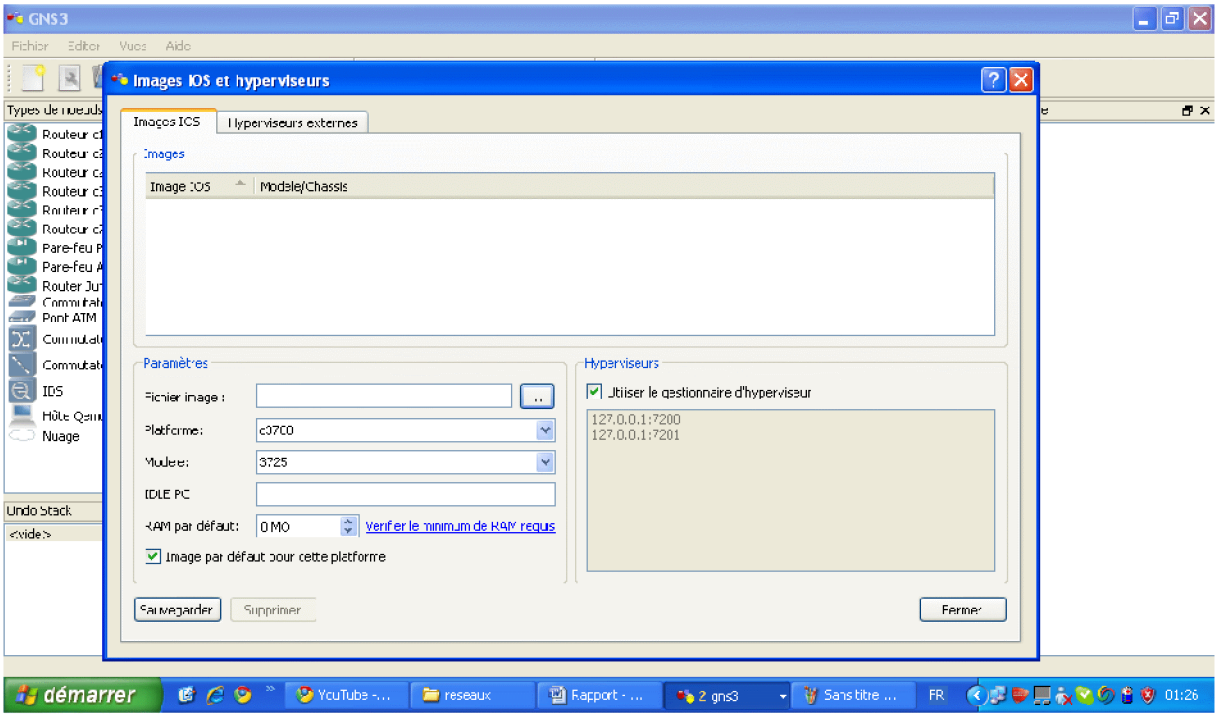


Figure 16 : étape 2 de l'insertion d'une image IOS

Sur cette interface on clique sur le bouton parcourir devant *Fichier image* dans les **Paramètres**.Une interface comme celle au dessous s'ouvre permettant de specifier l'image depuis le repertoire dans le quel elle se trouve.

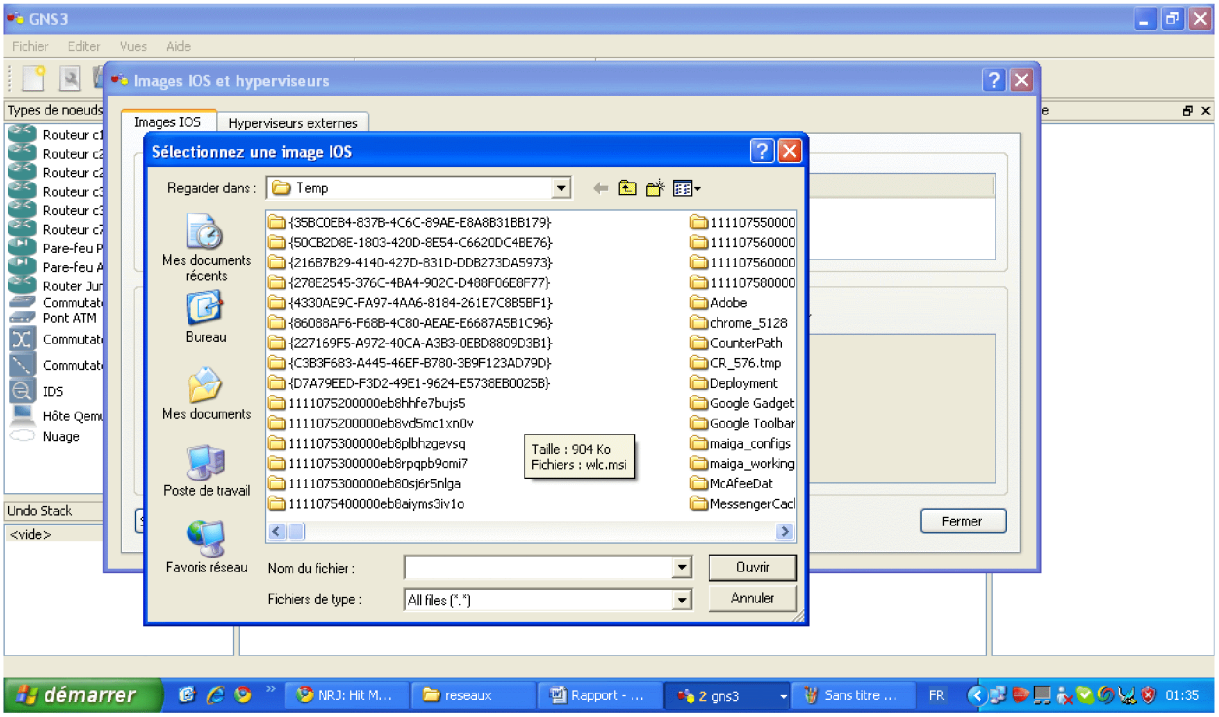


Figure 17 : étape 3 de l'insertion d'une image IOS

Une fois l'image sélectionnée on appuis sur *Ouvrir* en bas de la fenêtre.

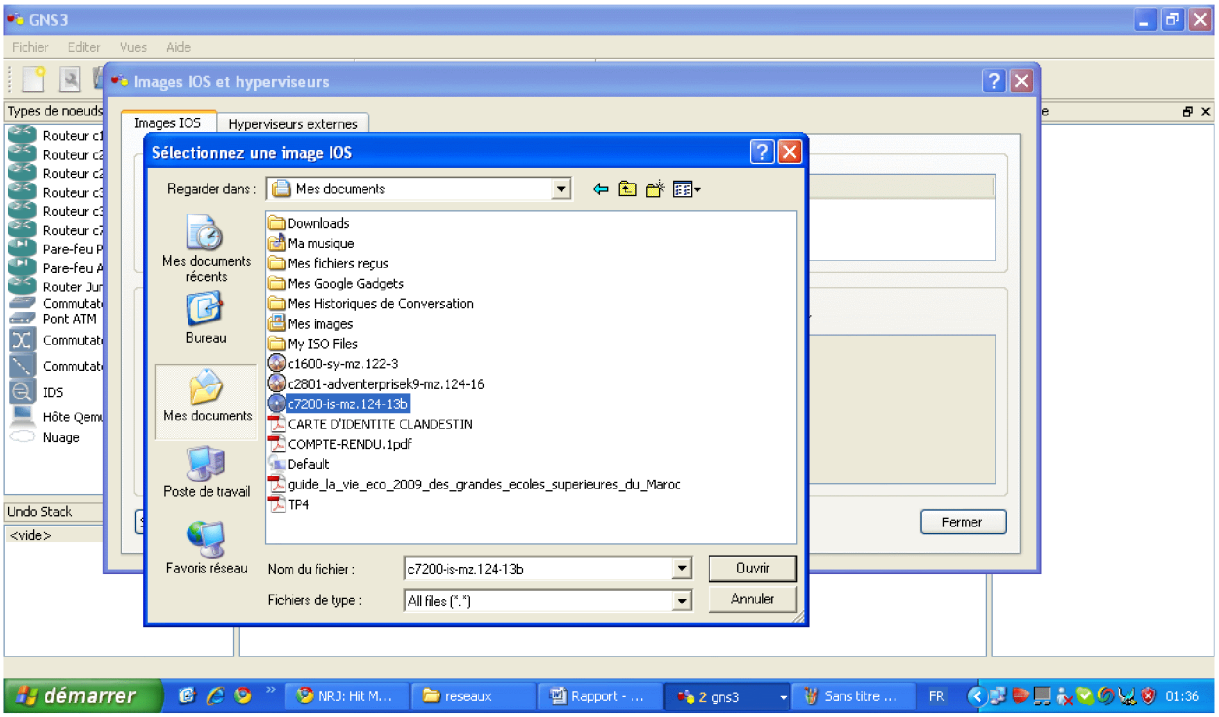


Figure 18 : étape 4 de l'insertion d'une image IOS

On obtient une fenêtre comme indiqué sur l'image ci-dessous sur la quelle les champs de saisie sont remplis par le lien sur l'image dans la partie *fichier image* et les caractéristiques comme *plateforme (*dans cet exemple : c7200*)*, *modèle (*dans cet exemple : 7200*)*, et *RAM par défaut (*dans cet exemple : 256Mo*)*.

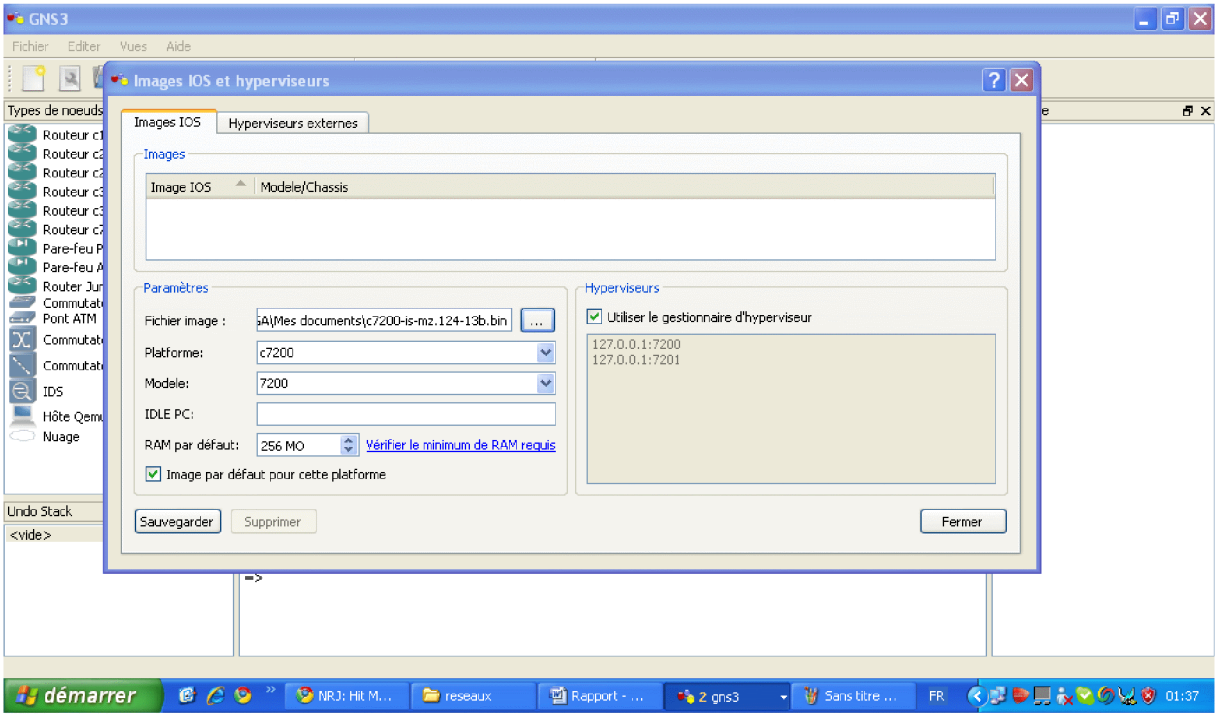


Figure 19 : étape 5 de l'insertion d'une image IOS

On appuis sur *Sauvegarder* pour enregistrer les informations, ainsi dans la partie haute apparaisse l'image ajoutée.

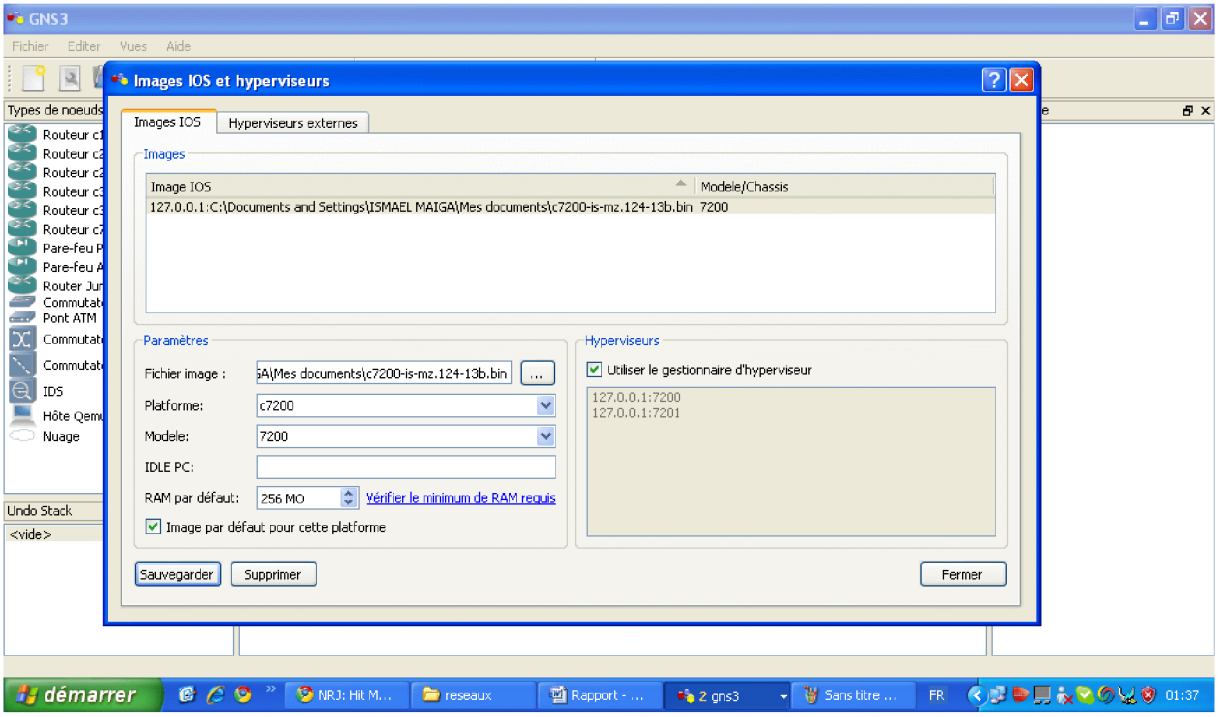


Figure 20 : étape 6 de l'insertion d'une image IOS

Voilà qu'après l'ajout de l'image d'un routeur 7200 ce dernier devient utilisable. (Pour mettre un routeur sur la partie centrale enfin de constituer une plateforme on fait un cliquer-glisser sur le routeur pour le prendre et faire un clique sur la partie centrale pour le déposer).

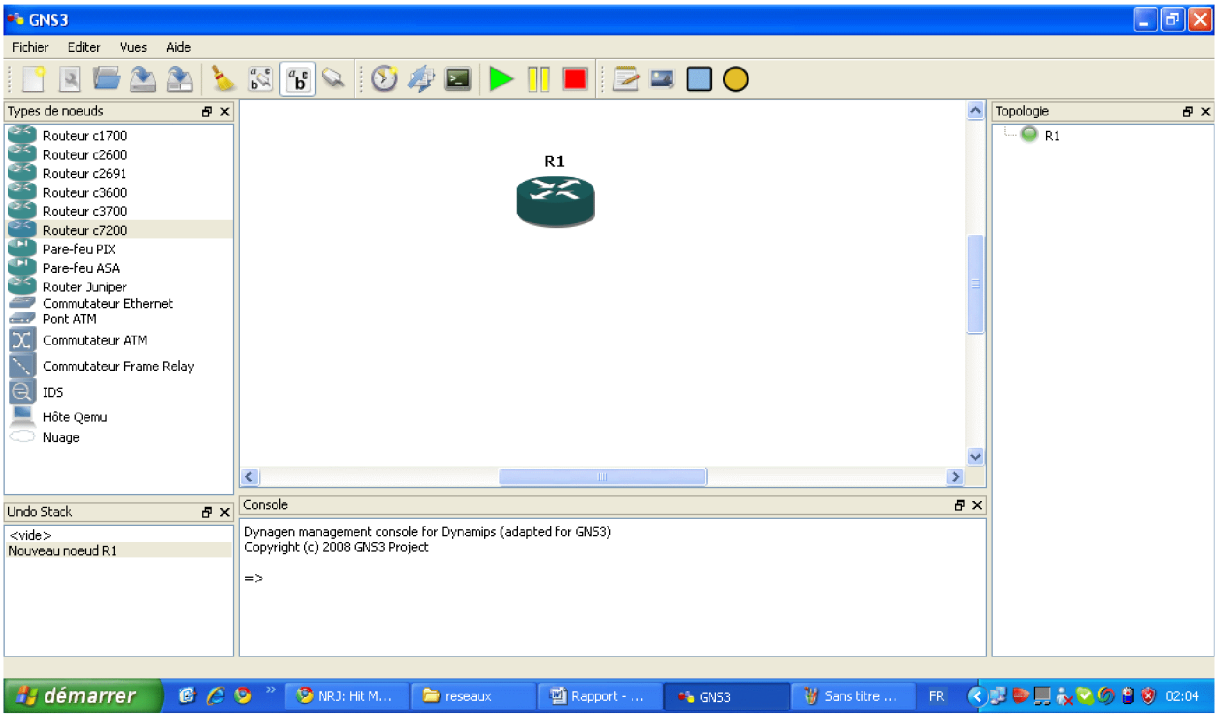


Figure 21 : essais après l'insertion d'une image IOS

- **Description des parties du logiciel GNS3**

Dans cette partie nous verrons les parties essentielles du logiciel GNS3 à savoir :

La barre des Menus :

Figure 22 : barre des Menus

Dans cette partie nous avons les menus qui mettent à votre disposition tous les éléments nécessaires pour la manipulation du logiciel. C'est comme le menu dans tout logiciel.

Les éléments de la barre d'outils de GNS3 :

Figure 23 :La barre d'outils GNS3

 Permet de créer un nouveau projet

 Permet d'éditer un projet

 Permet d'ouvrir un projet

 Permet de sauvegarder un projet en court dans le répertoire au se situe la plateforme

 Permet de sauvegarder un projet en court dans un répertoire que vous aller préciser

 Permet d'effacer la topologie

 Affiche ou cache sur la plateforme le nom des interfaces des équipements

 Affiche ou cache sur la plateforme le nom des équipements

 Permet de choisir le type de câble pour interconnecter vos équipements

 Permet de pour l'image de la plateforme

 Permet d'importer / d'exporter les fichiers de configuration des équipements

 Permet de lancer la console pour un ou tous les équipements de la plateforme

 Permet de démarrer/mettre en pause/arrêter un équipement ou toute la plateforme

 Permet de mettre une note sur la plateforme

 Permet d'insérer une image

 Permet de dessiner un rectangle /cercle

Bibliographie :

Ouvrages et mémoires :

[1] FOUDHAILI(O). « Analyse des performances de MPLS en terme de "Traffic Engineering" dans un réseau multiservice », Mémoire d'ingénieur de l'Ecole Supérieur De Tunisie, 2004/2005.

[2] NOUCHTI(O). El QASMI (M) et HILALI (T) « Virtual Private Network Etude comparative et réalisation d´unVPN MPLS »Ecole Marocaine des Sciences de L'ingénieur 2009/2010.

[3] CHARBONNIER LAURENT « EVALUATION DE LA SECURITE DES RESEAUX PRIVES VIRTUELS SUR MPLS » Ecole De Technologie Supérieure Université Du Québec 2007.

[4] GARNIER NICOLAS « Étude, conception et déploiement des technologies d'ingénierie de trafic sur l'infrastructure de production MPLS de RENATER »Ecole D'ingénieur CNAM 2013.

[5] ANDRE PEREZ « gestion des ressources et des défaillances dans les réseaux IP MPLS et Ethernet » Lavoisier 2009.

[6]ABDESSALEM MRIBAH « Etude et Dimensionnement d'un Réseau de Nouvelle Génération (NGN)Cas d'étude : Tunisie Télécom »mémoire Ecole Supérieur des Communications de Tunisie 2005/2006.

[7] STEPHANE LOHIER « transmission et réseaux » 3eme edition preface de Guy Pyolle

Sites web :

http://www.frameip.com/mpls-cisco/

http://www.frameip.com/mpls/

http://ccie.julienberton.fr/2012/01/01/mise-en-place-dun-vpn-mpls/

http://wapiti.telecomlille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2008-ttnfa2009/Fort-Gengembre/index.htm

Résumé

Le principe de "Best Effort" ne peut offrir aucune garantie de QoS pour les exigences des nouvelles applications (vidéo, voix, etc). En même temps, il ne serait pas raisonnable d'abandonner les réseaux IP qui sont tellement répandus de nos jours. MPLS apporte une solution ingénieuse à ce problème et rend ainsi possible le multiservice sur les réseaux IP. Cette technologie a réussi à conjuguer la simplicité de IP avec la gestion de QoS d'ATM. MPLS a permis entre autres de réaliser des applications comme le "Traffic Engineering vpn et qos " qui permet d'accéder à un haut niveau d'optimisation des réseaux, facilitant ainsi le passage au "tout IP".

Mot clés

MPLS, Traffic Engineering, commutation de label, RSVP TE.