RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'études

En vu de l'obtention du diplôme de Master II en Informatique
Option : Conduite des projets Informatique

Thème :

La prise en compte de la Qualité de Service QoS dans les réseaux IP

Cas Wataniya Telecom Algérie.

Proposé et dirigé par :

M: H. Iguer
Mr: S. Hamrioui

Réalisé par :

M^{r}: HAMOUNI Mourad

Promotion: 2014/2015

Remerciements

*Je tiens tout d'abord à remercier **Dieu** le tout puissant et miséricordieux, qui m'a donné la force et la patience d'accomplir ce Modeste travail.*

En second lieu, je tiens à remercier mon promoteur Mr Hamrioui Sofiane qui s'est dévoué pour me dispenser de tous conseils et directives utiles pour la réalisation de ce modeste travail.

je tiens à remercier mon encadreur Mr Iguer Halim et l'ensemble de l'équipe de Wataniya télécom de Bab Zeouar pour leur accueil bienveillant et leurs conseils avisés, et cela malgré leur emploi du temps chargé.

Mes vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à ma recherche en acceptant d'examiner mon travail Et de l'enrichir par leurs propositions.

Enfin, je remercie tous ceux qui, de près ou de loin, ont contribué à l'accomplissement de ce modeste travail.

Dédicaces

Je dédie ce modeste travail à :

La mémoire de mon défunt père qui restera toujours présent dans mon cœur.

Ma chère et tendre mère source de ma joie et de ma réussite.

Mes adorables sœur Lynda, Nassima, Hayet et Amel ainsi que leurs époux qui m'ont toujours encouragé.

Mon frère Salim, son épouse ainsi que son fils Mohand.

A toute ma famille & mes proches.

Mon encadreur Halim pour son aide précieux.

Mes amis(es) pour leurs soutiens.

A toute la promotion Informatique LMD 2014/2015

ABRIVIATION

ACL	**Access Control**
ARP	**Address Resolutions Protocol**
AS	**Autonomes system**
BGP	**Border Gateway Protocol**
DES	**Data Encryption Standard**
DHCP	**Dynamic Host Configuration Protocol**
DNS	**Domain name service**
DIFFSERV	**Differentiation Service**
EGP	**Exterior Gateway Protocol**
FTP	**File Transfert Protocol**
FAI	**Fournisseur d'accès à l'Internet**
FIFO	**First in first out**
GSM	**Global system of communication**
HTTPs	**Secure HTTP**
ICMP	**Internet Control Message Protocol**
IGP	**Interior Gateway Protocol**
IntServ	**Integrate service**
IP	**Internet Protocole**
Ipv4	**Internet Protocol version 4**
IPv6	**Internet Protocol version 6**
IETF	**Internet Engineering Task Force**
ISO	**International Standard Organisation**
LAN	**local area network**
MAC	**Media Access Control**
MAC	**Message Authentication Code**
MAN	**Metropolitan area network**
MTU	**Maximum Transfer Unit**
MPLS	**Multiprotocol Label Switching**
NBAR	**Network-based Application Recognition**
OSI	**Open System Interconnections**
OSPF	**Open Shortest Path First**
OSPFng	**OSPF next generation**
PPP	**PPP: Point-to-Point Protocol**

PHB	**Per Hop Behavior**
PVN	**Private virtual network**
PQ	**priority Queuing**
QoS	**Quality of Service**
RADIUS	**Remote Authentication Dial-In User Service**
RARP	**Reverse ARP**
RFC	**Request For Comment**
RIP	**Routing Information Protocol**
RIPng	**RIP next generation**
RSVP	**Ressource réservation setup Protocol**
RTCP	**Real time control protocol**
RTP	**Real Time Application**
SSH	**Secure Shell**
SSL	**Secure Socket Layer**
SNMP	**Simple Network Management Protocol**
TAN	**Tiny Area Network)**
TCP	**Transfert Contrôle Protocol**
TOS	**Type of Service**
TTL	**Time to live**
UDP	**User Data gram Protocol**
WAN	**wide area network**

Liste des figures

Liste des figures

Sommaire

Sommaire

Chapitre II : Présentation de l'organisme d'accueil

Chapitre III : La Qualité de service dans les réseaux IP

Chapitre IV : Mise en œuvre et application de QoS

Introduction Générale

La qualité de service ou QoS (Quality of service) est un nouveau concept incontournable dans le monde des réseaux des télécommunications. Bien que complexe, il n'a rien de révolutionnaire, puisqu'il se fonde sur des technologies préexistantes, qu'il vise à rationaliser, et souvent à simplifier, afin d'en faciliter la mise en œuvre. Néanmoins, la normalisation n'est pas encore achevée et de nombreuses philosophies s'affrontent. Ce concept revêt de multiples aspects technologiques, et qui doit être précisé selon ses objectifs et son contexte d'utilisation.

En fait, la plupart des réseaux informatique et télécommunications reposent aujourd'hui sur le Protocol IP, conçu à l'origine pour véhiculer des données informatiques. Cependant, avec la prolifération du réseau Internet marquée par la croissance exponentielle du trafic et la naissance de nouvelles applications, ce réseau se trouve face à des problèmes sévères. Le best effort n'est plus suffisant pour suivre l'évolution des technologies. Donc, il ne s'avère pas un support de communication qui permet de satisfaire pleinement les contraintes variées de ces nouvelles applications.

Face à cette impasse, un effort de recherche important a été mené, ces dernières années, pour qu'internet offre un support d'interconnexion ou de nombreux types d'applications puissent cohabiter et fonctionner raisonnablement.

La croissance des demandes de trafic générées par les applications est toujours plus nombreuses et plus exigeantes en matière de Qualité de service, cela oblige les opérateurs à utiliser des technologies qui permettent à gérer efficacement leur infrastructure réseau (équipements) et leurs ressources (liens d'interconnexion).

Ce projet nous a permis de découvrir le monde du réseau (IP, routage, …) et se familiariser avec les outils et les technologies de la QoS (IntServ, RSVP, DiffServ, MPLS, policing, shaping,….), en montrant à travers une maquette réduite d'un réseau opérateur les avantages que peut apporter l'implémentation de la QoS dans les réseaux IP.

Afin de mener à bien notre projet, nous avons réparti le contenu de notre travail de la manière suivante :

- Dans le premier chapitre nous verrons des « Généralité sur les réseaux »
- Dans le deuxième chapitre nous allons présenter notre organisme d'accueil (watanya telecom) et sa structure.
- Dans le troisième chapitre nous allons consacrer à la Qualité de service dans les réseaux IP, Avant d'entrer dans les détails des techniques, nous précisons dans ce chapitre la terminologie et le concept lié à la QoS, ainsi qu'une classification générale des modèles et protocoles de QoS

- Dans le quatrième et le dernier chapitre nous verrons la réalisation de la maquette on commençant par la description des outils et l'environnement de développement utilisés puis une brève explication pour la mise en œuvre et applications de la QoS.

CHAPITRE

I

Généralités sur Les réseaux

I. Généralités sur les réseaux informatiques :

I.1 Introduction :

Un réseau est constitué d'un ensemble d'ordinateurs et d'organes périphériques généralement éloignés et reliés entre eux par un système de communication suivant une architecture, une topologie, et une technologie.

Le terme générique « réseau» définit un ensemble d'entités (objet, personnes, etc.)

Dans ce chapitre, nous allons se familiarisé avec les différents éléments qu'un réseau doit constituer pour qu'une information émise d'un ordinateur puisse être acheminée et routée vers son ordinateur réceptif voulu.

I.2 Définition de réseau :

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles afin que les utilisateurs et les applications qui fonctionne sur ces dernières puissent échanges des informations.

Le terme réseau en fonction de son contexte peut designer plusieurs choses :

- désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qu'est le cas lorsqu'on parle de l'Internet.
- décrire la façon dont les machines d'un site sont interconnectées
- spécifier les protocoles qui sont utilisés pour que les machines communiquent on peut parler de réseau TCP/IP.

I.3.1 Définition de topologie :

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique. Il en existe trois:

- La topologie en bus
- La topologie en étoile
- La topologie en anneau

➢ Topologie en bus:

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

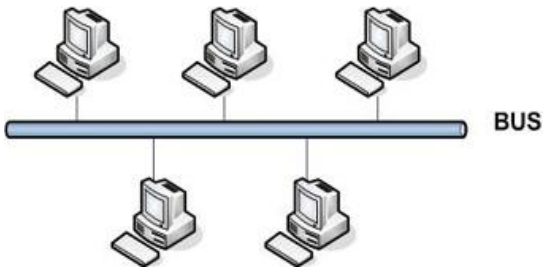


Figure I.1 : topologie en bus

Cette topologie a pour avantages d'être facile à mettre en oeuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

➢ Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé hub ou concentrateur.

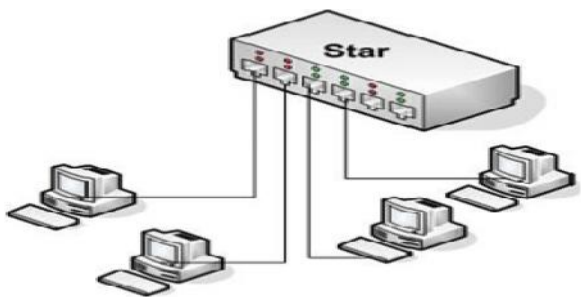


Figure I.2 : topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérable car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.

En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

➢ Topologie en anneau :

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole" successivement.

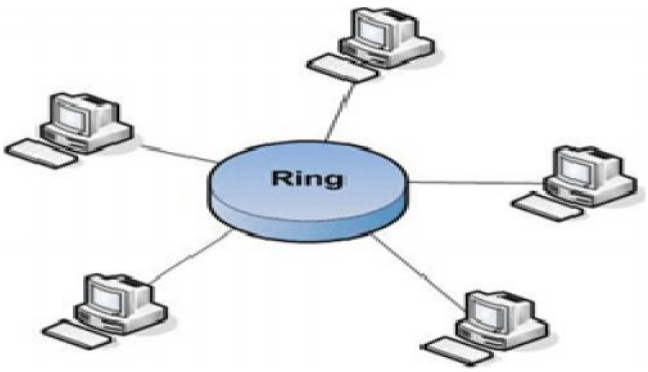


Figure I.3 : topologie en anneau

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole.

Les deux principales topologies logiques utilisant cette topologie physique sont TOKEN RING (anneau à jeton) et FDDI.

I.3.2 Les différents types de réseaux :

On distingue différents types de réseaux (privés) selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On fait généralement trois catégories de réseaux:

- LAN (local area network).
- MAN (metropolitan area network).
- WAN (wide area network).

I.3.3 Interconnexion :

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelles, Routeurs, Ponts …) qui assurent le transfert des données :

a) Les ponts

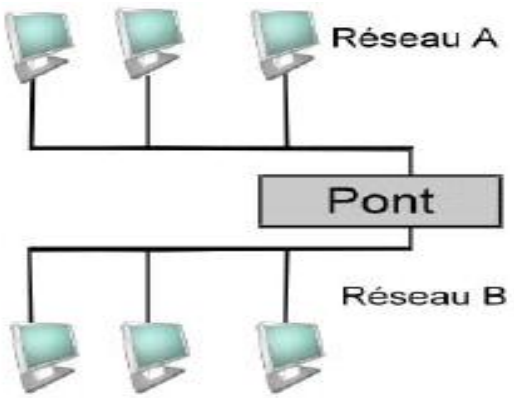


Figure I.4: Deux réseaux relies avec un pont.

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont (*figureI.4)*.

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel côté du réseau se trouve l'émetteur.

Ainsi le pont est capable de savoir si émetteur et destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau.

b) Les Passerelles

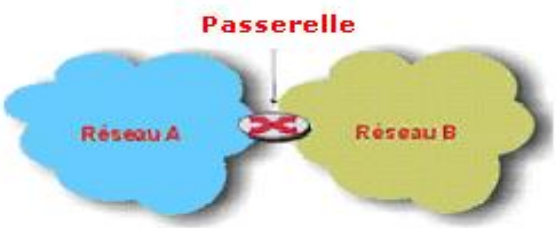


Figure I.5: deux réseaux reliés avec passerelle

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun des réseaux.

Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en terme de taille de paquet de données,

mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données.

c) Les Routeur :

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts). Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en terme de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation (*figure I.6*).

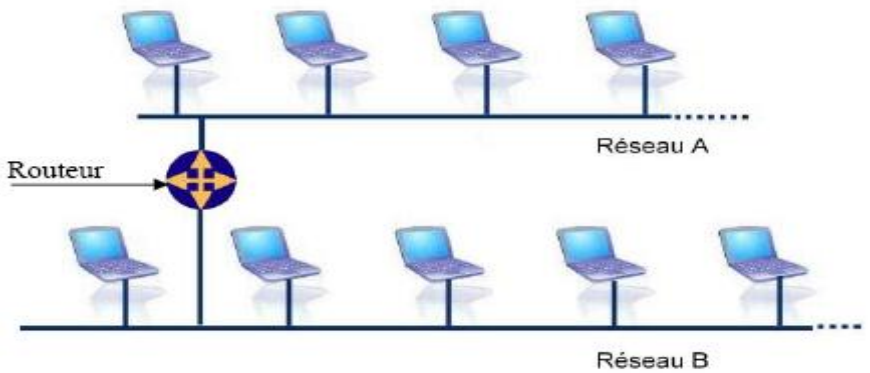


Figure I.6: Routeur connecter à deux réseaux locaux

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quelque soit l'architecture.

d) Les Hubs (concentrateurs) :

Le Hub est également appelé concentrateur ou répétiteur. C'est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire).

e) Switch :

Egalement appelé Commutateur, Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de données inutiles sur le réseau.

I.4 Le Modèle OSI :

OSI signifie (Open System Interconnections), Ce modèle a été mis en place par l'ISO (**I**nternational **S**tandard **O**rganisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire). Ainsi de nombreux réseaux incompatibles coexistaient. Le modèle OSI est un modèle qui comporte 7 couches :

- ✓ **Couche physique:** S'occupe de la connexion physique d'une machine avec le réseau.
- ✓ **Couche liaison** : S'occupe de l'acheminement de trames de données entre deux équipements voisins.
- ✓ **Couche réseau :** Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage.
- ✓ **Couche transport :** Assure un contrôle de bout en bout en permettant à un processus destinataire de communiquer directement avec le processus source.
- ✓ **Couche session** : Définit la manière dont les protocoles peuvent être organisées pour fournir toutes les fonctionnalités dont les programmes d'applications se servent.
- ✓ **Couche présentation :** Est destinée à supporter les fonctions dont bouceaup de programme ont besoin comme la compression de texte ou la conversion d'image graphique.
- ✓ **Couche application :** Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers.

I.4.1 Encapsulation des données :

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

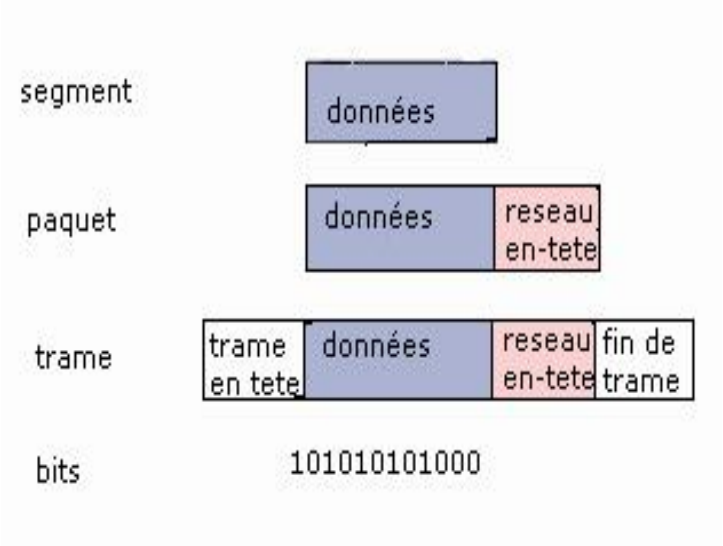


Figure I.7: principe d'encapsulation.

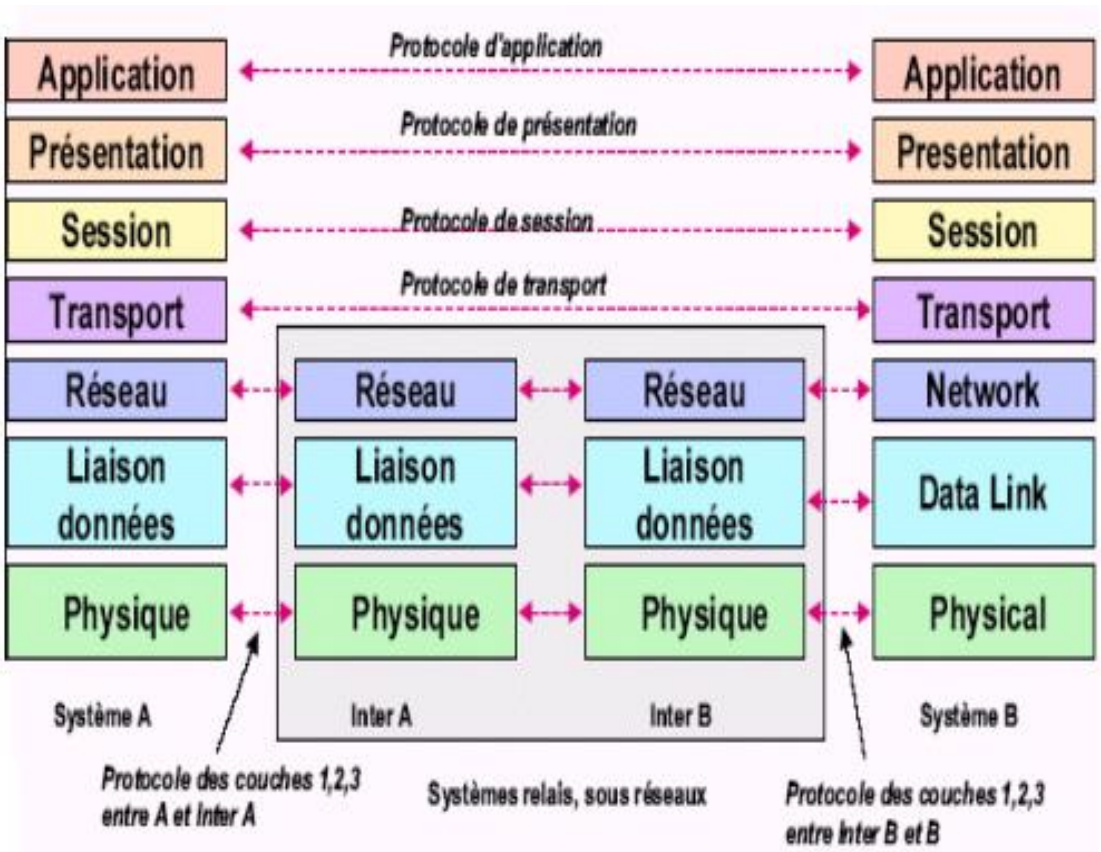


Figure I.8: Couches fonctionnelles du modèle OSI

I.5 MODELE TCP\IP

I.5.1 Introduction

Le modèle TCP/IP est le modèle le plus utilisé actuellement que ce soit pour des réseaux locaux ou de plus grandes dimensions. Le modèle TCP/IP (Transmission Control Protocol /Internet Protocol) a été développé par le ministère de la Défense des Etats Unis (DOD) à partir du début des années 70 pour servir de base au réseau militaire ARPANET qui est devenu plus tard Internet. Ce protocole est tellement répandu qu'il en est devenu une norme de fait, aucun constructeur ne peut faire l'impasse TCP/IP, s'il ne veut pas que son produit soit rejeté, il est donc disponible sur tous les systèmes informatiques, il est livré en standard sans supplément et par défaut pour toutes les stations de travail.

I.5.2 Description

TCP/IP, comme son nom l'indique, est en fait constitué de deux protocoles TCP et IP. TCP (Transmission Control Protocol) se situe au niveau transport du modèle OSI, il s'occupe donc d'établir une liaison virtuelle entre deux ordinateurs. Au niveau de l'ordinateur émetteur, TCP reçoit les données de l'application dans un buffer, les sépare en datagrammes pour pouvoir les envoyer séparément, l'ordinateur distant (qui utilise le même protocole) à la Réception doit émettre un accusé de réception, sans celui-ci, le data gramme est ré émis.

Au niveau de l'ordinateur récepteur, TCP réassemble les data grammes pour qu'ils soient transmis à l'application dans le bon ordre. IP (Internet Protocol) IP assure l'acheminement de chaque paquet sur le réseau en choisissant la route la plus appropriée. Pour pouvoir s'y retrouver IP va de pair avec un système d'adressage qui identifie de manière unique les réseaux traversés ainsi que chaque entité d'un réseau (appelé aussi noeud: ordinateur, routeur, ...).

La relation entre TCP et IP et la suivante, TCP fait passer à IP un datagramme accompagné de sa destination, IP ne s'occupe pas de l'ordre d'expédition, c'est TCP qui s'occupe de tout remettre en ordre, il se contente de trouver la meilleure route possible.

Souvent les termes « datagrammes » et « paquet » semblent identiques. En fait, on parle de datagramme lorsqu'il est question de TCP (couche 4 de l'OSI), le datagramme est l'unité de données. On parle de paquet pour les couches réseaux (3 IP) et liaison (2 et 1), c'est une réalité physique, on peut les voir circuler sur le réseau. Généralement, un paquet contient seulement un datagramme, si bien que concrètement, il y a peu de différence entre les deux.

I.5.3 Les couches du modèle TCP\IP

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches.

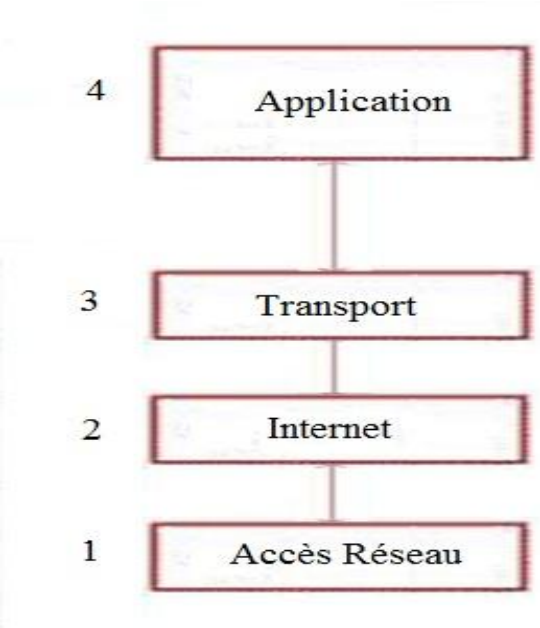


Figure I.9: Modèle TCP/IP

- **La couche hôte réseau**

Elle spécifie la forme sous laquelle les données doivent être acheminées, quelque soit le type de réseau utilisé.
Elle prend en charge les notions suivantes :

- Acheminement des données sur la liaison.
- Coordination de la transmission de données (synchronisation).
- Format des données.
- Conversion des signaux (analogiques/numériques) pour les modems RTC (Réseau Téléphonique Commuté).
- Contrôle des accès à l'arrivée.

- **La couche Internet**

Elle est chargée essentiellement de l'acheminement et le routage des datagrammes. La couche internet contient cinq protocoles (les trois premiers sont importants).

- ✓ **Protocole IP (Internet Protocol):** protocole responsable d'adressage, fragmentation et réassemblage des datagrammes. Ce protocole ne contrôle pas les erreurs de transmission.
- ✓ **Protocole ARP (Adresse Résolution Protocol) :** gère les adresses des cartes réseaux. Chaque carte a sa propre adresse d'identification codée sur 48bits.

- ✓ **Protocole ICMP (Internet Control Message Protocol) :** gère les informations relatives aux erreurs de transmission, il ne corrige pas les erreurs, mais signale aux autres couches que le message contient des erreurs. Ce protocole est utilisé par tous les routeurs pour signaler une erreur.
- ✓ **Protocole RARP (Reverse Adresse Résolution Protocol):** fait la correspondance entre l'adresse MAC de la carte réseau (48bits) et l'adresse IP (32bits).
- ✓ **Protocole IGMP (Internet Group Management Protocol) :** responsable de la gestion des groupes IP multicast ou multipoint.

- ➢ **La couche transport**

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation. Officiellement, cette couche n'a que deux implémentations : le protocole TCP et le protocole UDP. TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un Internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche Internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

- ➢ **La couche application**

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP, SMTP, HTTP. Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

I.6 Protocole Ipv4 :

I.6.1 Définition d'un protocole :

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP).

Sur Internet par exemple les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles reliés entre eux. Cette suite de protocole s'appelle TCP/IP.

I.6.2 Protocole IP :

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, Mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de0 à 255 (4 fois 8 bits), on les note sous la forme **xxx.xxx.xxx.xxx** où chaque **xxx** représente un entier de 0 à 255.

Par exemple, **194.153.205.26** est une adresse IP Ont peux distinguer deux parties dans une adresse IP:

- Les nombres de gauche désignent le réseau (on l'appelle **netID**).
- Les nombres de droite désignent les ordinateurs de ce réseau (on l'appelle **host ID**).

I.6.2 .1 Format de data gramme :

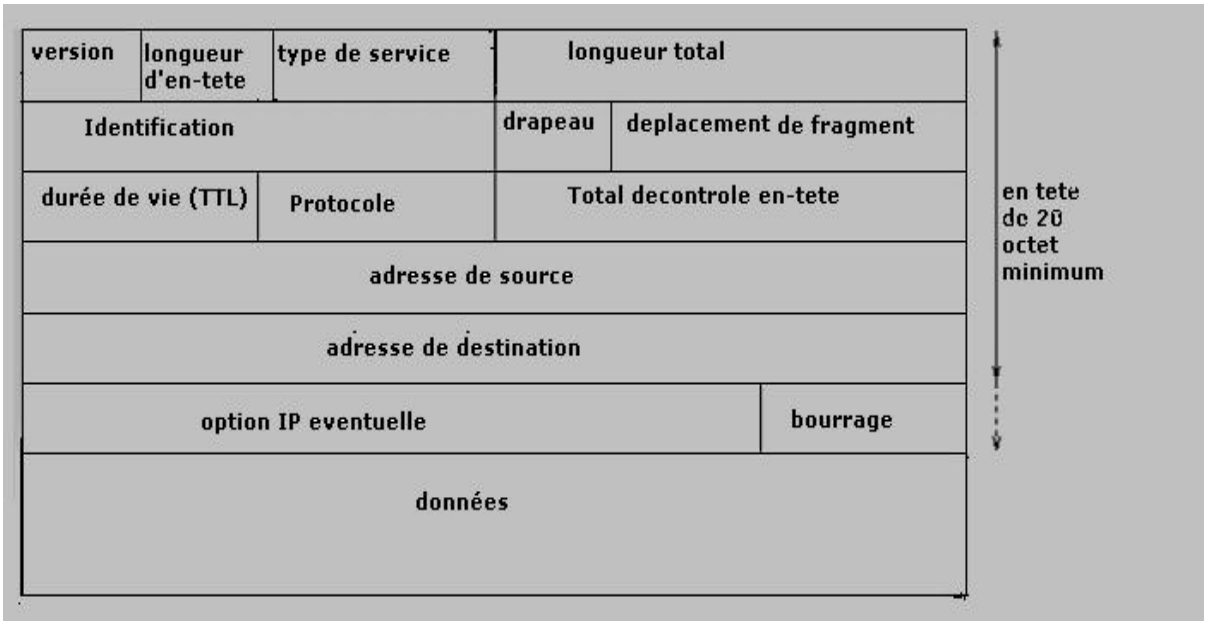


Figure I.10: Structure d'un datagramme IP

La version : codée sur 4 bits, renseigne sur le format de l'en-tête Internet, ce champ indique la version 4 du protocole IPv4.

La longueur d'en-tête : représente sur 4 bits la longueur, en nombre de mots de 32 bits de l'en-tête du datagramme. Ce champ est nécessaire car un en-tête peut avoir une taille supérieure à 20 octets (taille de l'en-tête classique) à cause des options que l'on peut y ajouter.

Le type de services (TOS) : est codé sur 8 bits, indique la manière dont doit être géré le datagramme et se décompose en six sous champs comme suit.

Bits 0-2	Priorité	
Bit 3	0= retard standard	1=retard faible
Bit 4	0= debit standard	1= haut debit
Bit 5	0= taux d'erreur standard	1= taux d'erreur faible
Bits 6-7	Réservé	

Figure I.11: type de service

- **Le champ "Longueur Totale" :** est la longueur du datagramme entier y compris en-tête et données, mesurée en octets. Ce champ ne permet de coder qu'une longueur de datagramme d'au plus 65,535 octets.

- **Le champ identification :** est un entier qui identifie de manière unique chaque datagramme émis et qui est recopié dans le champ identification de chacun des fragments si ce datagramme est fragmenté.

- **Le champ drapeaux :** comprend trois bits pour les divers commutations de contrôle dont deux qui contrôlent la fragmentation.
  Le premier bit est réservé, le deuxième bit égal à 0 signifie une fragmentation possible égal à 1 signifie une fragmentation impossible, le troisième bit si 0 signifie : dernier fragment et si 1 signifie : fragment intermédiaire

- **Le champ déplacement de fragment :** précise la localisation du début du fragment dans le datagramme initial. À part cela, les fragments sont des datagrammes dont l'en-tête est quasiment identique à celle du datagramme.

- **La durée de vie (TTL) :** La durée de vie est initialisée par l'émetteur du datagramme à la durée maximum pendant laquelle le datagramme pourra exister dans le réseau. Si un routeur ou autre composant réseau intercepte un datagramme dont l'existence a dépassé cette durée, il doit être détruit.

- **Contrôle d'en-tête (16 bits) :** Un Checksum est calculé sur l'en-tête uniquement. Comme certains champs de l'en-tête peuvent être modifiés (ex., durée de vie) pendant la transmission du paquet IP à travers le réseau, ce

Checksum doit être recalculé et vérifié à chaque point du réseau et l'en-tête est réinterprété. Ceci dans le but de préserver l'intégrité des paquets.

- **Adresse source (32 bits)** : C'est l'adresse de l'émetteur du paquet IP.

- **Adresse destination (32 bits) :** C'est l'adresse de destination vers laquelle le paquet a été envoyé.

- **Le champ options :** Est une liste de longueur variable, mais toujours complétée par des bits de bourrage pour atteindre une taille multiple de 32 bits pour être en conformité avec la convention qui définit le champ longueur de l'en-tête. Ces options sont très peu utilisées car peu de machines sont aptes à les gérer. Parmi elles, on trouve des options de sécurité et de gestion (domaine militaire), d'enregistrement de la route, d'estampille horaire, routage strict, etc...

- **Bourrage :** Le champ de bourrage n'existe que pour assurer à l'en-tête une taille totale multiple de 4 octets. Le bourrage se fait par des octets à zéro.

I.6.3 Adressage :

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque interface de réseau. Une adresse IP est toujours représentée dans une notation décimale pointée constituée de 4 nombres (1 par octet) compris chacun entre 0 et 255 et séparés par un point.

Plus précisément, une adresse IP est constituée d'une paire *(*id. de réseau, id. de machine*)* et appartient à une certaine classe (A, B, C, D ou E) selon la valeur de son premier octet, comme détaillé dans la (*figure 1.12*).

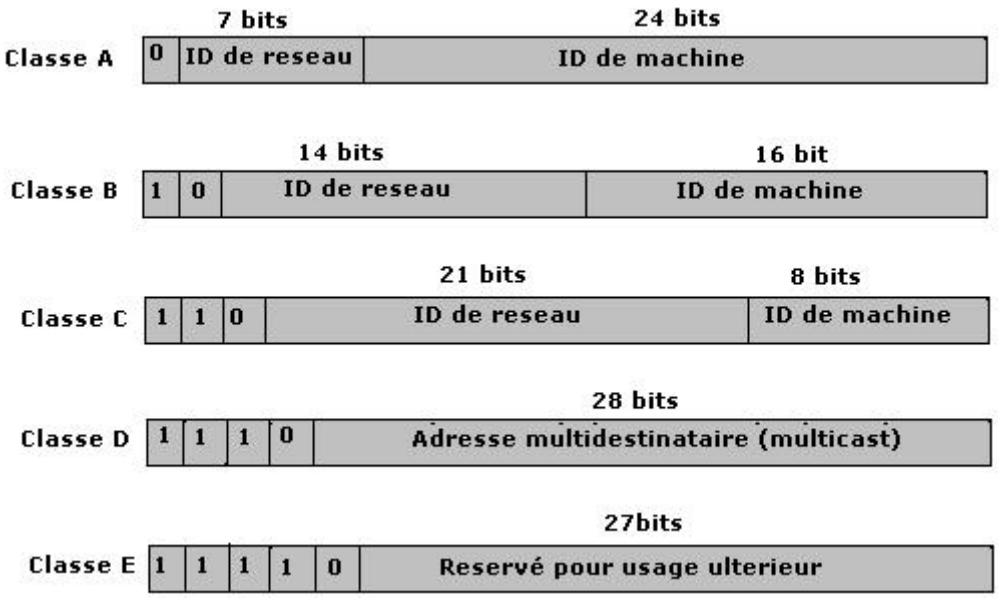


Figure I.12: les cinq classes d'adresses IP

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

Classe	Adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C	192. 0. 0. 0 à 223. 255. 255. 255
D	224. 0. 0. 0 à 239. 255. 255. 255
E	240. 0. 0 .0 à 247. 255. 255. 255

Figure I.13 : l'espace d'adresse

I.6.4 ARP ET RARP

Ces protocoles permettent de convertir l'adresse logique en adresse physique et vice versa.

I.6.4.1 Protocole ARP:

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse. Chaque machine connectée au réseau possède un numéro d'identification sur 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte réseau en usine.

Toutefois, la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme. On parle alors de *l'adresse IP*.

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête (contenant l'adresse de la machine demandée) sur le réseau. Chaque machine du réseau compare par la suite l'adresse logique reçu, avec la sienne. Si l'une des machines s'identifie à cette adresse, elle répondra alors à ARP par une requête contenant son adresse physique, qui va stocker la couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu.

I.6.4.2 RARP (Reverse ARP) :

Il est dans le réseau Internet. Permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique.

I.6.5 Le routage IP :

Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'un internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme. D'une manière générale on distingue la remise directe, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et la

remise indirecte qui est mise en œuvre dans tous les autres cas, c'est-à-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final.

I.6.5.1 Table de routage :

Table de routage spécifique à chaque routeur qui permet de déterminer vers quelle voie de sortie envoyer un datagramme destiné à un réseau quelconque. Évidemment, à cause de la structure localement arborescente d'Internet la plupart des tables de routage ne sont pas très grandes. Par contre, les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux. D'un point de vue fonctionnel une table de routage contient des paires d'adresses du type (*D*, *R*) où *D* est l'adresse IP d'une machine ou d'un réseau de destination et *R* l'adresse IP du routeur suivant sur la route menant à cette destination.

I.6.5.2 Routage interne :

- **RIP :**

L'un des protocoles de routage les plus populaires est RIP (Routing Information Protocol) qui est un protocole de type vecteur de distance. C'est-à-dire que les messages échangés par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage. Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'«infini». Ceci implique que RIP ne peut être utilisé qu'à l'intérieur de réseaux qui ne sont pas trop étendus.

- **OSPF:**

Est un nouveau type de protocole de routage dynamique qui élimine les limitations de RIP. C'est un protocole d'état de liens, c'est-à-dire qu'ici un routeur n'envoie pas des distances à ses voisins, mais il teste l'état de la connectivité qui le relie à chacun de ses voisins. Il envoie cette information à tous ses voisins, qui ensuite le propagent dans le réseau. Ainsi, chaque routeur peut posséder une carte de la topologie du réseau qui se met à jour très rapidement lui permettant de calculer des routes aussi précises qu'avec un algorithme centralisé. En fait, RIP et OSPF, sont des protocoles de type IGP (Interior Gateway Protocol) permettant d'établir les tables des routeurs internes des systèmes autonomes. Un système autonome peut être défini par un ensemble de routeurs et de réseaux sous une administration unique. Cela peut donc aller d'un seul routeur connectant un réseau local à Internet, jusqu'à l'ensemble des réseaux locaux d'une multinationale. La règle de base étant qu'un système autonome assure la connexité totale de tous les points qui le composent en utilisant notamment un protocole de routage unique. À un niveau plus global, Internet apparaît donc comme une interconnexion de systèmes autonomes comme illustré dans la *figure 1.14*

Figure I.14 : Interconnexion de systèmes autonomes.

Dans chaque système autonome les tables sont maintenus par un IGP et sont échangées uniquement entre routeurs du même sous-système. Pour obtenir des informations sur les réseaux externes, ceux de l'autre système autonome, ils doivent dialoguer avec les routeurs externes R1 et R2. Ceux-ci sont des points d'entrée de chaque système et via la liaison qui les relie, ils échangent des informations sur la connectivité grâce à EGP (Exterior Gateway Protocol) ou BGP (Border Gateway Protocol) qui remplace EGP actuellement.

I.6.5.3 Routage externe :

❖ BGP (Border Gateway Protocol):

C'est le protocole de routage externe le plus utilisée sur l'Internet .BGP gère le routage basé sur une politique qui utilise des raison non techniques (des considérations routage politiques, organisationnelles ou de sécurité) pour prendre les décisions en matière de routage .BGP améliore la capacité d'un système autonome à choisir entre différentes routes et à implanter des politiques de routage sans se baser sur une autorise centrale de routage (dans le d'absence de passerelle centrales).

❖ ICMP :

Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles. ICMP rapporte les messages d'erreur à l'émetteur initial. Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet : machine destination déconnectée, durée de vie du datagramme expirée, congestion de passerelles intermédiaires.

Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'Internet. Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP.

❖ IGMP:

Ce protocole permet au groupe de machines d'utiliser les ressources de réseau de façon efficace et optimale. L'adressage multipoint Permet l'envoi de datagrammes vers plusieurs destinataires, l'envoi du réponse pour chaque machine d'un sous réseau est unique.

I.7 La fragmentation des datagrammes IP :

La taille d'un datagramme maximal est de 65535 octets. Toutefois cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer de si gros paquets. De plus, les réseaux sur Internet utilisent différentes technologies, si bien que la taille maximale d'un datagramme varie suivant le type de réseau. La taille maximale d'une trame est appelée **MTU** (Maximum Transfer Unit), elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau.

Type de réseaux	MTU (Octet)
ARPANET	1000
ETHERNET	1500
FDDI	4470

Figure I.15: Le MTU de quelques réseaux

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus faible. Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter, c'est-à-dire le découper en fragments de tailles inférieures au MTU du réseau et de telle façon que la taille du fragment soit un multiple de 8 octets (*figure 1.16*).

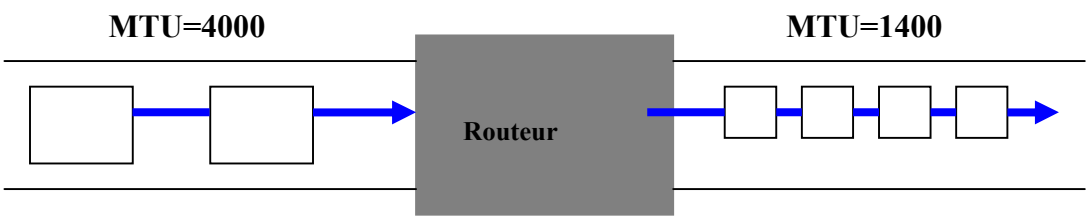


Figure I.16: Exemple de fragmentation des Datagrammes.

Le routeur va ensuite envoyer ces fragments de manière indépendante et les réencapsuler (En ajoutant un en-tête à chaque fragment) de telle façon à tenir compte de la nouvelle taille du fragment, et en ajoutant des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre (rien ne dit que les fragments vont arriver dans le bon ordre, étant donné qu'ils sont acheminés indépendamment les uns des autres).

I.8 Les faiblesses d'Ipv4 :

- **Le problème de pénurie d'adresse :**

Le problème le plus connu concerne l'espace d'adressage. Les adresses IP sont actuellement stockées sur 32 bits ce qui permet environ plus de quatre milliards d'adresses, taille largement suffisante à l'origine lorsque le modèle dominant était celui d'un ordinateur par campus ou centre de recherche. Aujourd'hui, l'informatique industrielle et commerciale ainsi que celle des particuliers rendent ce nombre trop faible, d'autant que de nombreuses adresses sont "gaspillée" par le mécanisme d'allocation hiérarchique. En outre, la généralisation des machines connectées au réseau risque d'aggraver ce problème.

- **L'explosion des tables de routage :**

Un autre problème est celui posé par l'explosion de la taille des tables de routage dans l'Internet. Le routage, dans un très grand réseau, doit être hiérarchique avec une profondeur d'autant plus importante que le réseau est grand.

Le routage IP n'est hiérarchique qu'à trois niveaux : réseau, sous réseau et machine. Les routeurs des grands réseaux d'interconnexion doivent posséder une entrée dans leurs tables pour tous les réseaux IP existants.

- **L'absence de type de données :**

IPv4 ne permet pas d'indiquer de façon pratique le type de données transportées (TOS ou Type of Service dans IPv4) d'où, par conséquent, leur urgence ou le niveau de service souhaité. Ce besoin est particulièrement critique pour les applications "temps réel" comme la vidéo mais aussi celles plus classiques (par exemple, en donnant des priorités à tel ou tel trafic). Ce problème a été évoqué et clarifié mais reste peu mis en oeuvre. Il est symptomatique que les protocoles de routage les plus répandus ne tiennent pas vraiment compte du TOS dans le calcul des routes.

- **Le manque au niveau de la sécurité**

IPv4 ne fournit pas de mécanismes de sécurité comme l'authentification des paquets, leur intégrité ou leur confidentialité. Il a toujours été considéré que ces techniques étaient de la responsabilité des applications elles-mêmes.

I.9 SNMP (Simple Network Management Protocol).

1. Présentation générale.

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux. SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications: les bases de données, les serveurs, les logiciels, etc. L'environnement de gestion SNMP est constitué de plusieurs composantes : la station de supervision, les éléments actifs du réseau, les variables MIB et un protocole. Les différentes composantes du protocole SNMP sont les suivantes:

Les éléments actifs du réseau sont les équipements ou les logiciels que l'on cherche à gérer.

Cela va d'une station de travail à un concentrateur, un routeur, un pont, etc.

Chaque élément du réseau dispose d'une entité dite agent qui répond aux requêtes de la station de supervision. Les agents sont des modules qui résident dans les éléments réseau. Ils vont chercher l'information de gestion comme par exemple le nombre de paquets en reçus ou transmis.

- La station de supervision (appelée aussi manager) exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail.
- La MIB (Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules MIB spécifiques.
- Le protocole, qui permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

2. Fonctionnement du SNMP.

Le protocole SNMP est basé sur un fonctionnement asymétrique. Il est constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. Le manager envoie des requêtes à l'agent, lequel retourne des réponses. Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (traps) au manager.

SNMP utilise le protocole UDP déjà étudie. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents.

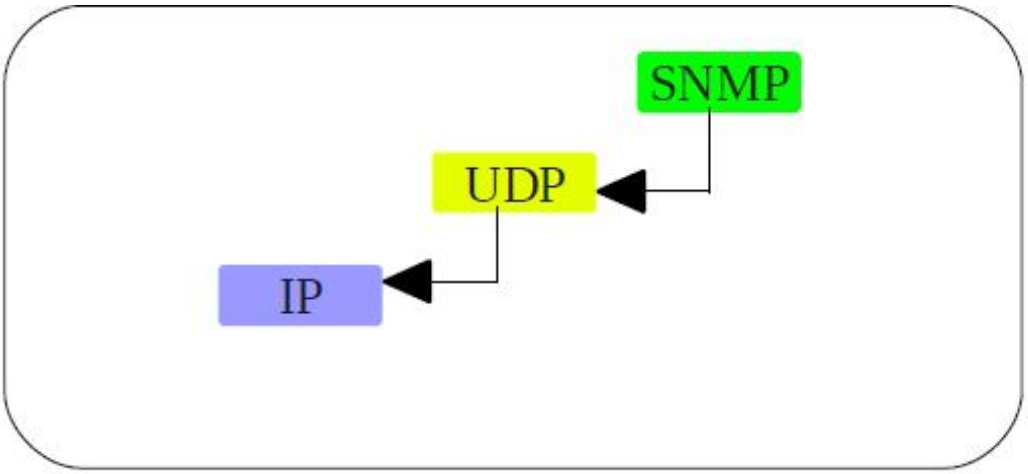


Figure I.16 encapsulation du protocole SNMP

I.9 Conclusion :

Nous venons de voir dans cette partie quelques concepts de base des technologies de l'information et de la communication à savoir les réseaux et leurs architectures, les différents protocoles utilisés pour cette communication.

Dans le chapitre suivant nous allons présenter l'entreprise ou notre travail se déroulera, nous parlerons de ses missions et activités des services en détaillant notre champ d'étude.

CHAPITRE

II

Organisme D'accueil

Historique :

WATANIYA TELECOM ALGERIE (WTA) a été mise en place par la société koweïtienne Wataniya Telecom, à laquelle s'est jointe United Gulf Bank (UGB). Dotée d'une licence d'une durée de 15 ans, WTA a adopté un programme d'investissements accéléré comportant des projets de 1 milliard de dollars US sur trois ans. Grâce à ces investissements, Nedjma sa taille la place de leader de l'innovation et de la plus-value : elle rend la technologie multimédia accessible à tous et facile à utiliser.

Wataniya Telecom, l'opérateur de référence WTA, a été fondée en 1999 au Koweït. Il fait partie des sociétés de KoweItProjectsCOmpany (KIPCO), la plus importante entreprise privée du Koweït avec un actif de plus de 10 milliards USD. Wataniya Telecom a connu une croissance fulgurante dans l'univers des télécommunications sans fil au Moyen-Orient et en Afrique du Nord. En mars 2007, Qtel devient actionnaire majoritaire (51%) de Wataniya Telecom Kuweit et détient par conséquent 80% de Nedjma.

C'est lors d'une conférence de presse organisée, le mardi 12 novembre 2013 à l'hôtel Sheraton du Club des Pins que le directeur général de Nedjma, Joseph Ged a annoncé le changement officiel de son identité commerciale et visuelle en adoptant le nouveau nom Ooredoo (le nom de la marque traduit de l'arabe signifie «je veux»). Il a également indiqué que le transfert de la marque de Nedjma vers Ooredoo s'effectuera dans la continuité sous le slogan de « Dima Maakoum » et que le lancement de la nouvelle marque coïncide avec la mise en service de la 3G.

II.1 Présentation de Wataniya Télécom Algérie :

Les investissements de l'opérateur de téléphonie mobile (Ooredoo) en Algérie ont atteint 485,5 millions de dollars US en 2013, contre 226 millions de dollars US en 2012, selon un bilan rendu public par la filiale algérienne du groupe qatari.

Ce volume représente 19% des investissements globaux de la maison mère qatarie Ooredoo, selon un communiqué de l'opérateur de téléphonie mobile.

Le bénéfice net de la filiale algérienne s'est chiffré à 201,4 millions de dollars US en 2013, contre 98,7 millions de dollars l'année précédente, soit une progression de plus que le double, selon la même source.

En 2013, les revenus d'Ooredoo ont atteint 1,06 milliard de dollars, contre 955,4 millions de dollars en 2012, soit une augmentation de 15%. Le nombre

d'abonnés de l'opérateur s'est établi au 4ème trimestre 2013 à 9,5 millions, en hausse de 200.000 abonnés par rapport au 3ème trimestre.

Elle détient 32% des parts de marché de la téléphonie mobile en Algérie, selon la même source.

Ooredoo est le premier investisseur dans le secteur des télécommunications en Algérie pour la quatrième année consécutive, selon le communiqué.

Ooredoo, détenu principalement par le qatari Qtel, avait obtenu une licence d'exploitation de la téléphonie mobile en Algérie en décembre 2003 suite à une offre de 421 millions de dollars. Mais, ce n'est qu'en août 2004 qu'elle avait procédé au lancement commercial de sa marque, ces numéros téléphoniques commencent par l'indicatif 05 xx xxxxxx ce qui donne un numéro de téléphone à 10 chiffres.

Logo de 2004 à 2009

Logo de 2010 à 2013

Logo actuel

II.2 Qualité de service :

Ooredoo offre aux utilisateurs algériens un nouveau monde en matière de télécommunications mobiles. En effet, Ooredoo met au service de la clientèle algérienne non seulement des produits et services innovateurs, mais aussi une haute qualité de transmission grâce à des équipements issus des technologies les plus récentes, un service à la clientèle basé sur les standards les plus élevés et une politique de prix hautement concurrentielle.

III.3 Réseau :

Le réseau Ooredoo a été déployé dans des délais record pour offrir aux consommateurs algériens des communications de qualité exceptionnelle en émission et en réception.

Ooredoo utilise le réseau GSM sur les fréquences 900/1800 et le réseau GPRS/EDGE pour les applications de données. D'après l'autorité de régulation de la poste et des télécommunications(ARPT), le réseau Ooredoo couvre 99% des chefs-lieux des wilayas, et plus de 95% des agglomérations et routes nationales.

Au 15 décembre, Nedjma devenue Ooredoo procède au lancement commercial de son réseau 3G HSPA+ après autorisation de l'ARPT, sous le label 3G++ et simultanément avec l'opérateur national Mobilis couvrant ainsi 10 wilayas au premier jour de lancement, en l'occurrence, Alger, Oran, Ouargla, Constantine, Sétif, Djelfa et en exclusivité à Béjaïa, Chlef, Bouira et Ghardaïa.

Le déploiement se poursuivra plus tard à Boumerdès, Blida, Tipasa, Tlemcen, Sidi Bel Abbès, AïnDefla et Biskra et El Oued et en exclusivité Médéa. L'opérateur envisage de couvrir d'ici la fin 2014, 25 wilayas représentant 80% de la population.

II.4 Organisation interne de Wataniya :

L'entreprise WTA se structure selon l'organigramme donné à la figure 3.1.

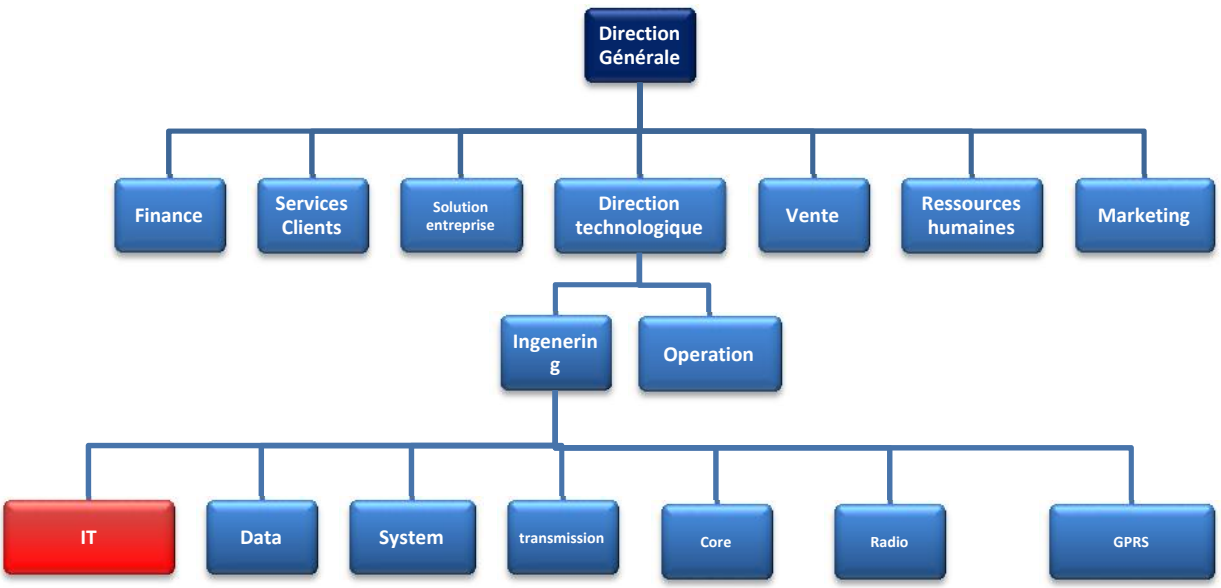


Figure II.1. Organigramme de WTA.

II.5 Présentation de la direction Engineering IT

Notre stage s'est déroulé dans la direction IT/IS et plus précisément dans le service IT Engineering. La direction IT/IS est composée des services suivants :

- IT Engineering : est chargé du maintien et de l'évolution de l'infrastructure réseau de l'entreprise.
- System engineering : assure la disponibilité et le bon fonctionnement des systèmes de bases de données.
- IT Windows : s'occupe des serveurs Windows et des applications sous-jacentes.

- IT UNIX : responsable de la configuration et de la maintenance des serveurs UNIX.
- IT Help Desk : prend en charge la résolution des problèmes techniques suite à la demande d'un utilisateur ou à un incident.

II.6 Objectifs du service IT infrastructure :

- Fournir un support aux autres départements qui utilisent l'infrastructure réseau et les technologies associées.
- Adapter les services liés aux technologies de l'information aux besoins actuels et futurs de l'entreprise et de ses clients.
- Participer à accroître la qualité des services rendues aux clients.
- Meilleur utilisation du personnel, pour une plus grande efficacité qui passe par une optimisation des coûts des opérations IT et une réduction du temps des différentes tâches liées à la gestion réseau.
- Surveiller l'environnement IT pour mieux gérer les performances. Par exemple, utilisation du CPU, de l'espace disque, de la mémoire centrale, de la bande passante, etc.
- Optimiser les possibilités de l'infrastructure informatique et du support, afin d'assurer un niveau de disponibilité[1] convenable permettant au business d'atteindre ses objectifs. En effet, le manager ne peut se permettre aucune interruption ou déni de service. Les services doivent être rendus 24h/24, 7j/7. La moindre défaillance ou baisse de performance entraine une chute directe de l'activité et de son résultat. Au-delà du coût d'une panne, il en va de l'image et de la réputation de l'entreprise.
- Minimiser les répercussions sur l'entreprise des incidents et des problèmes provenant d'erreurs dans l'infrastructure et rendre invisible à l'utilisateur les effets des pannes des éléments informatiques ainsi que les interruptions de service par une résolution rapide.
- Faire évoluer l'esprit du service d'une attitude réactive à une attitude proactive en prenant les mesures nécessaires pour empêcher l'apparition des incidents, des dysfonctionnements et des dégradations de performance avant qu'ils n'impactent les métiers portés par le service IT Infrastructure.
- Analyserles incidents et les problèmes ayant cours sur l'infrastructure du service IT. Cette analyse a pour objet de rendre un diagnostic clair et précis de l'origine des dysfonctionnements.

- Assurer la sécurité et la continuité des activités de l'entreprise et prévenir les menaces externes.

II.7 Infrastructure du réseau de WTA:

La fiabilité et la bonne maitrise du réseau de Wataniya Télécom Algérie constituent des éléments indispensables pour garantir les meilleurs services à sa clientèle. Le réseau de WTA se divise en deux parties :

- ***La partie O&M (operating and maintenance) :*** Il s'agit de la partie GSM du réseau de Wataniya pour assurer les communications téléphoniques sans-fil.
- ***La partie Corporate*** : il s'agit de la partie IP du réseau de Wataniya
- **Le noyau** de ce réseau est constitué de quatre switchs multicouches interconnectés avec des liaisons de 10 Go/s, 2 switchs redondants pour la partie utilisateurs et O&M et les 2 autres pour la partie serveurs. Le noyau a été divisé en deux parties pour séparer le trafic des serveurs de celui des utilisateurs connectés au réseau téléphonique privé.

L'un des switchs multicouches est connecté à un firewall PIX. Ce dernier contrôle l'accès des équipements du réseau privé depuis et vers l'Internet.

Un autre switch du noyau est connecté via deux routeurs (pour assurer la redondance) et des liaisons séries aux sites distants (exemple : site d'Ouled Fayet, Est, Boutiques …).

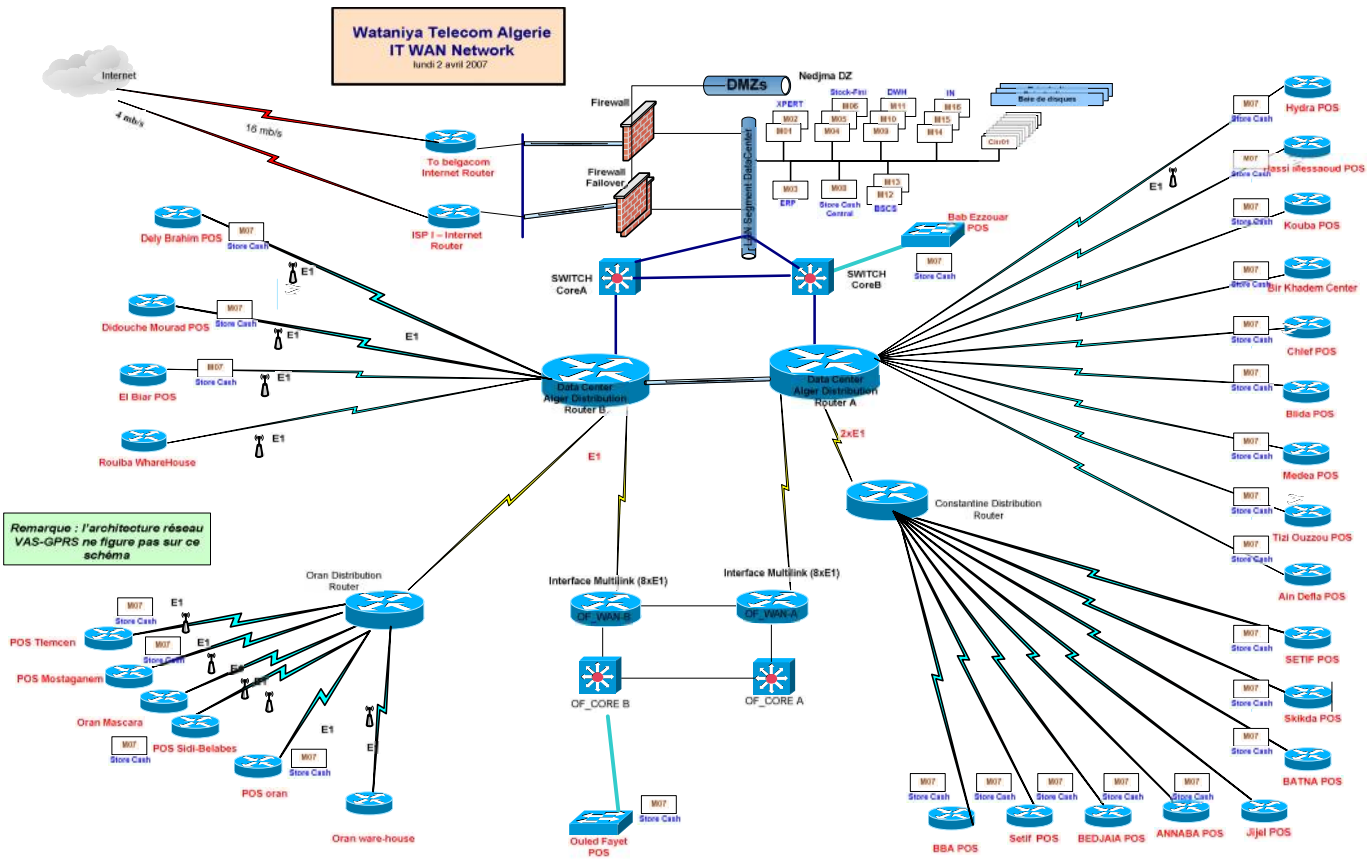


Figure II.2. Architecture du réseau de Wataniya

II.8 Conclusion :

Ooredoo est une compagnie internationale leader des télécommunications qui fournit les services de téléphonie mobile, fixe et l'Internet haut débit et les services Entreprise adaptés aux besoins des particuliers et des entreprises.

Et dans le prochain chapitre on va évoquer le problème de la qualité de service dans le réseau IP.

CHAPITRE

III

La Qualité de Service

III.1. Introduction :

A ses débuts, Internet avait pour seul objectif de transmettre les paquets à leur destination. Conçu pour le transport asynchrone des données, IP (internet Protocol) n'a pas été prévu pour les applications en temps réel comme la téléphonie ou la vidéo, très contraignantes. Le besoin en équipement de plus en plus fiables, d'un bout à l'autre du réseau, est donc devenu incontournable.

Cependant, les défauts rencontrés sur les réseaux (perte de paquets, congestion) ne peuvent pas être surmontés sans une rénovation profonde de l'architecture.

Dans ce chapitre, on va évoquer le problème de la qualité de service dans le réseau IP tout en détaillant les paramètres de performances du réseau afin de fournir un service meilleur et plus prévisible en terme de : débit, délai de latence, variation de délais ou gigue et taux de pertes de paquet.

III.2. Définition :

La qualité de service d'un réseau désigne sa capacité à transporter dans de bonnes conditions les flux issus de différente application.

Les applications concernées peuvent alors générer des flux de type : informatique(transfert de fichiers, transactionnel, etc.), voix (stream audio), ou images vidéo (stream vidéo).

Les flux engendrés par les applications étant très divers, ils donnent lieu à des mises en œuvre variées selon le niveau de QoS exigé par les applications.

III.3. Paramètres de qualité de service :

La maitrise de la qualité de service est un enjeu essentiel. Elle doit être visualisée et mesurée de bout en bout .Le contexte joue un rôle crucial dans l'appréciation des paramètres de la qualité de service qu'il faut adapter aux besoins de l'entreprise.

Il y a cinq paramètres techniques à prendre en compte dans la qualité de service qui sont :

1. **La disponibilité du réseau :**

La disponibilité d'un réseau se définit comme le rapport entre le temps de bon fonctionnement du service et le temps total d'ouverture du service. C'est la forme la plus évidente de QoS, puisqu'elle représente la possibilité d'utiliser un réseau.

2. **Débit :**

Le débit maximum ou la bande passante est considérée comme étant le taux de transfert maximum pouvant être maintenu entre deux points terminaux.

La QoS ne génère pas la bande passante. En revanche, ses mécanismes permettent de gérer de façon optimale la bande passante du réseau en fonction des demandes des applications. Dans les réseaux à commutation de paquets, la garantie de bande passante est un paramètre de performance très important pour garantir la QoS aux flux temps réel. Ces derniers, ont une exigence minimale en terme de bande passante égale à leur débit moyen.

3. Temps de réponse (latence):

Il s'agit du temps d'attente pour mesurer le temps écoulé pour la transmission des paquets IP.

La maitrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode de transmission. Or la durée de traversée d'un réseau IP dépend de nombreux facteur :

- Le débit de transmission de chaque lien.
- Le nombre d'éléments réseaux traverse.
- La taille des paquets.

Les éléments d'infrastructure, notamment les routeurs, peuvent également mettre en œuvre des buffers de gigue.

4. Variation des délais de traversée (gigue ou jitter)

La Gigue est une variable temps causée par le fait que les paquets ne traversent pas le réseau à la même vitesse. Pour supprimer ce phénomène, il faut collecter les paquets et les garder assez de temps pour que les paquets les plus lents arrivent et qu'ils se placent correctement dans la séquence d'où la gestion d'un buffer de paquets. Ce phénomène est plutôt gênant car il engendre des retards importants.

La gigue est encore plus problématique puisque les deux objectifs que sont l'élimination de cette dernière et la diminution des délais sont clairement contradictoires. Il faut donc optimiser la taille du buffer pour minimiser son impact sur les délais engendrés. En téléphonie sur le câble la solution est de compter le nombre de paquets qui arrivent en retard et de créer un ratio de ce nombre au nombre de paquets arrivés dans les temps. Ce ratio est utilisé pour ajuster au mieux le buffer de gigue.

5. Taux de perte de paquets

Dans les réseaux IP d'aujourd'hui, les trames de données de voix sont traitées comme celles de données. Lors des hausses d'utilisation du réseau et de congestion de celui-ci, les trames de données de voix vont être transmises au même taux que les trames de données.

Il existe plusieurs solutions au problème de la perte accidentelle de paquets. Ici la retransmission des paquets n'est pas de mise puisque les temps de latence engendrés seraient trop importants. Il faut donc envisager d'autres solutions :

- L'interpolation consiste à remplacer le paquet perdu par le dernier paquet reçu. Cette méthode est relativement efficace sauf si un grand nombre de paquets consécutifs sont perdus
- La redondance consiste à envoyer les paquets N avec les paquets N+1, et ce, continuellement. Cette méthode a l'avantage de très bien remédier au problème des paquets perdus. Cependant cette méthode utilise beaucoup la bande passante et contribue à créer des temps de latence.
- Une autre méthode consiste à envoyer les informations redondantes après les avoir codées pour qu'elles soient moins volumineuses. Cette méthode réduit le problème de bande passante mais continue à générer du délai.

III.4. Les classes de services :

Ces paramètres sont ensuite regroupés entre eux en fonction des besoins des applications et des services. Ces groupes forment alors des **Classes de Services** (class of services : CoS).

Les requêtes de QoS des applications ou des services seront toujours affectées à une classe de service donnée. A chaque classe, correspond un ensemble de paramètre de QoS avec des objectifs quantifiés. Plusieurs modèles de CoS ont été standardisés et peuvent être utilisés indifféremment.

- **Voix :** Regroupe toutes l'application du type conversationnel (voix, Visio, conférence,..) ayant pour contrainte forte des objectifs sur le délai et la gigue. Elles sont également sensibles au taux de perte bien qu'il ne soit pas possible de retransmettre les données et requièrent des débits assez faibles.

- **Vidéo :** Regroupe toutes les applications multimédia (vidéo à la demande-VoD, la télévision sur IP –IP TV,..) ayant pour contrainte forte le taux de perte et le débit et dans une moindre mesure le délai et la gigue.

- **Donnée :** Regroupe toutes les applications de transfert de données ayant pour seule contrainte un taux de perte nul et qui s'accommodent d'un délai et d'une gigue quelconque. Un débit garanti caractérise cette classe sans toutefois en faire une contrainte stricte.
- **Défaut :** Désigne toutes les applications n'exigeant aucune garantie de QoS. Bien connu sous l'anglicisme «**BEST-EFFORT**» c'est le mode de transport du protocole IP.

III.5. Déploiement de QoS dans un réseau :

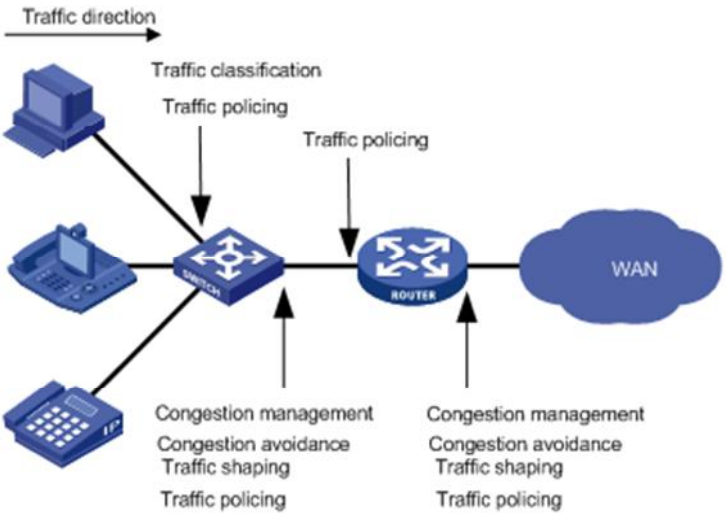


Figure III.1. Position des techniques de QoS dans un réseau

Comme le montre la **Figure III.1,** la classification du trafic, mise en forme du trafic, de la police de la circulation, gestion de la congestion, et l'évitement d'encombrement principalement mettre en œuvre les fonctions suivantes:

- La classification du trafic utilise certains critères de correspondance pour attribuer les paquets avec les mêmes caractéristiques à une classe. Basé sur les classes, vous pouvez fournir des services différenciés.
- Traffic policing police les flux entrant ou sortant d'un dispositif, et impose des sanctions sur les flux de trafic qui dépassent le seuil de pré-série pour empêcher l'utilisation agressive des ressources du réseau. Vous pouvez appliquer police de la circulation à la fois le trafic entrant et sortant d'un port.
- Trafic Shaping proactive adapte le taux de sortie de trafic vers les ressources réseau disponibles sur l'appareil en aval pour éliminer les paquets gouttes. Le lissage du trafic applique habituellement le trafic sortant d'un port.
- Gestion de la congestion fournit une politique de planification des ressources pour déterminer la séquence de transmission de paquets en cas de congestion se produit. Gestion de la congestion applique habituellement à le trafic sortant d'un port.
- Congestion avoidance surveille l'utilisation des ressources du réseau, et est généralement appliqué pour le trafic sortant d'un port. Lorsque la congestion se détériore, l'évitement d'encombrement réduit la longueur de la file d'attente en éliminant des paquets.

III.6. Mécanismes de garantie de la qualité de service (modèles de services) :

La transmission des paquets à travers un réseau IP nécessite des performances respectables ainsi qu'une grande stabilité. Une transmission est gravement perturbée par d'éventuels retards ou coupures, il faut donc veiller à ce que le flot soit le plus continu possible et que les variations restent faibles.

Un réseau IP Classique offre un simple service qui est best effort. La diversité des services à supporter entraine également une stratégie de gestion de qualité de service différente. IntServ est une technique qui permet un service garanti en traitant les flux des paquets en fonction de la demande de la source juste avant de démarrer l'envoi des paquets utiles et cela par la réservation des ressources. Cependant, ce mécanisme ce heurte à un autre problème, celui du facteur d'échelle. Avec IntServ chaque routeur dans le réseau doit garder l'état de chaque flux qui y transite jusqu'au moment ou la liaison s'achève. Un deuxième service qui est permit sur le réseau IP est le service différencié et cela par le mécanisme DiffServ. Ce dernier permet de différencier les classes au niveau de chaque routeur. Il résout le problème du facteur d'échelle d'IntServ en définissant un nombre limité de comportement au niveau de chaque nœud. Le MPLS est aussi un mécanisme de qualité de service permettant des applications temps réel parce qu'il permet une optimisation de trafic et délai d'acheminement plus court.

Cette partie présente plus en détails les mécanismes : Best effort, IntServ (INTegratedSERvice), DiffServ (differenciated Services) et finalement le **MPLS (**multi-Protocol Label Switching).

III.6.1. Service Best effort :

Le réseau Internet est basé sur un service réseau très simple dit best-effort. Le service best-effort offre le transfert de paquets mais sans aucune garantie sur le délai qui dans le pire des cas peut être infini, c'est à dire le paquet peut être perdu. Les applications utilisant ce service sont des applications élastiques, c'est à dire qu'elles peuvent s'adapter aux conditions variables de bande passante disponible et aux variations du délai des paquets. Avec le service best-effort les applications n'ont pas besoin de faire une requête avant de commencer à envoyer leurs paquets et elles peuvent envoyer autant de trafic qu'elles veulent. Bien évidemment, il se peut que tout le trafic ne puisse pas être acheminé à cause d'un manque de capacité du réseau. L'idéal est que l'application adapte son trafic en fonction de la capacité disponible à tout moment. Ceci peut être effectué, par exemple, en utilisant TCP. Cependant, avec le service best effort, il existe aussi le risque qu'un ou plusieurs utilisateurs surchargent les routeurs et ne permettent pas que d'autres utilisateurs puissent envoyer leurs paquets. Bref, un problème majeur dans le service actuel best-effort est le manque d'isolation de flux.

Une observation importante est que le buffer dans un router est utilisé en fait pour deux tâches. Tout d'abord il sert à multiplexer les différents flux qui passent par le routeur, mais aussi un buffer sert à absorber les rafales de trafic de chaque flux. Dans les routeurs actuels une fonction dégrade l'autre car un même buffer est utilisé pour les deux fonctions et il n'existe vraiment pas de contrôle du trafic dans les routeurs.

III.5.2. Services Intégrés : Intserv (INTegratedSERvice) :

III.5.2.1. Présentation d'IntServ :

L'Internet a été conçu pour assurer l'interconnexion des réseaux en mode paquet sans prendre en compte la qualité de service. Il est fondé sur un service unique, le Best Effort, qui permet une simplification des équipements d'interconnexion opérant par la discipline FIFO (First In First Out), mais aucune garantie pour le délai ou la perte des paquets. Avec l'apparition de nouvelles applications multimédia (visioconférence, …) exigeant de la bande passante ainsi que des contraintes strictes de la qualité de service, le Best Effort n'est plus suffisant pour éviter les congestions; phénomène qui allonge les délais, génère de la gigue et provoque la perte des paquets.

Pour améliorer la QoS dans l'Internet, le groupe IntServ (Integrated Services) de l'IETF, crée en 1994, a proposé une architecture à Intégration de Services dans laquelle il est possible de garantir le taux de perte et le délai d'acheminement observés par un flux individuel, tout en contrôlant la distribution de ressources entre les flux.

Le modèle de IntServ, issu des travaux de standardisation, définit deux nouveaux services: Garanti (Guaranteed) et à charge contrôlée (ControlledLoad), mieux adaptés aux nouveaux besoins des utilisateurs et des applications.

La philosophie de ce modèle repose sur un contrôle d'admission et sur la réservation de ressources sur tous les nœuds traversés et pour chaque flux. Pour effectuer cette réservation par flux, le protocole de signalisation RSVP (ReSerVation Protocol) a été développé.

RSVP établit et maintient un état logiciel entre les nœuds constituants le chemin emprunté par les paquets. Cet état logiciel est caractérisé par des messages périodiques de rafraîchissement envoyés le long du chemin pour maintenir l'état de réservation. Au niveau technique, la réservation de ressources par flux présente des difficultés d'implémentation et des limitations de déploiement. Le déploiement à grande échelle de RSVP se heurte à la difficulté de gérer un grand nombre d'utilisateurs (scalability). Plus il y a d'utilisateurs de IntServ/RSVP, plus il y a d'états à créer et maintenir pour des destinations différentes à chaque fois. Le coût introduit par la gestion des états et l'ordonnancement par flux peut entraîner une réduction considérable de leur performance.

L'architecture Intserv s'organise autour du concept de flot de données correspondant à un ensemble de paquets résultant d'une application utilisatrice et ayant un besoin d'une certaine QoS. Afin de satisfaire la QoS requise, Intserv propose d'effectuer une réservation des ressources nécessaires à l'établissement de celle-ci via le protocole de réservation de ressources nommé RSVP. Le signal RSVP étant constitué par l'information de contrôle de la QoS, celui-ci propose des directives afin de mettre en place la réservation mais ne dit pas comment la mettre en place, ce domaine étant réservé aux routeurs du réseau qui prennent en compte la signalisation RSVP.

Pour se faire, les routeurs disposent de quatre fonctions de contrôle du trafic :

1. **Le protocole de réservation de ressource :** qui, de façon implicite, signalise le chemin à établir en sollicitant des réservations de bande passante sur chaque routeur traversé du réseau.
2. **Le contrôle d'admission** : permet d'autoriser l'arrivée d'un nouveau flot muni de sa QoS sans perturber les QoS des autres flots existant.
3. **Le classificateur de paquets :** qui classent les paquets de flots admis dans les classes spécifiques. Le classificateur se base sur le contenu de l'en-tête du paquet détermine à quelle classe appartient le paquet. Une classe correspond à une catégorie de flux par exemple le flux audio, ou encore le flux vidéo. Cela permet d'attribuer des caractéristiques distinctes à chaque flux.
4. **L'ordonnanceur de paquets :** qui détermine l'ordre de service des paquets.

Ainsi RSVP va maintenir un chemin dynamique à l'intérieur du réseau,*dynamique* car rafraîchit par des messages périodiques stipulant l'état du chemin au travers des routeurs.

III.5.2.2. Le protocole RSVP (ReSerVation Protocol)

RSVP est un protocole de signalisation pour allouer dynamiquement de la bande passante aux applications orientées réseaux dans des environnements traditionnellement datagramme. Il est particulièrement utile pour les applications multimédias de type CBR. RSVP est utilisé dans le modèle IntServ mais il peut être utilisé hors de ce contexte (par exemple pour établir des chemins MPLS).

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

mise en œuvre et n'aurait pas été adaptée aux besoins du récepteur. D'autre part, certains émetteurs auraient eu tendance à toujours demander la réservation la plus importante qui aurait nui au système dans sa globalité. Le fait que le récepteur décide des ressources dont il a besoin permet une facturation différenciée par récepteur.

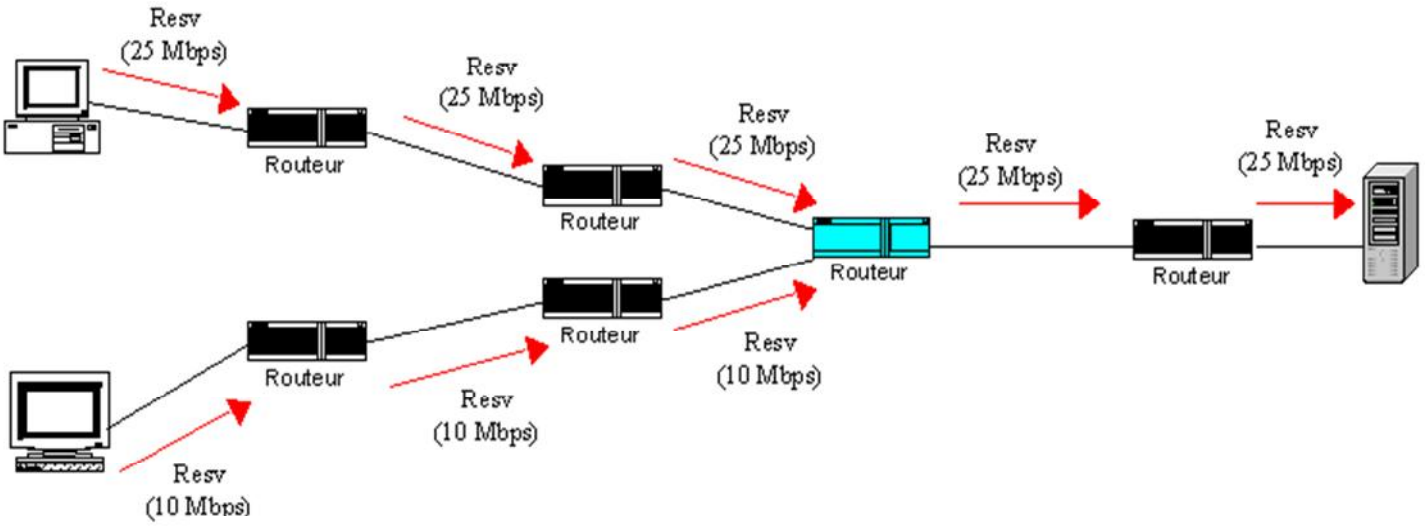


Figure III.1. Réservation de ressources dans un flux multicast

RSVP n'est pas un protocole de routage. Il est censé travailler avec les protocoles de routage unicast et multicast

RSVP fait des réservations de ressources pour les applications unicast et multicast et s'adapte dynamiquement aux évolutions (participants, changements de routes). Il demande des ressources dans une seule direction et traite l'émetteur et le récepteur de manière différente.

Il est utilisé par un "host" pour le compte d'une application, pour demander une QoS au réseau (bande passante garanti, débit crête,..). Il est utilisé par les routeurs pour le contrôle de la QoS et l'établissement et maintient du service demandé.

III.5.2.3. Fonctionnement de RSVP

1) Types de messages

Sept Types de Messages RSVP ont été prévus:

- Path: envoyé par la source pour indiquer la liste des routeurs du chemin suivi par les données;
- Resv: demande de réservation;
- PathErr: message d'erreur concernant le chemin;
- ResvErr: message d'erreur de demande de réservation;
- PathTear: indique aux routeurs d'annuler les états concernant la route;

- ResvTear: indique aux routeurs d'annuler les états de réservation (fin de session);
- ResvConf (optionnel): message de confirmation envoyé par le routeur au demandeur de la réservation;

Un message RSVP est constitué d'une en-tête et d'un nombre variable d'objets qui dépend du type du message.

L'entête est constitué de 64 bits:

Vers	Flags	Type du Msg	Checksum
Send_TTL		Réservé	Longueur Msg.

- Vers (4 bits): version du protocole RSVP (=1);
- Flags (4): non utilisé à ce jour;
- Type de Msg (8): 1 à 7 selon le type ci-dessus;
- Checksum (16): Contrôle d'erreurs;
- Send_TTL (8): valeur du TTL IP à comparer avec le TTL du paquet IP pour savoir s'il y a des routeurs non-RSVP;
- Longueur (16): longueur du message en octets (en-tête et objets)

III.5.3. Services différenciés(DiffServ):

III.5.3.1. Présentation de DiffServ :

La différenciation de services consiste dans une situation de congestion à reporter les pertes de paquets sur certaines classes de trafic, pour en protéger d'autres. Il n'y a donc pas de garantie sur les flux car il n'y a pas de contrôle d'admission dynamique permettant d'éviter une congestion.

Le contrôle d'admission est fait a priori par la définition d'un contrat pour chaque classe de trafic et par le dimensionnement des ressources pour pouvoir garantir ce contrat. Les paquets DiffServ sont marqués à l'entrée du réseau et les routeurs décident en fonction de cette étiquette de la file d'attente dans laquelle les paquets vont être placés. Cette architecture convient à des réseaux pour lesquels il n'est pas raisonnable d'envisager une signalisation flux par flux. Elle ne considère donc que des agrégats de flux pour lesquels une signalisation avec réservation de ressources peut être envisagée. En fait un routeur de cœur ne conserve pas d'état pour un flux ou un

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

Cette zone se décompose en un premier champ de trois bits baptisé" IP Precedence ", qui précise le niveau de priorité appliqué au paquet. Vient ensuite un champ de 4 bits, dont la valeur détermine un critère de routage. Le dernier bit du champ reste inutilisé. Cette classification s'opère à l'entrée du réseau étendu, déchargeant ainsi les routeurs de la tâche. La différenciation de services présente les avantages suivants :

- La signalisation est faite dans chaque paquet en attribuant une signification différente aux bits du champ type de service. Il n'est plus besoin de garder dans le routeur un contexte liant le flux de signalisation au flux de données. Cela permet aussi une agrégation naturelle des flux, ainsi pour un opérateur, les paquets qu'il reçoit marqués pour une certaine classe peuvent appartenir à plusieurs sources.
- La complexité du traitement est concentrée dans les routeurs aux frontières du réseau. Ils effectuent les opérations « complexes » de contrôle de la validité du contrat pour les différentes classes de trafic. Dans le cœur du réseau, le traitement est plus simple, ce qui autorise un relayage rapide des données. • La tarification du service est plus simple, il suffit de définir les paramètres de contrôles de classes de service.

Au contraire du modèle Intserv qui traite indépendamment chaque flot, le modèle Diffserv sépare le trafic par classes. Nous avons donc affaire à une granularité moins fine mais qui devient en revanche plus « scalable ». En effet, la granularité du flot implique la réaction en chaîne suivante : plus il y a d'utilisateurs dans le réseau, plus il y a de flots, plus il y a de variables de classification et d'ordonnancement dans les routeurs à maintenir, ce qui a pour conséquence une charge importante au niveau des routeurs qui deviennent alors de moins en moins performants. Les routeurs DiffServ traitent les paquets en fonction de la classe codée dans l'entête IP (champ DS) selon un comportement spécifique : le PHB (Per Hop Behaviour). Chaque ensemble de paquets défini par une classe reçoit alors un même traitement etchaque classe est codée par un DSCP (DiffServ Code Point). Un PHB est défini par les priorités qu'il a sur les ressources par rapport à d'autres PHB. En aucun cas, les routeurs ne traiteront différemment des paquets de même PHB et de sources différentes. L'avantage de Diffserv est qu'il n'y a plus nécessité de maintenir un état des sources et des destinations dans les routeurs, d'où une meilleure scalability.

Diffserv définit quatre PHB ou classes de service :

- Best Effort (priorité basse) : PHB par défaut et dont le DSCP vaut 000000 ;
- **Assured Forwarding (AF) (RFC 2597)**: regroupant plusieurs PHB garantissantun acheminement de paquets IP avec une haute probabilité sans tenir compte des délais, cette famille de PHB est scindée en 4 classes garantissant de fournir une bande passante et un délai minimum, chaque classe comprenant 3 niveaux de priorité (Drop Precedence) ;
- **Expedited Forwarding (EF) ou Premium Service (RFC 2598):** correspondant à la priorité maximale et a pour but de garantir une bande passante avec des taux de perte, de délai et de gigue faible en réalisant le transfert de flux à fortes contraintes temporelles comme la téléphonie sur IP par exemple ;
- **Default Forwarding (DF),** utilisé uniquement pour les flux Internet qui ne nécessitent pas un trafic en temps réel. Cette notion de PHB permet de construire une variété de services différenciés.

Les PHB sont mis en œuvre par les constructeurs dans les routeurs en utilisant des mécanismes de gestion de files d'attente (Custom Queuing, WeightedFair Queuing, ...) et de régulation de flux.

III.5.3.2. Architecture Diffserv

Le groupe Diffserv propose donc d'abandonner le traitement du trafic sous forme de flots pour le caractériser sous forme de classes.

Chaque classe est identifiée par une valeur codée dans l'en-tête IP. Cette classification doit se faire sur les routeurs de bordures (*edge router*) à l'entrée du réseau.

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

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

Les routeurs d'accès sont connectés aux clients, tandis qu'un routeur de bordure est connecté à un autre routeur de bordure appartenant à un domaine différent. Les routeurs de bordure jouent un rôle différent de ceux qui sont au cœur du domaine. Ils sont chargés de conditionner le trafic entrant en indiquant explicitement sur le paquet le service qu'ildoit subir. Ainsi, la complexité des routeurs ne dépend plus du nombre

de flux quipassent mais du nombre de classes de service. Chaque classe est identifiée par une valeurcodée dans l'en-tête IP.

Le trafic conditionné est identifié par un champ DS ou un marquage du champ

Type of Service (ToS) de l'en-tête de paquet IPv4 ou l'octet Class Of Service (COS)d'IPv6. Ce champ d'entête IP porte l'indice de la Classe de Service DSCP (Differentiated service Code Point). Sachant que ce travail de marquage est assez complexe et coûteuxen temps de calcul, il vaut mieux limiter au maximum les répétitions.

Les opérations de classification, contrôle et marquage sont effectuées par les routeurs périphériques (*Edge Router*) tandis que les routeurs centraux (*Coré Router*)traitent les paquets en fonction de la classe codée dans l'en-tête d'IP (champ DS) selon uncomportement spécifique : le PHB (*Per Hop Behavior*) codé par le DSCP.

DSCP :c'est le champ qui identifie le traitement que le

Paquet doit recevoir. Ce champ est codé sur 6 bits et fait partie des 8 bits codant le champTOS d'IPv4 ou le champ classe de trafic d'IPv6.

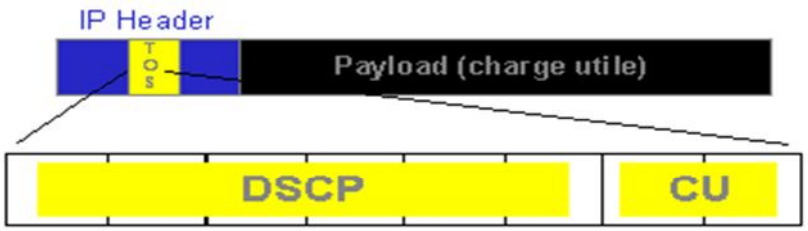


Figure III.2: champ DSCP

DSCP: Differentiated Service Code Point (6bits)

CU : Currently Unused (2bits)

Pour la classe EF DSCP = 101110

Pour la classe AF DSCP = 12 codes (cf. précédemment)

L'architecture des services différenciés proposée dans le [RFC2475] contient deuxd'éléments fonctionnels :

Les **éléments de bordures** (*edge functions*): ils sont responsables de la Classification des paquets et du conditionnement du trafic. En bordure du réseau, C'est à dire à l'arrivée du premier élément actif capable de traiter les champs DS (*DS-capable*), les paquets arrivant ont dans leur champ TOS (pour IPv4) ou Traffic Class Octet (pour IPv6), une certaine valeur DS. La marque qu'un paquet Reçoit identifie la classe de trafic auquel il appartient. Après son marquage, le Paquet est envoyé dans le réseau ou jeté.

Les **éléments du cœur du réseau** (*core functions*) : ils sont responsables de L'envoi uniquement. Quand un paquet, marqué de son champ DS, arrive sur unRouteur *DS-capable*, celui-ci est envoyé au prochain nœud selon ce que l'onappelle son *Per Hop Behaviour* (PHB) associé à la classe du paquet. Le PHBinfluence la façon dont les buffers du routeur et le lien sont partagés parmi les différentes classes de trafic. Une chose importante dans l'architecture DS est que les PHB routeurs se basent uniquement sur le marquage de paquet, c'est à dire laclasse de trafic auquel le paquet appartient ; en aucun cas ils ne traiterontdifféremment des paquets de sources différentes.

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

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

La deuxième opération est assurée par les algorithmes d'ordonnancement servantà contrôler la distribution de ressources entre les classes de service. On peut donner en exemple un type d'ordonnanceurs : **PQ** (*Priority Queueing*).

Le modèle PQ utilise plusieurs files d'attente logiques. Les paquets classifiés sontmis dans une file d'attente correspondant à la valeur du DSCP. Les files sont ensuite servies suivant un algorithme spécifique. Celle qui contient les paquets avec la plus hautepriorité sera favorisée par rapport aux autres files.

III.5.3.3 Classification et conditionnement du trafic

La classification s'effectue suivant une ou plusieurs valeurs contenues dans l'en-tête IP (exemple : adresse source - destination, port source - destination, Protocol ID, ...). Celle-ci faite, elle dirige le paquet vers la fonction de marquage appropriée comme le montre la figure III.3.

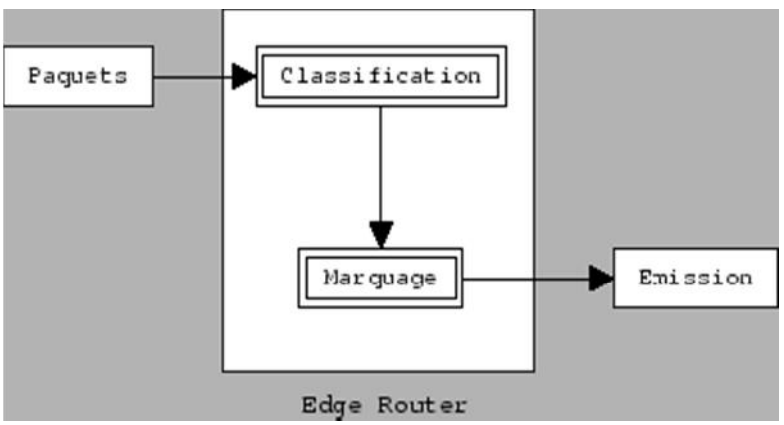


Figure III.3: Arrivée des paquets dans un *edge router*.

Une fois les paquets marqués, ils sont envoyés à leur destination puis à chaque routeur *DS-capable*, ils reçoivent le service associé à leur classe.

Il n'est pas précisé par le groupe de travail Diffserv comment le classificateur est paramétré pour effectuer cette classification, ou plus exactement, qui le paramètre ? Cela doit être fait manuellement, aux bon soins de l'administrateur qui paramètre les tables de marquage des paquets en fonction d'une table d'adresse source, par exemple, donnée au *edge router*. Ou par le biais d'un protocole de signalisation ... RSVP pourrait d'ailleurs très bien faire l'affaire, en effet, celui-ci n'étant pas un protocole de signalisation propre à Intserv uniquement, on pourrait l'utiliser afin de signaler les classes qu'auront les routeurs à traiter.

En plus de cette classification/marquage, un mécanisme de profilage du trafic est défini par le groupe de travail Diffserv. Ce *traffic profile* a pour objet la prise en compte du taux d'arrivée des paquets, afin de ne pas dépasser le seuil maximum de paquets pouvant être envoyés sur le réseau. Ainsi, un mécanisme de mesure du trafic permet de savoir si le flot de paquets entrant correspond au profil de trafic négocié. Si ce flot dépasse un certain seuil, certains paquets seront marqués comme moins prioritaires et seront automatiquement jetés en cas de congestion dans le réseau comme le montre la figure **III.4.**

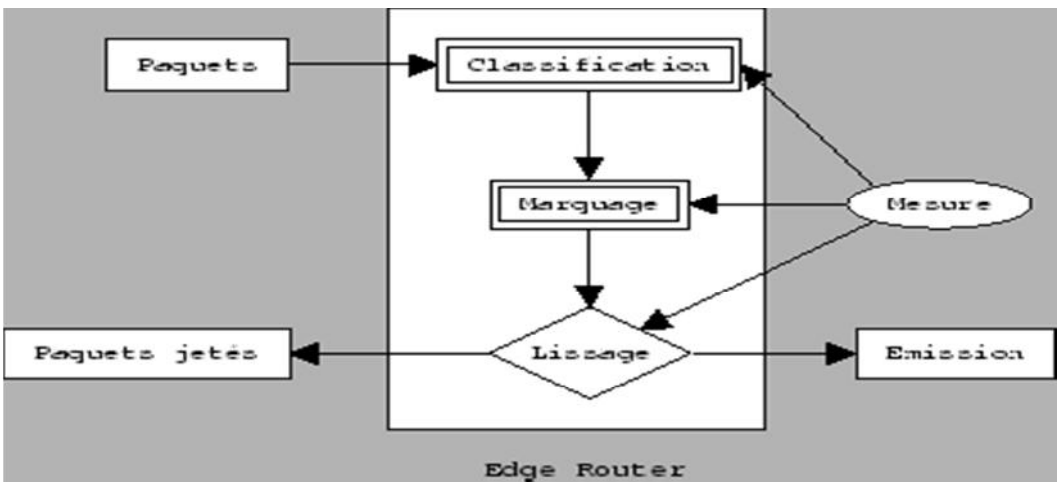


Figure III.4: Classification, marquage et conditionnement du trafic au niveau du edge router

III.5.3.4.GESTION DES FILES et ORDONNANCEMENTS

III.5.3.4.1. Introduction

La gestion des files est nécessaire pour équilibrer le trafic. Elle évite la monopolisation de la queue par un seul flux. Une simple gestion de file n'évite pas que les queues soient pleines pour des périodes longues, alors que pour avoir de faibles délais il est souhaitable que les queues ne soient pas trop chargées. En effet, de petites files d'attente réduisent les délais de transmission. L'objectif de la bufférisassions dans le réseau est avant tout d'absorber des pointes de trafics fugitives. Pour ces raisons des mécanismes supplémentaires complètent la simple gestion de file d'attente de sortie. L'objectif de ces mécanismes est de diminuer le nombre de datagrammes éliminés, de diminuer le délai de bout en bout, d'éviter le remplissage permanent des files d'attente et cela tout en gardant une bonne utilisation du réseau.

Le [RFC2309] définit deux types d'algorithmes de contrôle de congestion :

la gestion des files et l'ordonnancement. Le premier gère la taille de la file en éliminant des paquets si nécessaire tandis que le second détermine quel est le prochain paquet à envoyer sur le lien. Tous deux sont utilisés pour gérer la bande passante utilisée par les flots de paquets.

III.5.3.4.2. L'ordonnancement de trafic :

La file d'attente traite d'ordonnancement des paquets avec des priorités différentes pour transmettre différemment les paquets de haute priorité préférentiellement.

Cette partie décrit brièvement plusieurs mécanismes de file d'attente :

1- First In First Out (FIFO)

C'est l'ordonnancement par défaut, le plus simple qui soit. Les paquets sont mis dans la file de sortie et servis dans l'ordre avec lequel ils ont été reçus par le ou les interfaces d'entrée. C'est aussi la discipline la plus rapide au point de vue de la vitesse de transmission des paquets, étant donné qu'elle n'effectue aucun traitement sur ceux-ci. Cette technique est suffisante dans un réseau à forte capacité car on peut considérer que les files restant presque toujours vides, les délais sont alors faibles voir insignifiants. Par contre, dans le cas d'une rafale, la file d'attente peut se retrouver en débordement et les paquets arrivés après la rafale peuvent être jetés. Dans ce cas, les paquets jetés le sont de manière indifférenciée, sans prise en compte du type de trafic auquel ils correspondent. En utilisant des stratégies de mise en file d'attente différenciée, on peut permettre à certains types de trafic d'être privilégiés en détruisant certains paquets plutôt que d'autres.

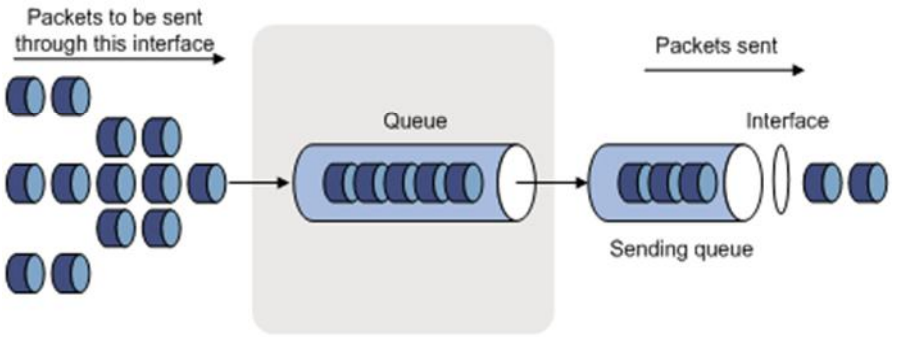


Figure III.5: FIFO Queuing

2- Priority Queuing

C'est la forme primitive de la différenciation de service. En effet, sous ce type d'ordonnancement, les paquets arrivant sur le lien de sortie sont classifiés en une, deux, voire plusieurs classes sur la file de sortie. La classe d'un paquet dépend alors d'un marquage explicite se trouvant dans l'en-tête même de celui-ci. Par exemple, en prenant en compte le champ TOS d'IPv4, ou alors en prenant en compte les autres données présentent nativement dans l'en-tête comme l'adresse source - destination, le port source - destination, ou un autre critère.

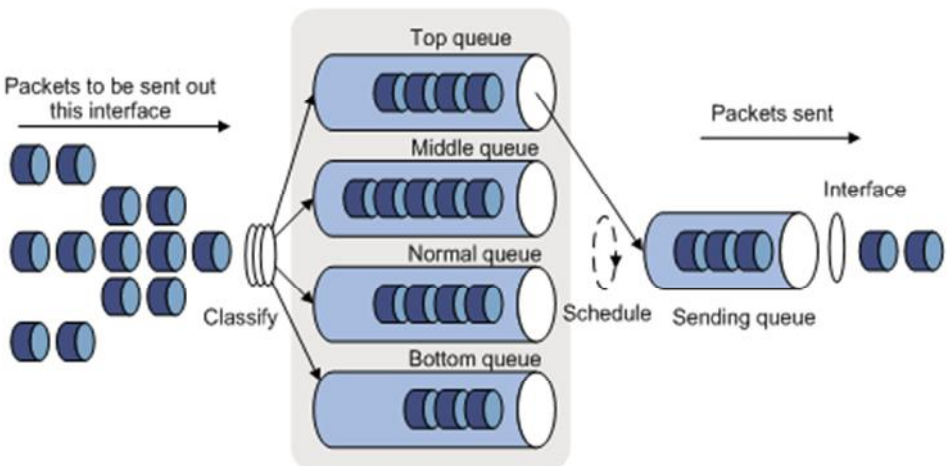


Figure III.6: Priority queuing (PQ)

Comme le montre la figure III.6, chaque classe a sa propre file d'attente. Le serveur choisira d'abord un paquet se trouvant dans la file d'attente haute priorité, si celle-ci est non vide avant ceux se trouvant dans la file basse priorité.

La granularité de classification se basant sur l'en-tête même du paquet est assez flexible. En revanche, ce système implique une dégradation des performances. Il peut y avoir un problème lorsque le trafic haute priorité est très important ; il peut y avoir rejet des paquets du trafic normal à cause de la taille de la file d'attente basse priorité.

L'autre problème qui est soulevé par toutes les disciplines non FIFO, est que le temps d'attente dans les buffers restant indéterminé, on ne peut pas calculer la gigue du réseau de bout en bout. En effet, dans le cas du *priority queuing* par exemple, il est impossible, au niveau du temps de mise en attente dans les files, de déterminer au bout de combien de temps un paquet de priorité basse va être servi, ce service ne pouvant être fait que lorsque aucun paquet ne se trouve en haute priorité.

3. Weighted Fair Queuing

Le partage équitable pondéré est une émulation du *round robin* bit à bit. Les paquets arrivant sont classifiés puis mis dans leurs files d'attente respectives et de la même manière que pour le *round robin,* les paquets sont servis de façon circulaire comme le montre la figure **III.7.**

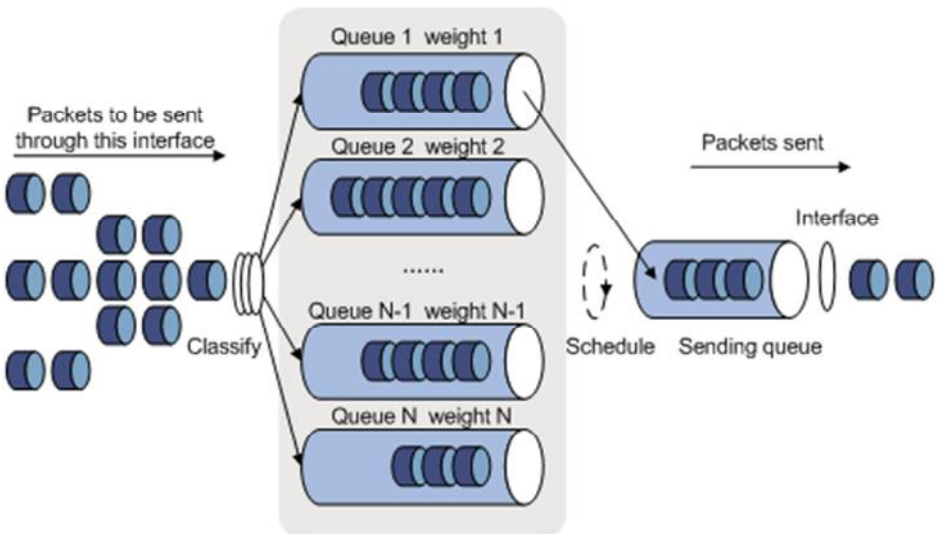


Figure III.7: ***Weighted Fair Queuing***

Ce mécanisme de gestion des files d'attente (qui peut, par exemple, être pondéré par le champ IP Precedence), permet une allocation de bande passante plus ou moins importante pour chaque classe. En effet, le tourniquet servant bit à bit, un poids va être donné pour la file de haute priorité.

Ce mécanisme de tri est dépendant du constructeur car le champ IP Precedence peut avoir milles interprétations différentes et donc tout dépend de ce qu'entend le constructeur dans le terme *weight*. En revanche, ce système de mise en file d'attente par flot peut nous amener à rencontrer certains problèmes de *scalability*.

4- Class Based Queuing

C'est une variation de WFQ, qui utilise également un tourniquet sur plusieurs files mais une classification en amont de la batterie de file va s'intéresser à classifier chaque paquet en fonction de sa classe dans sa file correspondante. Il n'y a donc plus de classification sur le flot. Grâce au *round robin* en sortie des files, on évite qu'une seule classe de trafic ne monopolise toutes les ressources.

Dans [CBQ], Sally Floyd et Van Jacobson proposent une architecture basée sur le partage de lien (*link sharing*). Ce découpage de la bande passante peut être fait en prenant en compte :

- La famille des protocoles utilisés sur le lien,
- Les types de trafics applicatifs (telnet, ftp, mail, ...),
- Les différentes organisations partageant le lien.

Le but du *link sharing* est la classification de ces différents types de trafic afin d'opérer à un partage de la bande passante entre ces trafics comme le montre la **Figure III.8**.

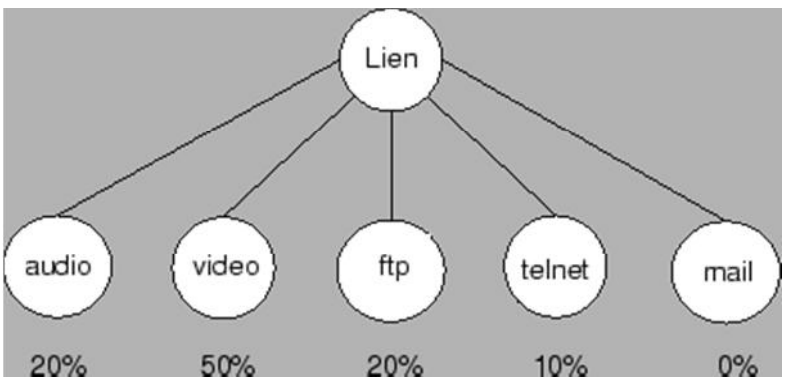


Figure III.8: Partage de lien entre plusieurs classes de services.

Le but principal du *link-sharing* est que chaque classe, avec une demande correspondante à ses besoins, doit être en mesure de recevoir approximativement sa bande passante allouée durant un certain intervalle de temps correspondant à une congestion sur le réseau. Sur la figure **III.8** le *link-sharing* ne donne aucune garantie de bande passante pour le trafic mail.

Le partage peut également être hiérarchisé, entre diverses organisations par exemple, comme le montre la figure**III.9.**

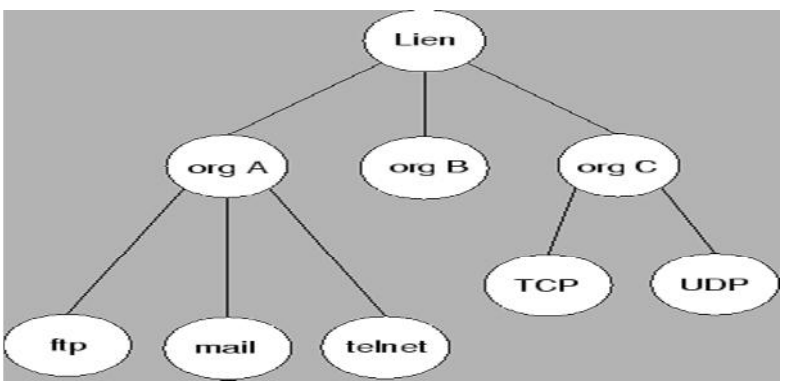


Figure III.9: Partage hiérarchisé d'un lien.

Une part de la bande passante est donc attribuée à chaque niveau. La gestion des queues met en œuvre les différentes variantes de gestion des listes de processus:

priorité, temps partagé. En fait, pour les cas extrêmes il est utile de pouvoir considérer qu'un certain type de trafic est éliminable.

Les mécanismes de partage dans [CBQ] ne tentent pas de fournir un contrôle de congestion au niveau des feuilles de l'arbre (correspondant à une classe de trafic). Ces mécanismes sont implémentés par l'ordonnanceur général à l'entrée du réseau.

Une autre approche consiste à ralentir les flux plutôt qu'à gérer les priorités ou la pénurie le cas échéant. Le ralentissement se commande à l'aide de messages ICMP de ralentissement émis depuis un routeur intermédiaire vers l'émetteur initial du message. Ces messages ne remontent cependant pas à l'application et ne sont donc pas forcément suivis d'effet, d'où l'idée de *trafic shaper* qui diminue la taille de la fenêtre d'anticipation dans l'en-tête TCP de façon à réduire le débit de certains flux. Le classement des trafics se fait selon différents critères: champs TOS, adresses IP source et/ou émetteurs, numéros de ports UDP ou TCP qui permettent d'identifier les flux. On distingue les applications à trafic temps réel ou les applications du type messagerie au trafic moins urgent. Ces modes de gestion sont plus ou moins extensibles à des réseaux importants. Le trafic est géré par une étiquette de TOS pour les datagrammes qui circulent de façon indépendante. Selon le RFC[2309], la notification et la prise en compte de la régulation par IP sont à recommander.

III.5.3.5. Politique de trafic :

Une application typique de la police de la circulation est de superviser la spécification de certains trafic entrant dans un réseau et limiter dans une fourchette raisonnable, ou à la «discipline» du trafic supplémentaire pour empêcher l'utilisation agressive des ressources du réseau par une certaine application. Par exemple, vous pouvez limiter la bande passante pour les paquets HTTP à moins de 50% du total. Si le trafic d'une certaine séance est supérieur à la limite, de la police de la circulation peut déposer les paquets ou réinitialiser la priorité IP des paquets. **Figure III.10** .montre un exemple de police trafic sortant sur une interface.

Trafic de police est largement utilisé dans le trafic de la police d'entrer dans les réseaux des fournisseurs de services Internet (FSI). Il peut classer le trafic policé et prendre des mesures prédéfinies police sur chaque paquet en fonction du résultat de l'évaluation:

- Transférer le paquet si le résultat de l'évaluation est "conforme."
- abandon du paquet si le résultat de l'évaluation est «l'excès."
- Transférer le paquet avec ses précédence IP re-marqué si le résultat de l'évaluation est "conforme."

- Fournir le paquet au niveau suivant police de la circulation avec ses précédence IP re-marqué si le résultat de l'évaluation est "conforme."
- Saisie de la police de niveau suivant (vous pouvez définir plusieurs niveaux de police de la circulation chaque axée sur des objets spécifiques).

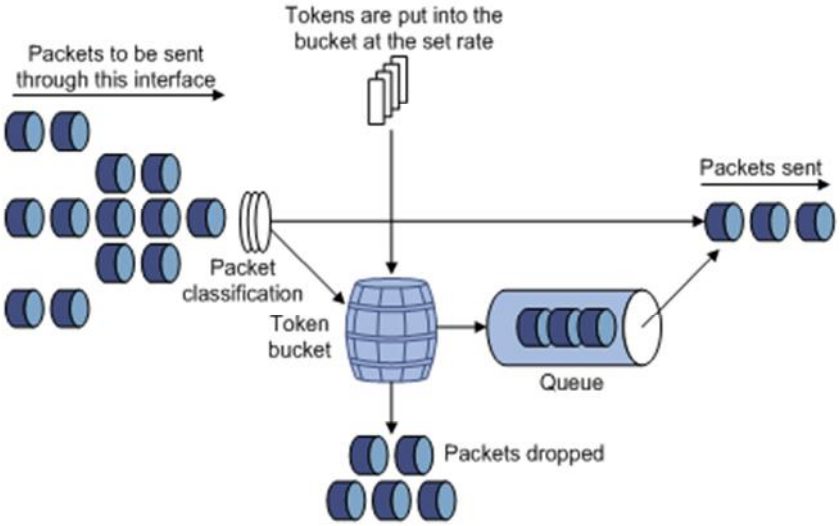


Figure III.10: Traffic policing

III.5.3.6. Lissage du trafic(Trafic shaping)

Le lissage du trafic limite la vitesse de trafic sortant en tamponnant trafic supérieur. Vous pouvez utiliser le lissage du trafic pour adapter le débit de sortie de la circulation sur un dispositif à la vitesse de la circulation de l'entrée de son appareil connecté pour éviter la perte de paquets. La différence entre la police de la circulation et GTS est que les paquets soient abandonnées avec la police de la circulation sont conservés dans une mémoire tampon ou la file d'attente avec GTS, comme montré dans la

Figure III.10 Lorsque suffisamment de jetons sont dans le seau de jetons, les paquets en mémoire tampon sont envoyés à un rythme encore. Le lissage du trafic peut entraîner un retard supplémentaire et la police de la circulation ne fonctionne pas

Par exemple, dans la **Figure III.11**, le routeur B effectue la politique de trafic sur les paquets de routeur A et tombe paquets dépassant la limite. Pour éviter la perte de paquets, vous pouvez effectuer le lissage du trafic sur l'interface de sortie du routeur A si les paquets qui dépassent la limite sont mis en cache dans le routeur A. Une fois que les ressources sont libérées, régulation de trafic prend les paquets cachés et les envoie.

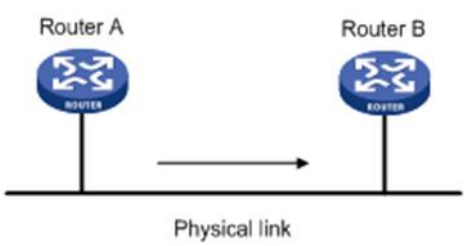


Figure III.11: Traffic shaping

III.5.3.7. Prévention de la congestion

TCP et UDP cohabitent mal, UDP ne possèdant pas de mécanisme de comportement adaptatif, la mise en route d'un algorithme de *congestion avoidance* de TCP laisse place à une augmentation de trafic UDP. Il existe également un autre problème lorsque des points de congestion se développent un peu partout dans un réseau chargé ; chaque flux TCP va détecter des pertes et engager un algorithme de congestion avoidance. Ainsi, de nombreux flux vont repasser en mode slow start et tenter de réémettre les paquets perdus, ce qui ne résolve en rien la congestion déjà présente car le redémarrage des flux se fera de manière synchrone. Ce phénomène connu sous le nom de *global synchronization* met en évidence l'importance de nouvelles techniques plus appropriées pour la prévention de la congestion.

III.5.4.Optimisation de trafic : MPLS(Multi-Protocol Label Switching) :

III.5.4.1. Présentation :

Il s'agit d'un nouveau standard de IETF permettant de simplifier l'administration d'un tel cœur de réseau en ajoutant de nouvelle fonctionnalités particulièrement intéressantes pour la gestion de la qualité de service. Dans le même esprit que l'architecture DiffServ, MPLS permet de réduire le cout des traitements associés au relayage des paquets en les reportant à la périphérie du réseau et en réduisant la fréquence. Il apporte aussi un mécanisme de routage hiérarchique efface, c'est-à-dire des tunnels permettant de gérer les réseaux privés virtuels (vpn).

Il permet également de pouvoir acheminer tous les types d'applications, données, audio, vidéo. Ainsi que de différencier le trafic selon les classes de service employées L'architecture MPLS est constitué de :

- **Routeur d'extremité(LER/LABEL Edge Router) :**

Situé à la frontière de réseau. Il responsable d'insérer et de retirer le label à un paquet au moment de son entrée et de sa sortie.

- **Routeur central (LSR :label Switcher router) :**

Responsable de la communication des paquets en fonction du label. Dans le cœur de réseau, les LSR lisent uniquement les labels, et non les adresses des protocoles supérieurs.

Les objectifs principaux de MPLS sont :

- Permettre un acheminement rapide des paquets IP en remplaçant la fonction de routage par une fonction de commutation rapide.

- Faciliter les fonctions d'ingénierie de trafic en fournissant aux operateurs la maitrise de l'acheminement des données, qui s'avère très complexe avec des protocoles de routage classiques.
- Implémenter des mécanismes de résiliences aux pannes.

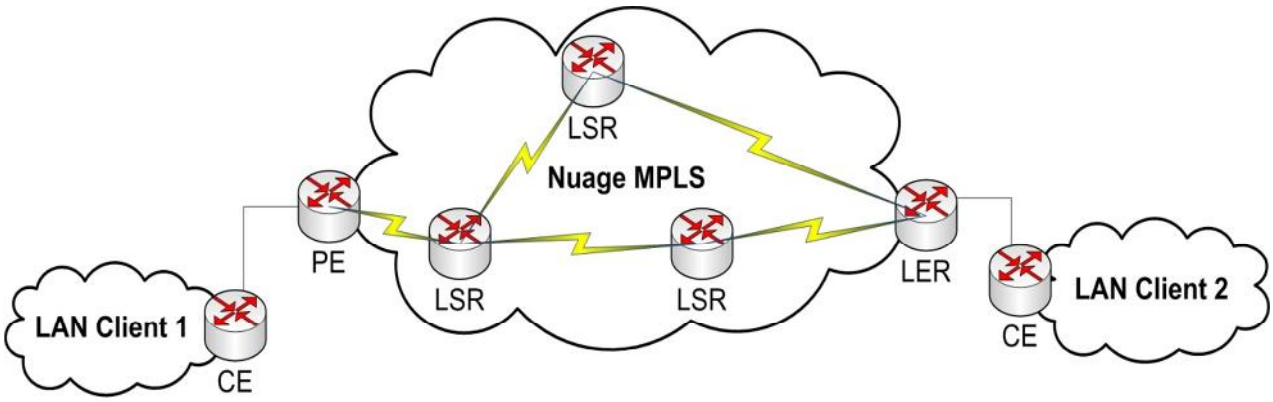


Figure III.12:Modèle MPLS

- CE : Customer Edge => routeur client
- PE / LER : Provider Edge / Label Edge Router => point d'entrée sur le réseau MPLS
- LSR : Label Switching Router => routeur de coeur de réseau
- ELSR : terme CISCO pour désigner un PE
- Nuage : réseau MPLS

III.5.4.2. Principe de fonctionnement de la technologie MPLS (Multi Protocol Label Switching) :

Ce protocole regroupe les qualités des couches 2 et 3 en s'intégrant entre ces 2 mêmes couches.

Il permet de faire un routage et une commutation efficace.

Dans un réseau MPLS les paquets entrant prennent un "label" assigné par un LER (Label Edge Router).

Ces paquets suivent ensuite une route définie LSP (Label Switch Path) et sont traités par le LSR (Label Switching Router) dans lequel ils arrivent.

Chaque LSR choisis la route des paquets qu'il voit arriver, il les renvois sur une interface en fonction du "label" qui est attribué au paquet.

A la sortie, le LSR remplace le "label" qui été présent sur la trame par le sien. Un des avantages majeurs de MPLS est qu'il ne dépend d'aucune technologie existante et donc permet de raccorder plusieurs réseaux de différentes technologies.

Pour acheminer un paquet, un LSR cherche le label dans sa table des labels entrant ILM (Incomming Label Map). A ce label correspond une adresse du LSR suivant, le label de sortie et l'interface de sortie NHFLE(Next Hop Forwarding Label Entry).

III.5.5. Intégration avec d'autres services

III.5.5.1. Intégration IntServ/DiffServ :

L'intégration de ces deux mécanismes est à l'étude. Plusieurs propositions ont été soumises. La première solution consiste à ne mettre l'intégration de service que dans lessites terminaux. Le cœur du réseau ne traite pas les messages de signalisation mais lestransmet comme des paquets normaux qui sont à nouveau interprétés dans le site destinataire.

Un contrôle d'admission en bordure du réseau Diffserv permet dedéterminer si le flux peut entrer dans la classe de service. L'autre possibilité est deconsidérer le réseau DiffServ avec la classe EF comme élément de réseau et lecaractériser pour permettre de construire un service garanti.

III.5.5.2. Intégration MPLS/DiffServ

MPLS permet de simplifier l'administration d'un cœur de réseau en ajoutant de nouvelles fonctionnalités particulièrement intéressantes pour la gestion de la qualité deservice. Dans le même esprit que l'architecture DiffServ, MPLS permet de réduire lecoût des traitements associés au relayage des paquets en les reportant à la périphérie duréseau et en réduisant la fréquence. Il apporte aussi un mécanisme de routagehiérarchique efficace, c'est-à-dire des tunnels permettant de gérer les réseaux privés

virtuels. Le principe de MPLS est d'attribuer un label à chaque paquet lorsqu'il entredans le réseau. Ce label est attribué en fonction de la classe de relayage à laquelleappartient le paquet. La définition de ces classes dépend de l'opérateur du réseau maiselle peut prendre aussi en compte la classe de service DiffServ.

Le label décide donc dans chaque routeur du prochain routeur, du comportement DiffServ et de l'utilisation éventuelle des ressources réservées.

III.6.Conclusion

Dans ce chapitre, nous avons présenté les paramètres de qualité de service pour un réseau IP ainsi que les différents mécanismes en introduisant les trois principaux de QoS sur les réseaux IP, à savoir Intserv convient plutôt aux réseaux de petites tailles, mais n'est pas vraiment adapté à Internet dans son ensemble. De ce fait, il a été peu déployé. Pour pallier ces carences, l'IETF a adopté un second modèle, Diffserv, qui assure une distinction des paquets par classes de flux. Les données sont identifiées grâce à un marquage dans le champ ToS (Type of Service, champ spécifique réservé dans l'en-tête IP de 8 bits), qui fixe les priorités. Cette zone se décompose en un premier champ de trois bits baptisé " IP Precedence ", qui précise le niveau de priorité appliqué au paquet. Vient ensuite un champ de 4 bits, dont la valeur détermine un critère de routage. Le dernier bit du champ reste inutilisé. Cette classification s'opère à l'entrée du réseau étendu, déchargeant ainsi les routeurs de la tâche. Diffserv définit quatre classes de services : Best Effort (priorité basse) ; Assured Forwarding (AF), qui garantit la transmission des données sans tenir compte des délais ; Expedited Forwarding (EF), correspondant à la priorité maximale, qui garantit le délai pour un trafic en temps réel ; et Default Forwarding (DF), utilisé uniquement pour les flux Internet qui ne nécessitent pas un trafic en temps réel. Chaque noeud du réseau apporte un traitement différencié en fonction de la classe de service du paquet. Mais l'arrivée de MPLS a changé la donne.

Cette nouvelle architecture permet de véhiculer davantage de trafic IP à des vitesses de transmission très élevées. Dans ce cas, les paquets transférés sont directement étiquetés (label de 32 bits) à l'entrée du réseau, spécifiant leur chemin, ce qui évite au routeur de chercher l'adresse à laquelle le paquet doit être envoyé. MPLS s'appuie sur les classes de service Diffserv et fonctionne avec tout protocole existant.

Dans le chapitre suivant nous allons présenter les outils matériels et logiciels qui sont utilisés pour mettre en pratique la plupart des solutions mentionnées.

CHAPITRE

IV

Mise en œuvre et application de QoS

IV.1.Introduction

Les réseaux de télécommunications, et en particulier les réseaux informatiques connaissent une expansion sans précédent. Devant l'évolution des techniques et de la technologie, de nombreuses solutions sont envisageables pour un même problème.

La simulation permet ainsi de tester sans aucun coût ces nouvelles technologies, les nouveaux protocoles mais aussi d'anticiper les problèmes qui pourront se poser dans le futur.

Dans ce chapitre nous allons présenter les outils matériels et logiciels qui sont utilisés pour la réalisation de notre maquette réseau, par la suite nous allons présenter notre simulation par la présentation de quelques scénarios.

IV.2. Les différents outils:

IV.2.1. Outils de conception et de réalisation :

- ✓ **Présentation de GNS3 :**

Définition :GNS3 est un simulateur de matériel réseau, il est la suite logique de Packet Tracer. Contrairement aux autres Simulateurs GNS3 utilise un véritable IOS entièrement fonctionnel.

On y retrouve toutes les commandes réelles du matériel Mais surtout:
Il donne la possibilité de mettre ses éléments (virtuels) dans le même réseau que les équipements réels de votre réseau (Machines, Switch, téléphones IP,...).

GNS3 est un produit libre qui utilise (Wincap, Wireshark, Putty…) ce qui parfois pourra un peu encombrer le poste de travail

Outil d'implémentation GNS3 : GNS3 est un simulateur de réseau graphique qui permet de simuler des réseaux complexes. Pour fournir des simulations complètes et précises, GNS3 est fortement lié à :
Dynamips : est un émulateur IOS Cisco.
Dynagen : est une extrémité avant à base de texte pour Dynamips.
Qemu: est un émulateur de machine source et virtualiseur.
VirtualBox: est un logiciel de virtualisation libre et puissant.

- **GNS3** est un excellent outil complémentaire à des véritables laboratoires pour les ingénieurs réseau, les administrateurs…

Il peut également être utilisé pour des fonctionnalités expérimentales de Cisco IOS pour vérifier les configurations qui doivent être déployées plus tard sur des vrais routeurs.

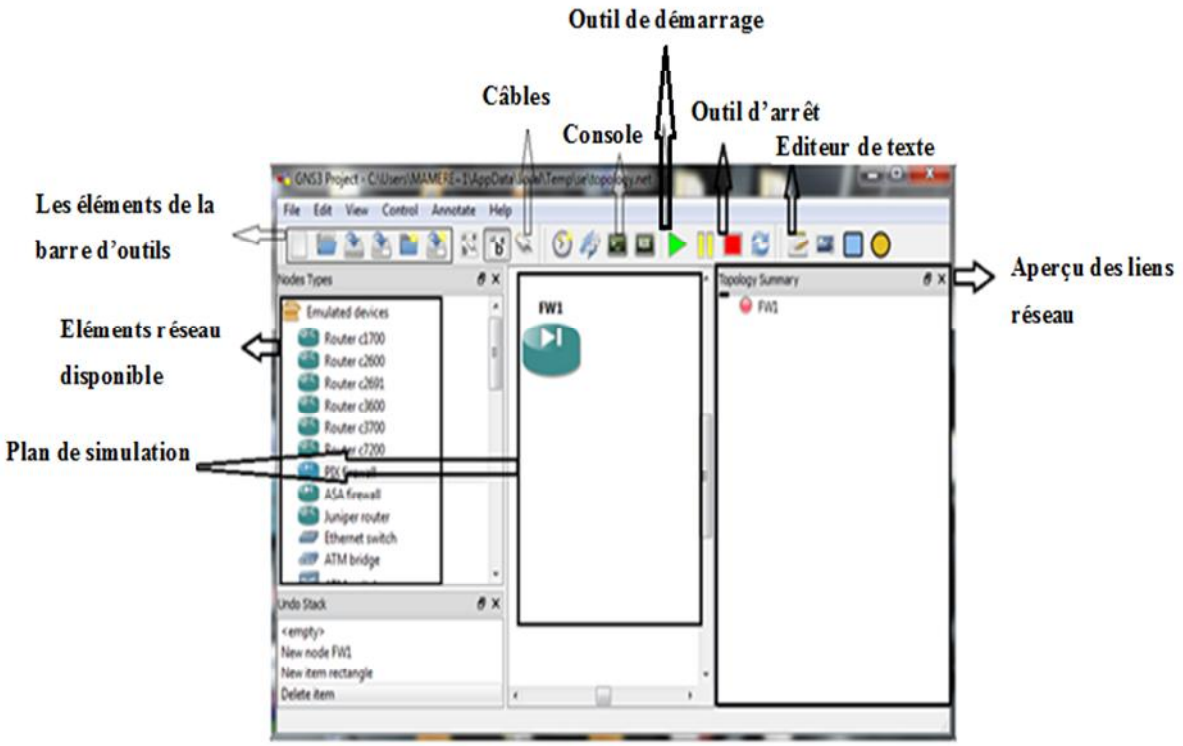


Figure IV.1 : Détail de la fenêtre du simulateur

✓ **Machine virtuelle, Workstation**

VMware permet d'exécuter plusieurs systèmes d'exploitation sur une seule machine hôte par le biais de machines virtuelles tout à fait protégées les unes des autres.

- **Description de VMwareWorkstation :** VMware Workstation permet de créer une machine virtuelle pour les Développeurs et les Administrateurs Systèmes qui veulent révolutionner le développement, le test et le déploiement dans leurs Entreprises. Livré depuis plus de 5 ans et détenteur de plus d'une douzaine de récompenses majeures, VMware Workstation permet de développer et tester des applications complexes s'exécutant sur plates-formes Microsoft Windows, Linux ou NetWare sur une seule machine.
  Les caractéristiques essentielles telles que la création de réseaux virtuels, de gestion de disques virtuels, glisser déposer entre machines, répertoires partagés, et le support de PXE font de VMware Workstation l'outil le plus puissant et le plus indispensable pour les Développeurs et les Administrateurs Systèmes.

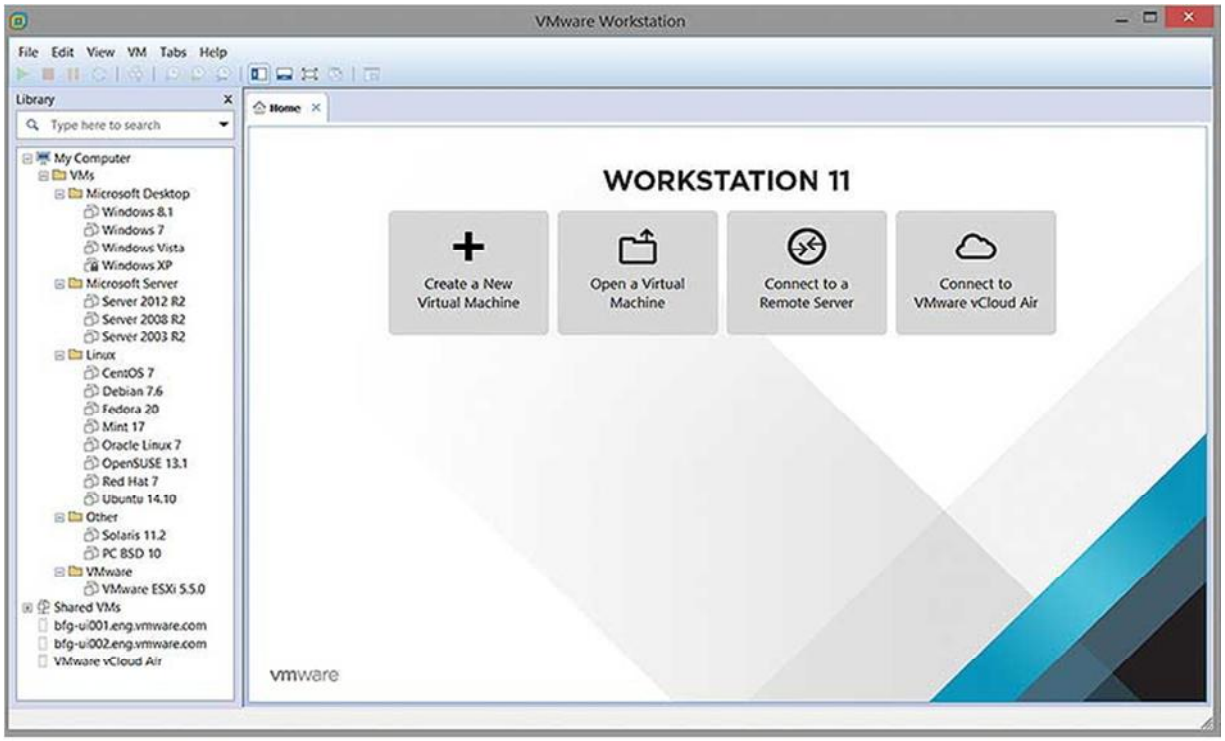


Figure IV.2 : InterfaceWorkstation

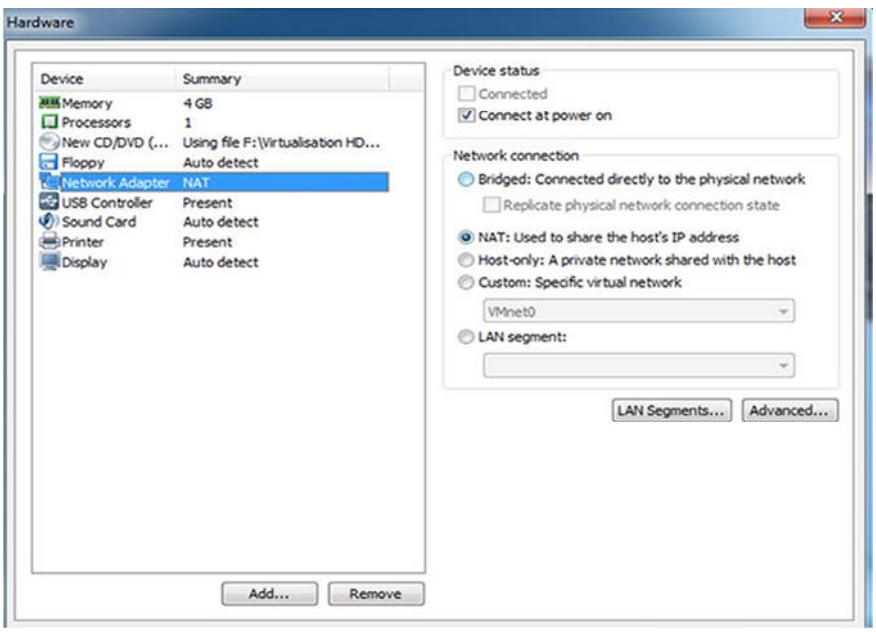


Figure IV.3 : La connexion réseau de la machine virtuelle

Dans la partie "Network Adaptater", vous pourrez modifier la connexion réseau de votre machine virtuelle.

Les différentes possibilités sont :

- **Bridged :** La machine apparait comme une machine connectée physiquement à votre réseau via un pont. (Correspond au mode "Accès par pont" de VirtualBox).
- **NAT :** Permet de partager l'adresse IP de la machine physique. La connexion de la machine virtuelle passe donc par la connexion de la machine physique.
- **Host-only :** La machine est connectée à un réseau virtuel se trouvant uniquement sur votre ordinateur.

IV.2.2. Outils de supervision

A. Netflow Analyzer: NetFlow Analyzer est un outil Web de surveillance de la bande passante, d'analyse scientifique du réseau et d'analyse du trafic réseau qui a contribué à optimiser des milliers de réseaux d'entreprises dans différents secteurs d'activité, leur conférant des performances et une utilisation optimales de la bande passante.

B. L'utilité de Netflow analyzer:

- Collecte des informations sur les performances du réseau
- Evaluation de l'impact des diverses applications et protocoles sur votre réseau
- Détection de tout trafic non autorisé sur le réseau
- Dépannage en cas d'incident
- Surveillance de la bande passante du réseau
- Génération de rapports planifiés et réglage de profils d'alertes

Le fonctionnement de NetFLow repose sur la collecte d'informations à partir de flux provenant directement des équipements réseau. Ces informations détaillées concernent différents critères comme le nombre de paquets et d'octets échangés, les ports applicatifs utilisés, les adresses IP, les interfaces par lesquelles transitent les flux, etc.

Un flux NetFLow se compose de sept champs caractéristiques qui sont :

1) Le protocole de la couche 3 du modèle OSI utilisé (IPv4, IPv6, ICMP, IPSEC, etc.)
2) L'adresse IP source
3) L'adresse IP de destination
4) Le port source
5) Le port de destination
6) Le champ « Type of Service »
7) L'interface d'entrée

Il peut également fournir en fonction de la version du protocole Netflow, des informations complémentaires comme par exemple le volume des données échangées.

L'une des particularités du protocole NetFLow est que les paquets appartenant à un même flux, autrement dit possédant les sept informations précédentes identiques, sont comptées comme un même et seul paquet pour les statistiques.

Un flux NetFlow peut contenir également des informations non caractéristiques, mais très utiles par exemple la date et l'heure de début et de fin d'un flux.

Le but premier de NetFLow étant de fournit un grand nombre d'informations, il est donc normal que les enregistrements NetFlow soient transportés via le protocole UDP.

1. Installation de Netflow Analyzer:

L'installation de Netflow Analyser se fait d'une manière traditionnelle sauf qu'il faut renter certains paramètres au cours de l'installation :

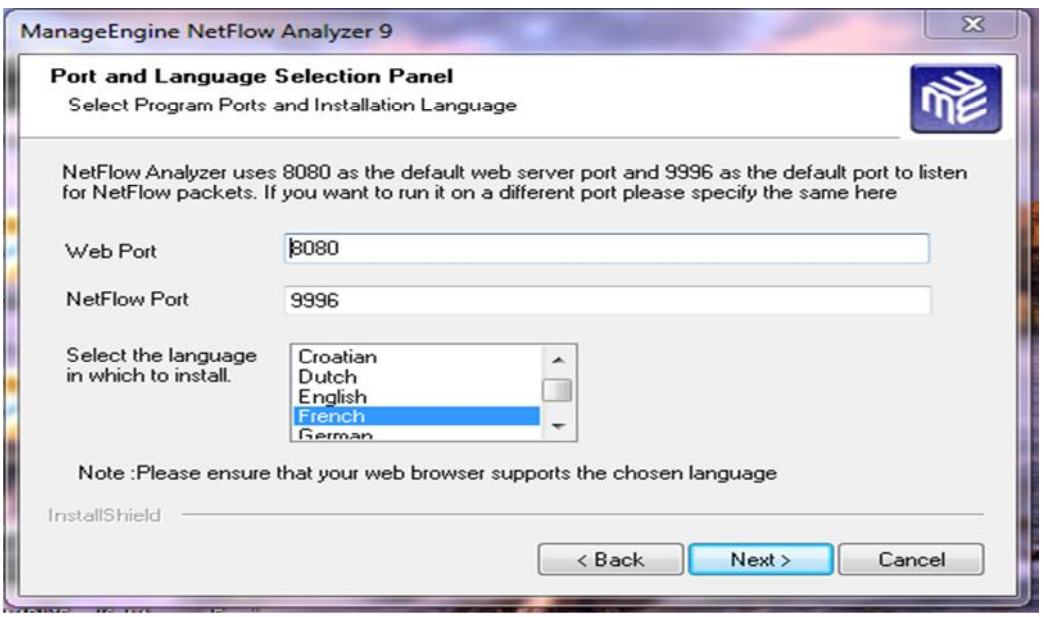


Figure IV.4 : configuration de numéro de port

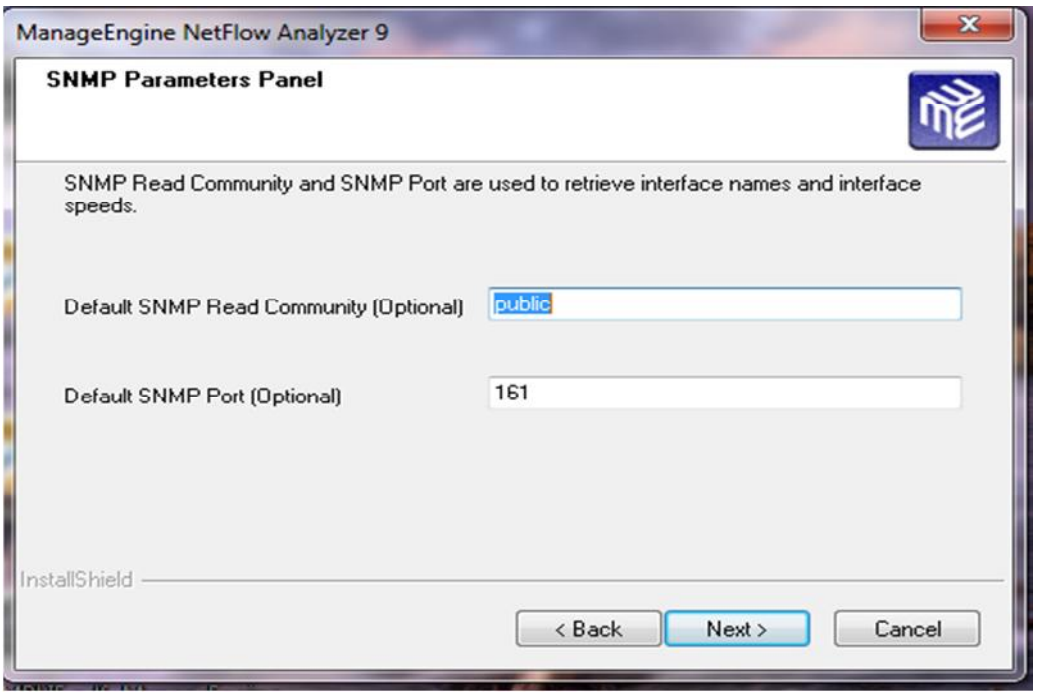


Figure IV.5: configuration du protocole snmp

2. Configuration de Netflow Analyzer

En pratique l'utilisation de NetFlow nécessite une redirection des flux de données dechaque interface des routeurs vers une machine de collecte.
La redirection des flux est décrite dans la configuration suivante:

```
R6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#int fa2/0
R6(config-if)#ip rout
R6(config-if)#ip route c
% Ambiguous command:  "ip route c"
R6(config-if)#ip route-c
R6(config-if)#ip route-cache f
R6(config-if)#ip route-cache flow
R6(config-if)#exit
R6(config)#ip flow-export destination 172.18.5.42 9996
R6(config)#ip flow-export source FastEthernet 2/0
R6(config)#ip flow-export version 5
R6(config)#ip flow-cache timeout active 1
R6(config)#ip flow-cache timeout inactive 15
R6(config)#snmp-server ifindex persist
R6(config)#int fa0/0
R6(config-if)#ip fl
R6(config-if)#ip flow in
R6(config-if)#ip flow ingress
R6(config-if)#ip fl
R6(config-if)#ip flow eg
R6(config-if)#ip flow egress
R6(config-if)#end
R6#
*Mar  1 01:56:15.819: %SYS-5-CONFIG_I: Configured from console by console
R6#wr
```

Figure IV.6 : activation du protocol flow sur le routeur

On fait la même configuration sur les autres routeurs qu'on veut superviser.

Commande	Explication
ip flow-export source {interface}	Neflow analyser va émettre les requêtes SNMP vers cette interface.
ip flow-export destination {ip-addr} {port}	Spécifie l'adresse à laquelle le routeur va envoyer les données SNMP. C'est l'adresse de la machine de supervision.
ip flow-export version {number}	La version de Netflow Analyser
ip flow-cache timeout active {min}	Période d'envoie des informations netflow
ip flow-cache timeout inactive {seconds}	Période de collecte d'informations netflow
ip route-cache flow	Activer la collecte d'informations sur l'interface.

Pour nous assurer que notre configuration est bien prise en compte, on effectue un test par la commande **show ip flow export :**

Figure IV.7 : résultats d'activation de Netflow

La supervision avec netflow analyser se fait à travers une interface web :

Figure IV.8 : interface d'accueil Nteflow Analyzer

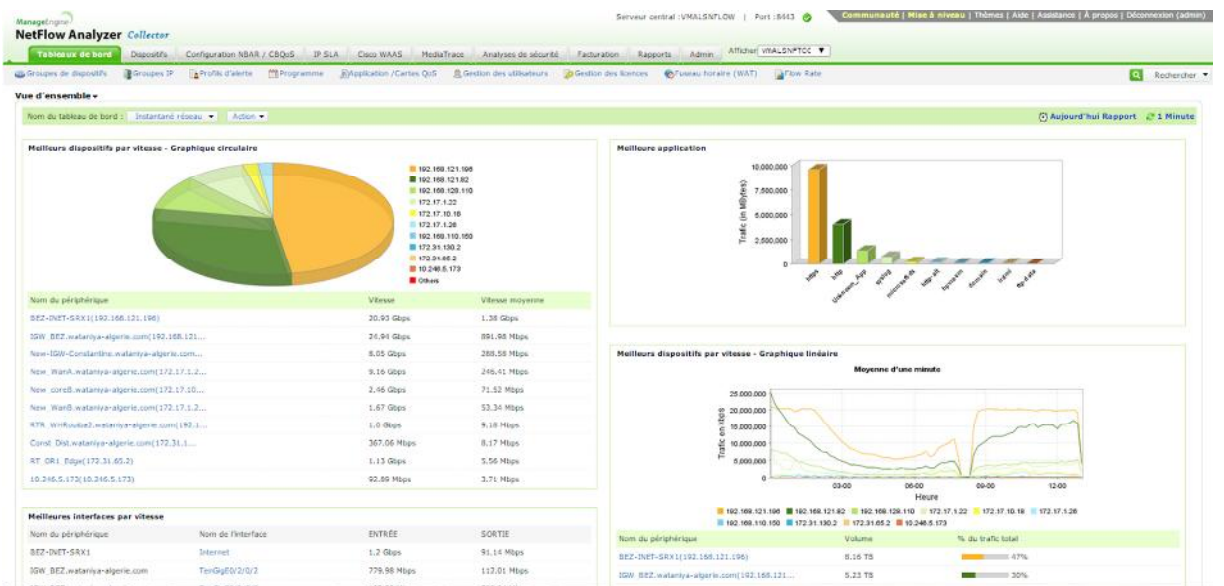


Figure IV.9 : le tableau de bord

- Exemple montrant le trafic passant par les routeurs :

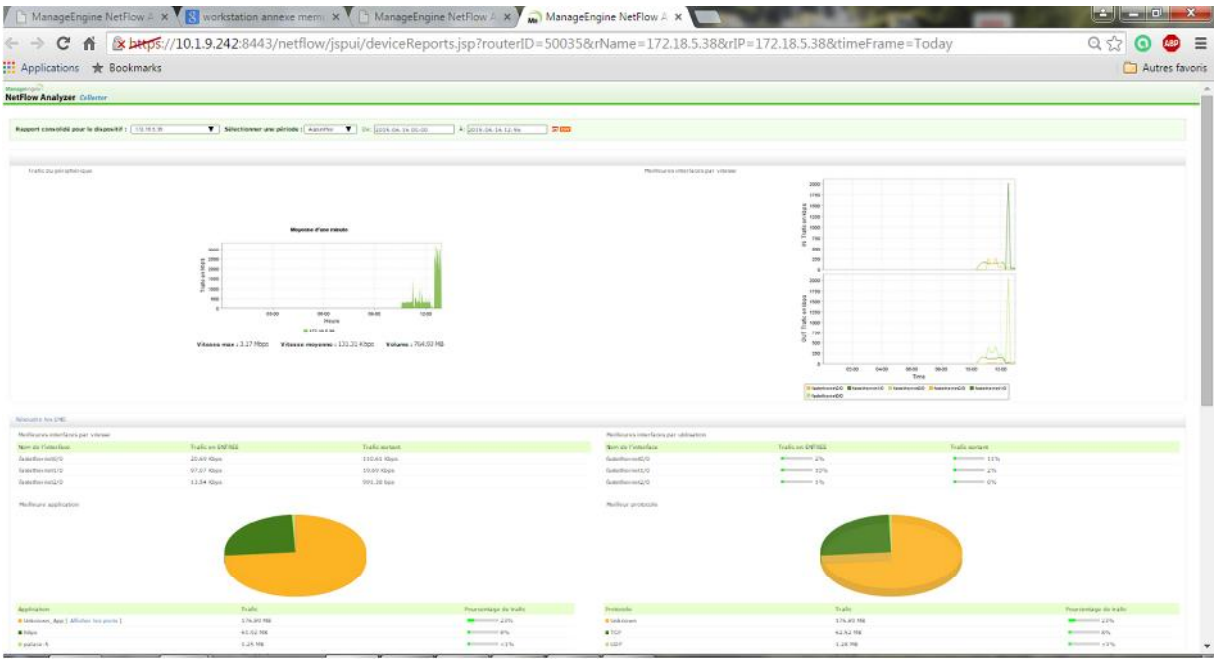


Figure IV.10: Le trafic passant par les routeurs

IV.3. Les services :

Il est nécessaire de présenter les différents services qu'on va définir dans les scénarios d'utilisations :

IV.3.1. TOIP (Telephony over Internet Protocol)

La téléphonie IP consiste à mettre en place des services téléphoniques sur un réseau IP en utilisant la technique de la voix sur IP. Les communications vocales sont alors transmises via un réseau IP à partir de la source à la destination de téléphones spéciaux. Les postes particuliers sont baptisés IP-Phone.

Le téléphone IP doit être alimenté par courant. Il est capable de numériser la voix pour la transmettre sur des réseaux IP et peut, à l'inverse, rassembler les paquets entrants pour interpréter la voix reçue. La téléphonie sur IP circule sur des réseaux privés - LAN ou VPN ou publics.

Le principe de la voix sur IP (dit VOIP pour Voice over IP) est de faire circuler sur Internet, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée.

Elle fait partie d'un tournant dans le monde de la communication. En effet, la convergence du triple Play (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication aujourd'hui.

IV.3.1.1. Les avantages et les inconvénients de la ToIP :

- ✓ **Les Avantages :**

Pour un opérateur ou une entreprise privée possédant son propre central téléphonique analogique ou digital, il existe de nombreux avantages à remplacer ce central traditionnel par un serveur de téléphonie IP. Parmi lesquelles on cite :

- Réduction des coûts
- Disponibilité et mobilité
- Flexibilité
- Simplification de la gestion des réseaux voix, données et vidéo
- les services à valeurs ajoutées

- ✓ **Les Inconvénients**

Evolution ne rime pas toujours avec les progrès. Il en va de même avec la ToIP. L'utilisation

De cette technologie procure certes des avantages mais également des inconvénients. En effet,

Lorsqu'on parle de téléphonie IP, quelques problèmes restent à régler. Les principauxInconvénients de la téléphonie IP sont les suivants :

- Fiabilité et qualité sonore :
  Un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels laqualité de la reproduction de la voix du correspondant ainsi que le délai entre lemoment où l'un des interlocuteurs parle et le moment où l'autre entend peuventêtre extrêmement problématiques dans le milieu professionnel. De plus, il se peutque des morceaux de la conversation manquent (des paquets perdus pendant letransfert) sans être en mesure de savoir si des paquets ont été perdus et à quelmoment.
- Technologie émergente et constante évolution des normes.
- Dépendance de l'infrastructure technologique et support administratif exigeant.
- Attaque de virus et vol.

IV.3.1.2. Solutions adaptées à la téléphonie sur IP :

- **Cisco Call Manager Express (CCME)**

Le Cisco Call Manager est un logiciel de traitement d'appels qui ajoute des fonctions de téléphonie aux réseaux locaux d'entreprise et aux périphériques réseau tels que les téléphones IP, les passerelles voix sur IP (VoIP) et les applications multimédia. Grâce à l'interface de programmation d'applications (API) ouverte du Call manager, les services de voix et de données tels que ceux proposés par la messagerie unifiée, les conférences multimédia, les centres de contact de collaboration et les répondeurs vocaux interactifs, peuvent enfin interagir avec les solutions de téléphonie sur IP.

On peut gérer environ 7500 téléphones IP par serveur Call Manager.

Le Call Manager peut opérer dans une architecture centralisée ou distribuée. L'architecture distribuée est réalisée par une construction d'une grappe (cluster) afin d'assurer la disponibilité duCall Manager et d'éviter sa surcharge pour éviter le blocage partiel ou total du réseau téléphoniquede l'entreprise. Le modèle en grappe permet une évolution de 1 à 30.000 Téléphones IP pour unegrappe.

Avant de nous plonger dans CME initialisation et configuration, nous avons besoin d'introduire quelques concepts et de se familiariser avec eux. Comprendre comment les fonctions de base du CallManager Express évoluent est indispensable pour la bonne configuration et le fonctionnement du système.

Comme mentionné, le CME fonctionne sur le routeur Cisco et fournit ses services sur le réseau. Les téléphones connectés au réseau via un commutateur sont utilisés pour gérer les appels entrants et sortants.

Une fois sous tension, les téléphones IP va démarrer et enregistrer avec Cisco CallManager Express. S'il est configuré, le CallManager Express fournira une extension pour chaque téléphone IP et alors est en mesure de mettre en place ou de couper les appels vers ou depuis les téléphones IP. Les téléphones IP et routeur CallManager Express utilisent un protocole propriétaire appelé Skinny Client Control Protocol (SCCP) pour communiquer. Ci-dessous est un schéma illustrant peu près ce qui se passe lorsque le téléphone compose un autre IP de téléphonie IP, tous deux connectés au même CallManager Express.

Quand un appel est placé entre deux téléphones IP sous le contrôle du CallManager Express, le protocole SCCP est utilisé pour mettre en place l'appel. SCCP est aussi communément connu comme le Protocol SKINNY. Le protocole SCCP est pas utilisé entre deux téléphones IP, mais seulement entre le téléphone IP et le système Cisco CME.

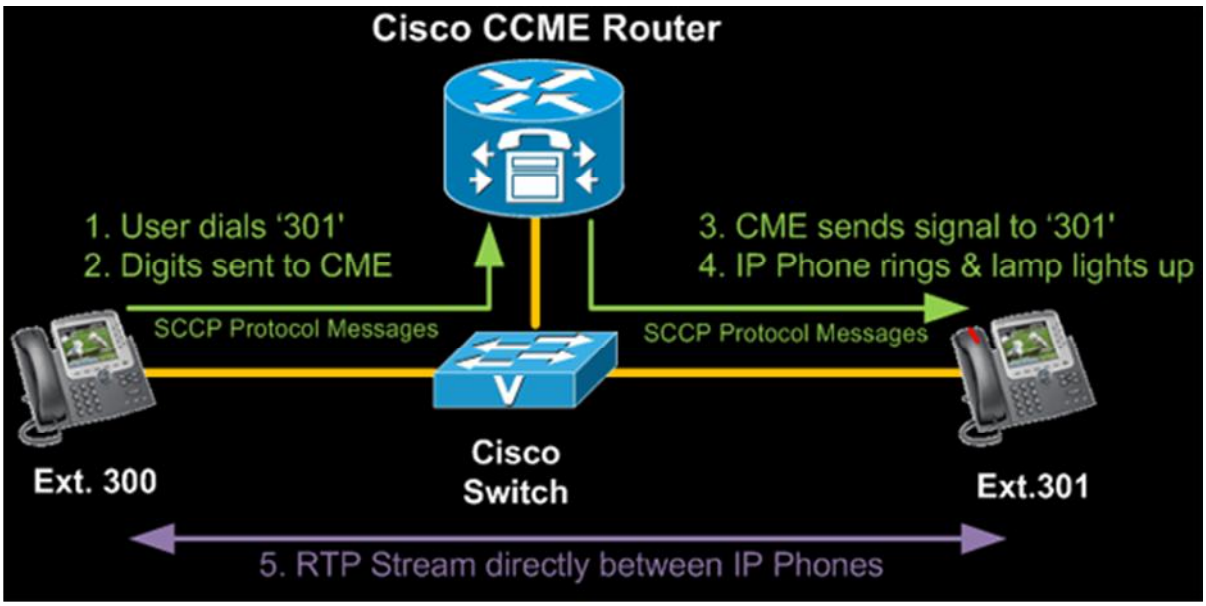


Figure IV.11 : Exemple d'architecture exploitant le CCME

Une fois que l'appel est mis en place, le protocole de transport en temps réel (RTP) sera utilisé pour transporter le flux audio. RTP est utilisé pour transporter la voix à l'intérieur de paquets IP.

RTP est un protocole commun qui est utilisé pour transporter le trafic sensible au temps comme la voix et la vidéo en temps réel. RTP est réalisée à l'intérieur d'un segment UDP, qui est ensuite transporté à l'intérieur d'un paquet IP.

Lorsque la session téléphonique entre les deux téléphones IP se termine et ils raccrocher, un signal sera envoyé à partir de chaque téléphone IP à CME pour informer le serveur de leur nouveau statut.

- **La configuration de call manager express :**

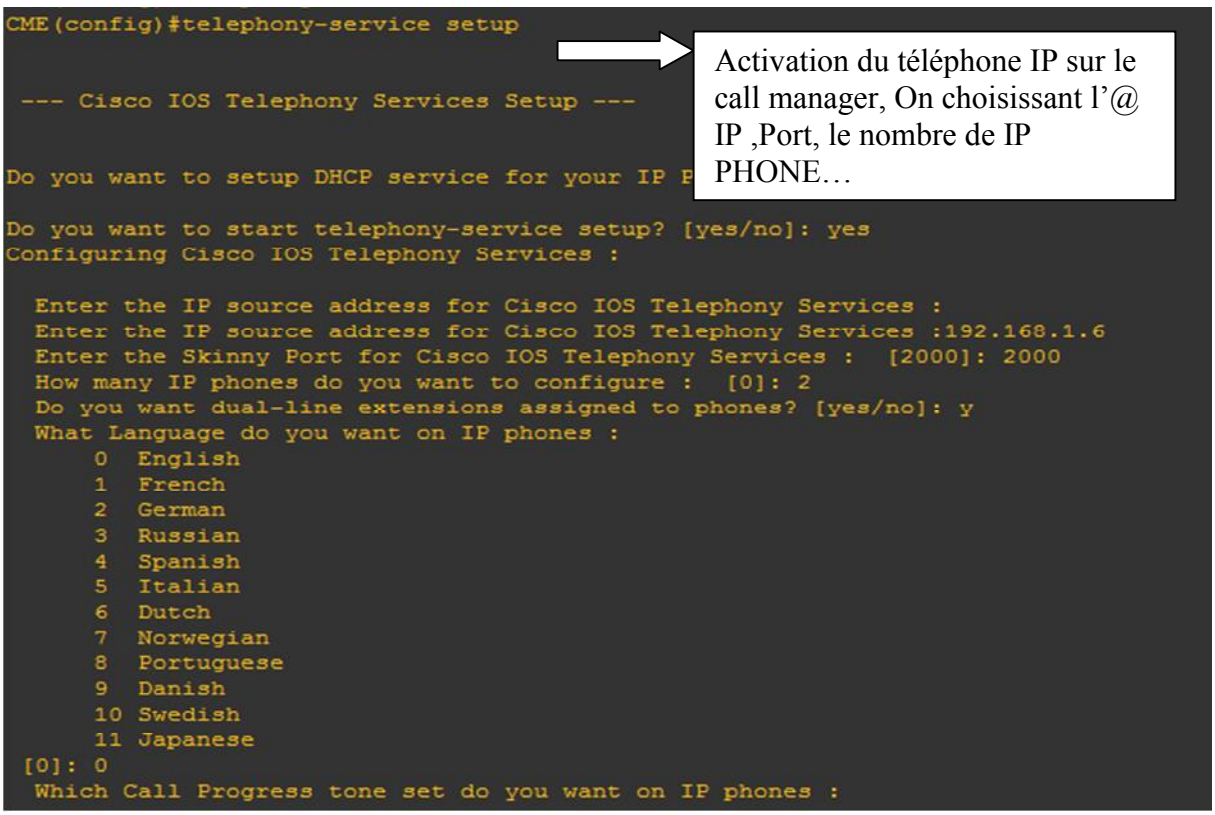


Figure IV.12 : Configuration de call manager express

Pour notre maquette nous avons installé IP Communicator sur notre machine pour simuler le trafic voix.

- **IP Communicator:**

L'IP Communicator est une application basée sur Windows et qui offre un support de téléphonie sur un ordinateur individuel. Cette application dote les ordinateurs des fonctions de téléphonie IP, en fournissant des appels de haute qualité de voix n'importe où lesutilisateurs peuvent accéder au réseau de l'entreprise.

La figure représente l'interface de l'IP Communicator Cisco que nous avons utilisé :

FigureIV.13 : IP Comminicator

IV.3.2.Trafic FTP :

IV.3.2.1. Définition de FTP:

FTP veut dire “File Transfert Protocol” ou Protocole de transfert de Fichier.

C’est donc un langage qui va permettre l’échange de fichiers entre 2 ordinateurs, et plus exactement entre un serveur et un client.

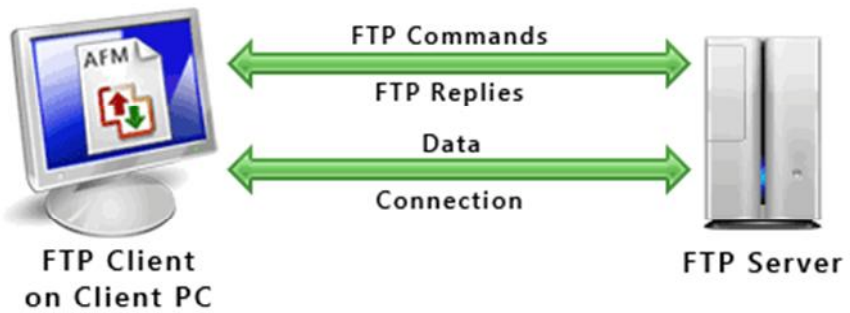
On parle alors de :

- serveur FTP
- client FTP

Je vais commencer par vous expliquer le fonctionnement d’un serveur FTP et d’un client FTP, puis plus loin nous regarderons dans quels cas, cela est intéressant.

IV.3.2.2. Détail de fonctionnement du FTP:

Comme je vous le disais au dessus, il y a 2 intervenants dans un échange FTP : le serveur et le client.



FigureIV.14 : Fonctionnement du FTP

1) le serveur FTP

Le serveur FTP est un logiciel qui va répondre aux demandes des clients. Lorsque le serveur reçoit une demande, il vérifie les droits et si le client à les droits suffisants, il répond à cette demande sinon la demande est rejetée.

Le serveur FTP passe son temps à attendre. Si les demandes ne sont pas nombreuses, les ressources utilisées par le serveur FTP sont quasi-nulles.

Quelques logiciels serveur FTP :

- VsFTPd (Linux)
- FilleZilla Server (Windows)
- WS_FTP server (Windows)
- ProFTPd (Linux)

2)le client FTP

C'est lui qui va être à l'initiative de toutes les transactions.

Il se connecte au serveur FTP, effectue les commandes (récupération ou dépôt de fichiers) puis se déconnecte. Toutes les commandes envoyées et toutes les réponses seront en mode texte. (Cela veut dire qu'un humain peut facilement saisir les commandes et lire les réponses).

Le protocole FTP n'est pas sécurisé : les mots de passe sont envoyés sans cryptage entre le client FTP et le serveur FTP. *(Le protocole FTPS avec S pour "secure" permet de crypter les données)*.

Quelques logiciels client FTP :

- FilleZilla client (Windows, Linux, IOs)
- Cute FTP Home (payant) (Windows, IOs)
- SmartFTP (payant)

3. Utilité de FTP :

Autrefois, il était incontournable d'utiliser FTP pour télécharger des fichiers. Maintenant, avec des connexions plus performantes, la plupart des téléchargements s'effectuent avec le navigateur web, en cliquant sur les liens proposés et les téléchargements démarrent directement. Pourtant dans certains cas encore, il est nécessaire d'utiliser FTP pour télécharger des fichiers.

Autant il est facile de télécharger des fichiers en surfant sur Internet, autant il serait difficile de mettre en ligne des fichiers sans le protocole FTP.

En effet, avec ce protocole, on va pouvoir se connecter aux différents serveurs et pouvoir y copier des fichiers (dans un sens ou dans un autre). Il est ainsi possible de sauvegarder ou d'envoyer des fichiers sur des serveurs distants sans passer par le web.

Quand le client envoie un fichier vers le serveur : on parle de "upload", quand le client télécharge un fichier : on parle de "download".

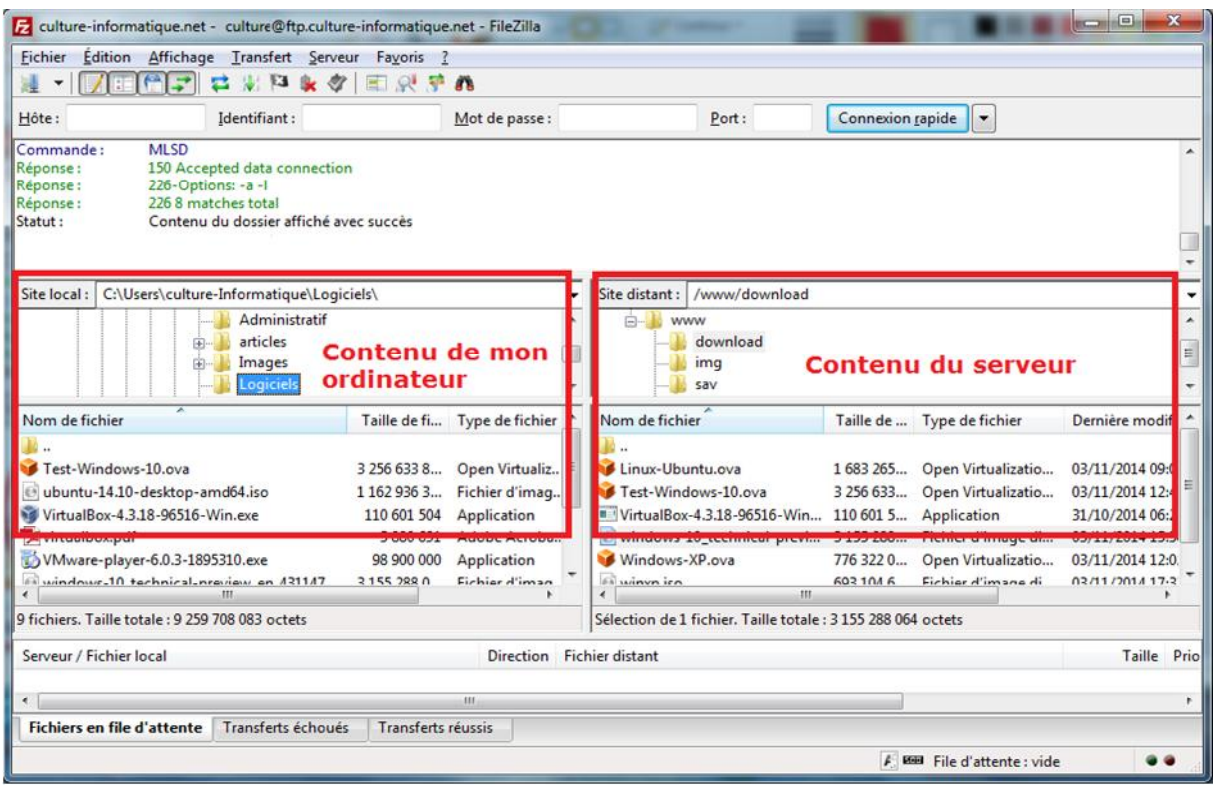


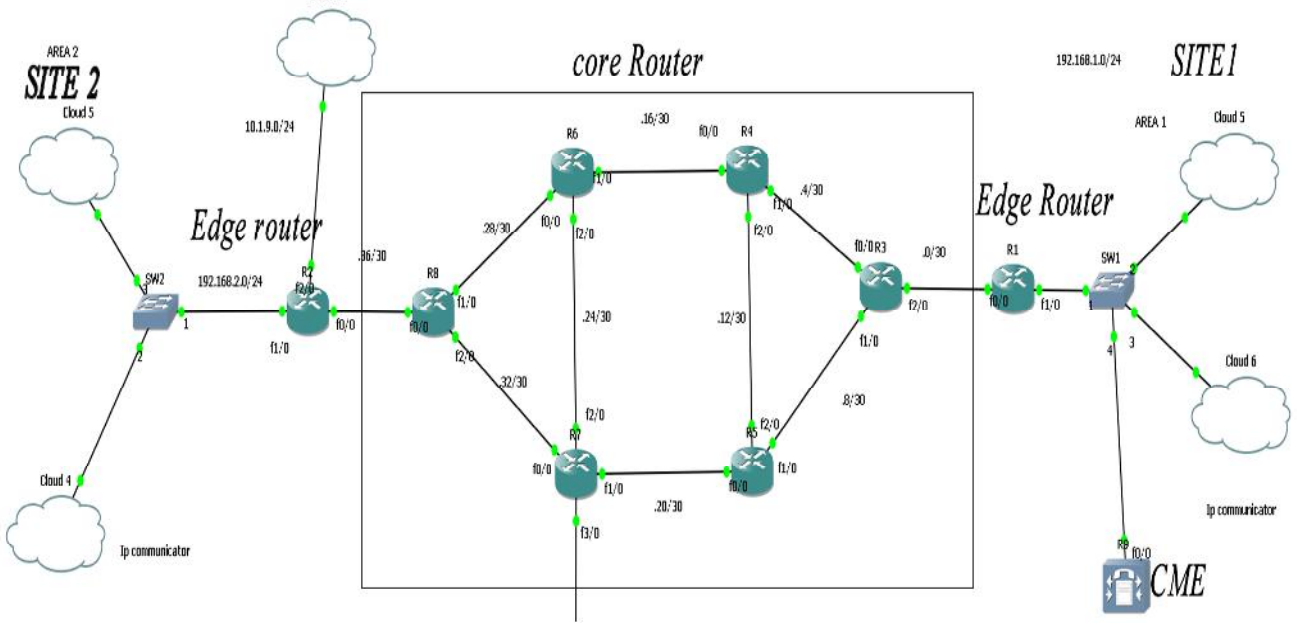
Figure IV.15: Téléchargement client/serveur

IV.3.3. Le World Wide Web (*WWW*):

Le *WWW* qui signifie "la toile d'araignée planétaire" est un système d'information graphique basé sur des liens hypertextes permettant de naviguer d'un site à un autre, sur Internet. *WWW* intègre pratiquement l'ensemble des services présents sur les réseaux. Il a tellement simplifié le travail sur Internet, que même les utilisateurs n'ayant aucune expérience informatique apprennent immédiatement à se servir de son interface graphique. Le système client de *WWW* sur l'ordinateur local (on l'appelle généralement *Web Browser* ou "navigateur") s'adresse à un serveur *WWW* du réseau.

Pour accéder au *Web*, il est nécessaire de disposer d'un logiciel appelé navigateur *Web*. L'accès à un document est conditionné par la connaissance de sa localisation qui est exprimée sous forme *d'URL*. Les clients et les serveurs dialoguent sur le *Web* en utilisant le protocole *HTTP*.

IV.4.Présentation du réseau existant :



FigureIV.16 : présentation du réseau existant

La figure nous montre que le réseau existant contient :

- ✓ **Deux sites différents :**

Site 1 :
Un Switch
2 nuage dont le premier on a installé Windows 7 et le deuxième server 2012
Call Manager.
Site 2 :
Un Switch
2 nuages dont le premier on a installé Windows 7 et le deuxième server 2012

- ✓ **Cœur réseau :**

8 routeur Cisco C3600 (R1 ,… ,R8)

Le routeur R2 est connecté au réseau d'entreprise (Ooredoo) avec une interface loopback pour accéder au service Netflow qu'on a présenté précédemment et une sortie vers Internet a fin de pouvoir simuler le trafic web (http,https…)

- ✓ **Configuration du protocole de routage OSPF pour tous les routeurs :**

On va montrer un exemple de la configuration basique du routeur R1 qui est connecté avec les trois zone area 0 , area 1 et area 2

```
R1# configuration terminal
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.1.1  255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#ip address 172.18.5.1  255.255.255.252
R1(config-if)#no shutdown
R1(config)#router ospf  10
R1(config-router)#network 172.18.5.0  0.0.0.3  area 0
R1(config-router)#network  192.168.1.0  0.0.0.255  area 1
```

Une fois que le protocole de routage mise en œuvre nous allons connecter notre réseau avec les machines virtuelles on choisissant le nom de la carte réseau

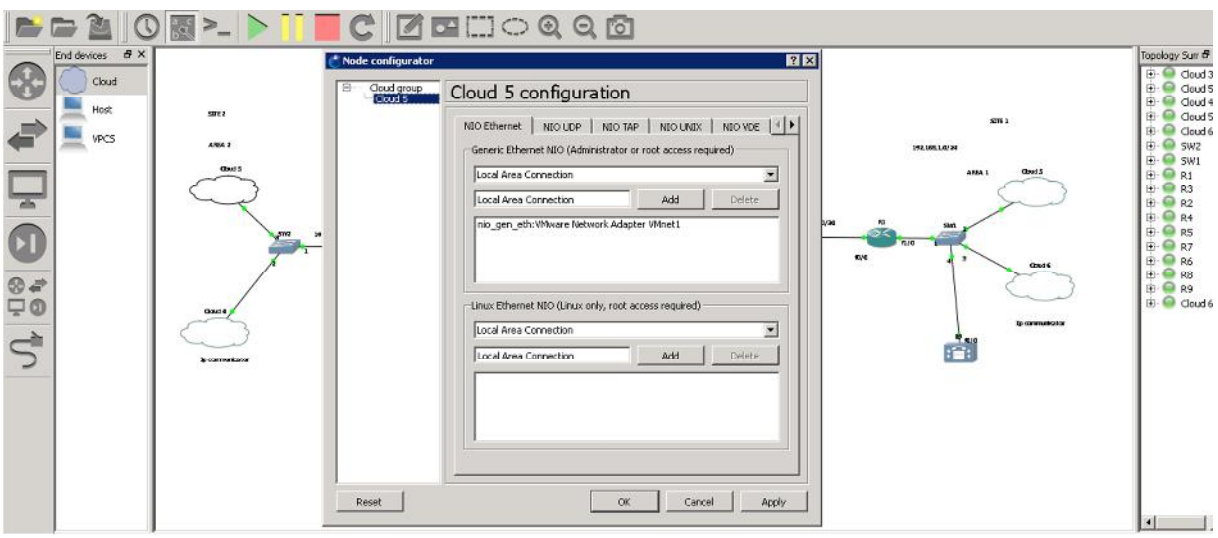


Figure IV.17: Connexion réseau et machines virtuelles

Puis on va configurer les paramètres de la carte réseau (window 7) :

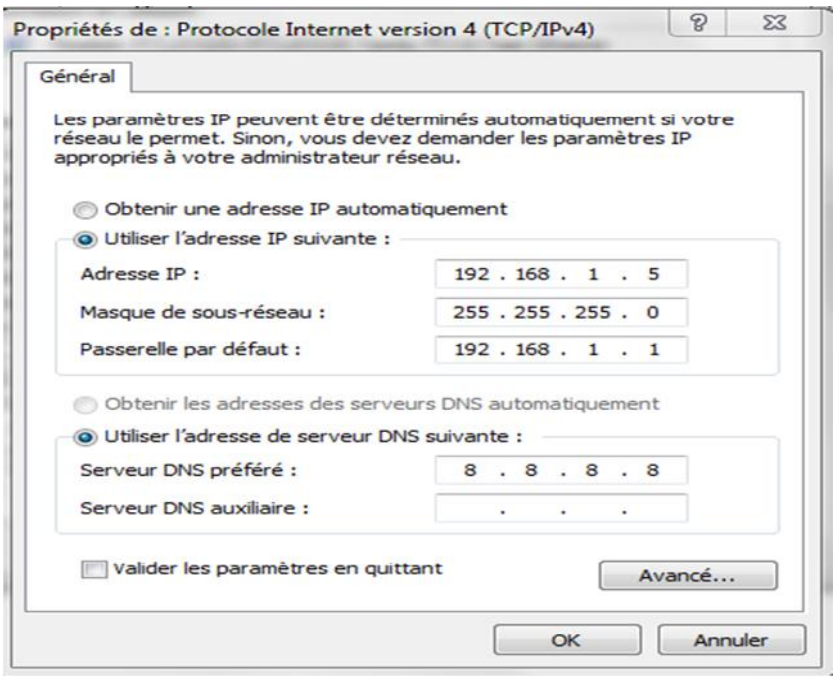


Figure IV.18: Configuration paramètre de la carte réseau

Une fois que tous les nœuds sont connectés entre eux on va commencer par simuler le trafic voix, car la mise en œuvre de la QoS est un préalable indispensable à l'intégration des flux voix sur les réseaux informatiques puis le trafic FTP-data et le trafic web (http).

Pour cella, certains constructeurs de routeurs ont développé un processus de classification et de reconnaissance d'applications sur leurs équipements. Ainsi la société Cisco intègre une telle fonction (**NBAR** network-based application recognition).

IV.4.Présentation et Activation du protocole NBAR dans l'interface du routeur :

La configuration Networked-Based Application Recognition (NBAR) , pour découvrir le trafic pour tous les protocoles connus de NBAR sur une interface particulière, on utilise IP nbar protocole Discovery pour la configuration d'interface.

Router# **configure terminal**

Router(config)# **interfacefa0/0**

Router(config-if)# **ip nbar protocol-discovery**

Router(config-if)# **end**

L'exemple suivant affiche la sortie du show pour les cinq protocoles les plus actifs sur une interface Ethernet:

Router# **show ip nbar protocol-discovery top-n 5**

```
Ethernet0/0 Input                    Output
  Protocol                  Packet Count             Packet Count
                            Byte Count               Byte Count
                            30sec Bit Rate (bps)     30sec Bit Rate (bps)
                            30sec Max Bit Rate (bps) 30sec Max Bit Rate (bps)
--------------------------- ------------------------ ------------------------
rtp                       3272685                  3272685
 242050604                 242050604
                             768000                   768000
                             2002000                  2002000
ftp                       482183                   482183
                             37606237                 37606237
                             121000                   121000
                             312000                   312000
http                      144709                   144709
                             32351383                 32351383
                             105000                   105000
                             269000                   269000
netbios                   96606                    96606
                             10627650                 10627650
                             36000                    36000
                             88000                    88000
   Total                     6298724                  6298724
989303872                 989303872
                             4213000                  4213000
                             8177000                  8177000
```

On va donnée un exemple de la configuration du routeur R2 :

interface FastEthernet0/0

description vers_site1

ip address 172.18.5.38 255.255.255.252

ip flow ingress

ip flow egress

ip nbar protocol-discovery ⟶ **activation du protocol NBAR**

ip nat inside

ip virtual-reassembly

ip route-cache flow

interface FastEthernet1/0

description vers_site2

ip address 192.168.2.1 255.255.255.0

ip flow ingress

ip flow egress

ipnbar protocol-discovery

ipnat inside

ip virtual-reassembly

load-interval 60

interface FastEthernet2/0

descriptionvers_internet

ip address 10.1.9.148 255.255.255.0

ip nbar protocol-discovery

ip nat outside

ip virtual-reassembly

load-interval 60

router ospf 10

redistribute static subnets

network 172.18.5.36 0.0.0.3 area 2

network 192.168.2.0 0.0.0.255 area 2

default-information originate always

} **route du protocol ospf**

ip flow-export source FastEthernet0/0 — **activation du protocol flow et Spécifie**

ip flow-export version 5 — **l'adresse à laquelle le routeur va envoyer les données SNMP**

ip flow-export destination 10.1.9.242 9996

ipforward-protocolnd

ip route 0.0.0.0 0.0.0.0 10.1.9.1 ← **la route par default**

ipnat inside source list NAT interface FastEthernet2/0 overload

ip access-list extended NAT

denyip any 10.1.9.0 0.0.0.255

permitip any any

snmp-server community spIrIth0n RW — **Activation du protocol SNMP**

snmp-server host 10.1.9.242 version 2c spIrIth0n

no cdp log mismatch duplex

ntp clock-period 17180021 — **Connexion au server pour la synchronisation d'heure des routeurs**

ntp server 10.1.9.11

ntp server 10.1.9.10

IV.5. Approche proposée pour assurer la QoS :

Nous allons nous intéresser maintenant à la définition et au comportement des protocoles faisant appel à IP, dans le cas de la mise en œuvre de la QOS.

Tout d'abord, il convient de remarquer que le protocole TCP n'est pas adapté aux applications multimédias, donc font appel au protocole UDP, beaucoup moins contraignant.Il a toutefois été nécessaire de développer des protocoles complémentaires pour tenir compte des besoins des applications multimédias.Nous avons déjà évoqué le protocole de signalisation RSVP, permettant aux applications d'indiquer au réseau leurs besoins en QOS.

IV.5.1. L'implémentation d'un scenario :

Pour l'implémentation, trois types de flux seront utilisés dans le scenario :
Un flux qui modélise le trafic voix (flux plus prioritaire).
Un flux qui modélise le trafic web (flux moins prioritaire).
Un flux qui modélise le trafic ftp-data (flux bas priorité).

- **La liste des différents protocoles pour simuler notre trafic :**

- **SCCP (Skinny Client Control Protocol)**
- **RTP(Real-time Transport Protocol)**
- **FTP (file tranfert protocol)**
- **HTTP(hyper text transfer protocol)**

Il s'agit essentiellement des applications actuelles, et notamment des applications de gestion critique de l'entreprise. Les technologies de QoS se référant à la priorité(Ethernet 802.1 p, DiffServ et, d'une certaine façon, les réseaux MPLS) sont donc bien adaptées à ces besoins.

Dans l'architecture DiffServ, le traitement différencié des paquets s'appuie sur trois opérations fondamentales. La classification des flux en classes de service, l'introduction de priorités au sein des classes et la gestion du trafic dans une classe donné.

Nous prenons comme exemple la mise en œuvre de l'interconnexion de deux réseaux locaux, fondés sur Ethernet, au travers d'un réseau Diffserv.

Nous allons examiner comment sont alloués les services on donnant un exemple de la configuration du routeur R1(routeur de bordure)

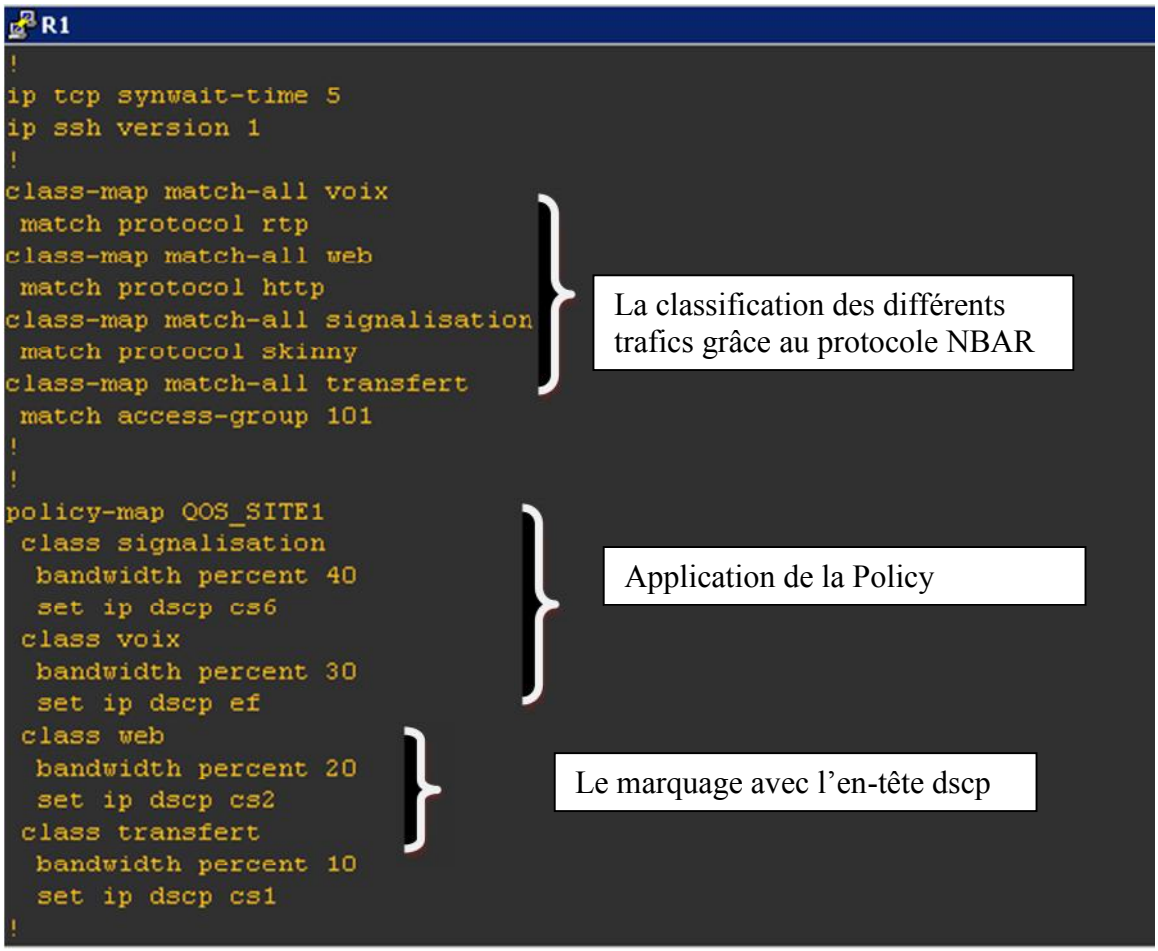


Figure IV.19 : la mise en œuvre de la classification, marquage et policy.

Le routeur R1 effectue une classification multi champs des paquets reçu du réseau Ethernet, en fonction du numéro de port TCP, le routeur R1 place les champs DSCP dans l'en-tête des paquets IP reçu

Conclusion :

Pour assurer la qualité de service QoS pour le réseau IP l'approche de DeffServ est mise en service pour garantir et assurer les caractéristiques de la qualité de service souhaité par les utilisateurs

La configuration des routeurs de bordure et cœur de l'architecture Deffserv est un impact essentiel pour assurer le bon déroulement de bout en bout.

Comme on la vue à l'exemple d'implémentation d'un scenario de DeffServ en termes de classification, marquage et la gestion de l'ordonnancement de ces agrégats.

Conclusion générale

Conclusion générale

En l'occurrence, la conclusion n'est pas aisée dans la mesure où la QoS est un sujet qui est loin d'être clos. De nombreux travaux de normalisation sont encore en cours. En outre, l'abondance des mécanismes décrits dans notre mémoire peut laisser perplexe. Certes, l'aspect best effort des technologies IP, et notamment de l'internet, a montré ses limites face aux nouveaux besoins.

Il est évident que les technologies de QoS se développerons encore plus rapidement sur les réseaux, s'il existe davantage d'applications pour en tirer parti. De même, de nouvelle application ne seront développées qu'à condition que les mécanismes de QoS soient disponibles.

Ce projet nous a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il nous a initiés au monde de la recherche sur les réseaux surtout en ce qui concerne la qualité de service ; Ainsi les différents modes de communication, leurs applications, ainsi que les protocoles qui les gèrent. Grâce notre modeste travail, nous avons eu l'occasion de voir beaucoup de choses de plus prés et d'enrichir nos connaissances ; nous avons aussi eu la chance de mettre nos capacités en valeur et de faire face aux situations les plus critiques et aux obstacles et apprendre comment procéder pour s'en sortir.

Références Bibliographiques

Bibliographie

Ouvrages :

 **Les réseaux [PUJ – 2003]**

Guy PUJOLLE, EYROLES Edition 2003.

 **Télécoms 1 [CLA – 2001]**

Claude SERVIN, DUNOD 2ème Edition Octobre 2001.

 **Qualité de service sur IP[CLA – 2001]**

Jean-louis Mélin, Eyrolles, Edition Septembre 2001.

 **Télécoms et réseaux [MAX – 1997]**

Maxime MAIMAN, Editions InterEdition, octobre 1997.

 **Teletrafic [ROU – 1970]**

J. M. ROUAULT, EYROLLES Editeur – Paris 1970.

Webgraphie

[Qualitty of Service forum]
www.qosforum.com

[groupe de travail de QoS de Internet]
www.internet2.edu/qos
www.cisco.fr/go/documentation/

[présentation de quelque scénarios GNS3]
http://gns3vault.com/labs/quality-of-service/
http://docs.oracle.com/cd/E19957-01/820-2982/ipqos-reference-11/index.html
http://www.cisco.com/cisco/web/support/CA/fr/109/1092/1092197_dscpvalues.pdf

[introduction to Qos mpls]
http://www.memoireonline.com/09/13/7405/m_Conception-et-deploiement-de-la-technologie-MPLS-dans-un-reseau-metropolitain17.html

[la politique d'ordonnancement]
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/15-s/qos-conmgt-15-s-book/qos-conmgt-cfg-wfq.html
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/15-s/qos-conmgt-15-s-book/qos-conmgt-cfg-pq.html

Annexe

Matériel Cisco

V.1.Introduction

Matériels et logiciels présentent de manière détaillée le matériel informatique et les différents systèmes d'exploitation. L'objectif de ce chapitre est d'apprendre les différentes fonctionnalités des composants matériels et logiciels et la méthode de configuration des différentes matérielles Cisco (Switch, routeur…).

V.2. Les équipements Cisco

Les réseaux hétérogènes utilisant le matériel Cisco formant Interne sont reliés entre eux grâce à des dispositifs d'interconnexion (Switch, routeur, firewall) qui assurent le transfert des données.

V.2.1. les Switch Cisco (CATALYST Cisco)

Les commutateurs intelligents Cisco Catalyst, nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité FastEthernet et GigabitEthernet optimisent les services de LAN sur les réseaux d'entreprise.

Et ces caractéristiques sont :

- Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de Contrôle d'accès (ACL) élaborées et une sécurité optimisée
- Sécurité du réseau assurée par une série de méthodes d'authentification, destechnologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.

Figure III.2 les Switch cisco

V.2.2. les Router Cisco

La fonction principale d'un routeur Cisco consiste à diriger les paquets destinés à des réseaux locaux et distants en :

- Déterminant le meilleur chemin pour l'envoi des paquets,
- Transférant les paquets vers leur destination.

Figure : Vue de l'arrière du routeur

V.3.Caractéristiques matérielles

Bien qu'il existe plusieurs types et modèles des équipements Cisco, chacun comporte, à la base, les mêmes composants matériels, et pour cela dans cette partie on présente sur les caractéristiques matériel d'un routeur et presque pareil pour le firewall et Switch.

La figure présente l'intérieur d'un routeur 1841. Pour voir les composants internes du routeur.

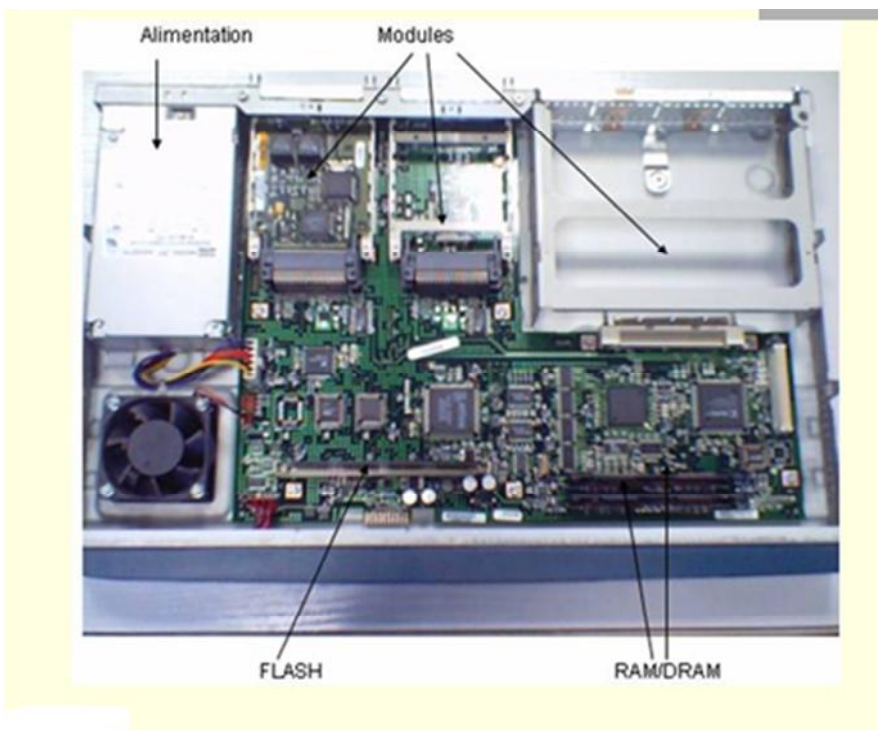


Figure 5 : Vue de l'intérieur du routeur

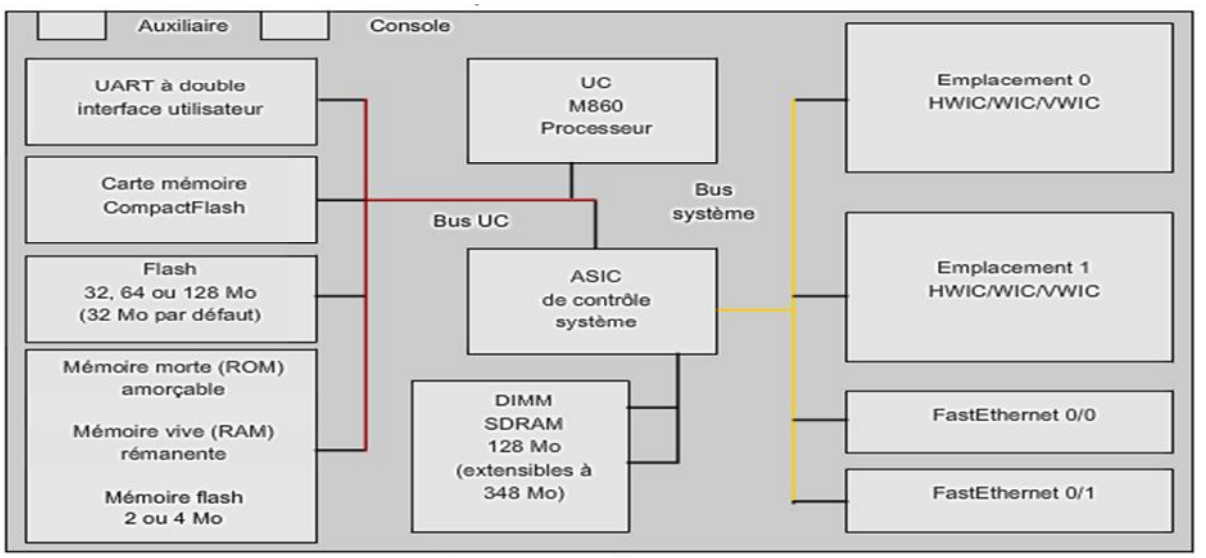


Figure 6 : composant matériel d'un routeur Cisco

Comme un PC, un routeur comprend également les éléments suivants :

- Unité centrale (UC)
- Mémoire vive (RAM)
- Mémoire morte (ROM)

V.3.1.Microprocesseur (UC)

Le Microprocesseur (CPU) L'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation du routeur.

V.3.2.Mémoire vive(RAM)

La mémoire vive stocke les instructions et données requises pour exécution par l'UC. La mémoire vive est utilisée pour enregistrer ces composants :

- **Système d'exploitation** : le système IOS (Internetwork Operating System) de Cisco est copié dans la mémoire vive pendant l'amorçage.
- **Fichier de configuration en cours** : il s'agit du fichier de configuration qui enregistre les commandes de configuration actuellement utilisées par l'IOS du routeur. À de rares exceptions près, toutes les commandes configurées sur le routeur sont enregistrées dans le fichier de configuration en cours, appelé running-config.
- **Table de routage IP** : ce fichier stocke des informations sur les réseaux directement connectés et les réseaux distants. Il permet de déterminer le meilleur chemin pour le transfert du paquet.
- **Cache ARP** : ce cache contient les mappages d'adresses IPv4 et MAC, de manière similaire au cache ARP d'un PC. Le cache ARP est utilisé sur les routeurs dotés d'interfaces de réseau local, telles que les interfaces Ethernet.

Mémoire tampon de paquets : les paquets sont stockés temporairement dans une mémoire tampon lors de leur réception sur une interface ou avant de quitter une interface.

La mémoire vive est une mémoire volatile : elle perd donc son contenu lorsque le routeur est mis hors tension ou redémarré. Cependant, le routeur contient également des zones de stockage permanent, comme la mémoire morte, flash et NVRAM.

V.3.2.Mémoire morte(ROM)

La mémoire morte est une forme de stockage permanent. Les périphériques Cisco utilisent la mémoire morte pour enregistrer les éléments suivants :

- Instructions d'amorçage
- Logiciel de diagnostic de base
- Version réduite d'IOS

La mémoire morte utilise un progiciel, qui est un logiciel incorporé dans le circuit intégré. Le progiciel inclut les logiciels qui n'ont habituellement pas besoin d'être modifiés ou mis à niveau, les instructions d'amorçage par exemple. La mémoire morte ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

- **Mémoire flash**

La mémoire flash est une mémoire non volatile pouvant être stockée et effacée électriquement. Elle sert de stockage permanent pour le système d'exploitation, Cisco IOS. Sur la plupart des modèles de routeurs Cisco, l'IOS est stocké de manière permanente dans la mémoire flash et copié dans la mémoire vive lors du processus d'amorçage, où il est ensuite exécuté par le processeur. La mémoire flash ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

- **Mémoire vive non volatile**

La mémoire vive non volatile ne perd pas les informations qu'elle contient lorsque le système est mis hors tension. Elle s'oppose aux formes les plus courantes de mémoire vive, telles que la mémoire vive dynamique (DRAM), qui nécessite une alimentation continue pour conserver les informations. La mémoire vive non volatile est utilisée par Cisco IOS comme stockage permanent pour le fichier de configuration initiale (startup-config). Toutes les modifications de configuration sont enregistrées dans le fichier de configuration en cours (running-config) dans la mémoire vive, et sont, à de rares exceptions près, immédiatement implémentées par l'IOS. Pour enregistrer ces modifications, au cas où le routeur serait redémarré ou mis hors tension, la configuration en cours doit être copiée dans la mémoire vive non volatile, où elle est enregistrée en tant que fichier de configuration initiale. La mémoire vive non volatile conserve son contenu, même si le routeur se recharge ou s'il est mis hors tension.

V.4.Network Operating System

Le logiciel du système d'exploitation utilisé dans les routeurs Cisco est appelé Cisco Internetwork Operating System (IOS). Comme tout système d'exploitation d'ordinateur, Cisco IOS gère les ressources matérielles et logicielles du routeur, notamment l'allocation de mémoire, les processus, la sécurité et les systèmes de fichiers. Cisco IOS est un système d'exploitation multitâche intégré aux fonctions de routage, de commutation, d'interconnexion et de télécommunications.

V.5.Les indicateurs LED

Le panneau avant d'un équipement Cisco comporte différents voyants permettant de surveiller les activités et les performances du système. Le panneau avant du commutateur comporte les LED suivantes:

- LED système
- LED pour le mode des ports
- LED pour l'état des ports

La LED système indique si le système est bien alimenté et s'il fonctionne correctement.

La signification des LED correspondant à l'état des ports varie en fonction de la valeur courante du LED Mode.

LED Stat :

- désactivé : aucune liaison
- vert fixe : liaison opérationnelle
- vert clignotant : envoi ou reçoit des données
- alternance vert et orange : liaison défectueuse
- orange fixe : port désactivé par l'admin, SpanningTre...

V.6.Les modes configuration de matériel Cisco

- mode utilisateur, accès restreint avec un prompt en '>'
- mode enable ou privilégie, accès par la commande 'enable' avec un prompt en '#'
- mode de configuration, accessible à partir de enable par la commande 'configure', prompt en 'configure#'; le mode de configuration le plus utilisé est 'configure terminal', il existe aussi 'memory' et 'network'

V.6.1. les commandes utiliser pour la configuration d'un Switch et d'un router

Le tableau suivant représente les différentes commandes utilisé pour la configuration d'un Switch et d'un routeur Cisco.

Commandes	*Descriptions*
configure terminal ou conf t ou confterm	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
exit	Sort et remonte d'un cran dans la hiérarchie des menus
hostname ou host <hostname>	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet | fastethernet | Serial | loopback <interface>ouint e | fa | s | lo	Entre dans le mode de configuration de l'interface
ip address <address><mask>ouip add	Configure l'interface avec l'ip et le masque de réseau
bandwidth ou band	Indique une bande passante
encapsulation <encap> [<type]> ou encap	Fournit l'encapsulation de l'interface
no shutdown ou no shut	Active ou Désactive l'interface
Les commandes de sauvegarde :	
copy running-config startup-configou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
copy running-configtftpou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup-configtftpou	Sauvegarde la configuration situé en

copy star tftp	NVRAM vers un serveur TFTP
copy tftp startup-configou copy tftp star	Charge un fichier de configuration d'un serveur TFTP en NVRAM
copy tftp running-configou copy tftp run	Charge un fichier de configuration d'un serveur TFTP dans la configuration courante
Commandes	***Descriptions***
erase startup-config ou erase star	Efface la configuration de la NVRAM
Configuration d'une connexion en telnet:	
router# conf t	
router(config)# line console 0	
router(config)# login	
router(config)# passwordxyz	
Les commandes de configurations du routage :	
router <xxx> [<process-id>,<autonomous system>] rip,ospf,bgp,igrp,eigrp,is-is,...	Configure le protocole de routage d'un routeur
exemple de configuration du routage RIP:	
router# conf t	
router(config)# router rip	
router(config-router)# version 1-2	la version 2 apporte le routage CIDR et l'utilisation de VLSM, un nombre de sauts à 128
router(config-router)#network *networknumber*	
exemple de configuration du routage OSPF:	
router# conf t	
router(config)# router ospf 10	
router(config-router)# network network number	
exemple de configuration du routage IGRP:	
router# conf t	
router(config)# router igrpautonomoussystem	
router(config-router)# network *networknumber*	
exemple de configuration du routage EIGRP:	
router# conf t	
router(config)# router eigrpautonomous system	
router(config-router)# network *networknumber*	
exemple de configuration du routage BGP:	
router# conf t	
router(config)# router bgp*autonomous system*	
router(config-router)# network *networknumber* [mask *network-mask*] [route-map *route-map-name*]	

D'autres commandes de routage	
ip multicast-routing	Permet de faire du routage multicast
ip rsvp bandwidth [*interface-kbps*] [*singleflow-kbps*]	Active la réservation RSVP sur une interface
Les commandes sur un Switch :	
vlan database vlan 1 name <vlan name>	Accès à la database et écriture dans le fichier vlan.dat
Exemple de configuration d'un vlan :	
switch# vlan database switch(vlan)# vlan<number><name> switch(vlan)# exit switch(config)#interface fa<iface-number> switch(config)#interface range fa... switch(config-if)#switchport mode access	affectation sur un port affectation sur un ensemble de ports on passe le mode de configuration de l'interface
Commandes	***Descriptions***
switch(config-if)# switchport access vlan <number-name>	on active le vlan sur le ou les interfaces
Activation du trunking sur l'interface	Le truncking sert dans l'extention d'un domaine VLAN sur d'autre switch, pour se faire CISCO utilise le protocole VTP VLAN Trunking Protocol
switchporttrunkencap dot1q	Il y a 2 protocoles utilisés dans l'étiquetage: le protocole ISL (CISCO) et le protocole 802.1q (IEEE)
switchport mode trunk	On active le mode trunk sur le port du commutateur serveur et client qui font le trunk le reste des ports sont en mode access
vlan database vtpdomain<domain-name> vtp server	Création d'un serveur VTP
vlan database vtpdomain<domain-name> vtp client	Création d'un client VTP
ip default-gateway <ip-gateway>	On peut définir une passerelle par défaut pour communiquer entre VLAN, pour se faire on utilise un routeur
encapsulation ISL | dot1q <vlan-number>	en mode interface on peut spécifier le type d'encapsulation sur le routeur
D'autres commandes communes :	
reload	Redémarre l'équipement réseau
setup	Passe en mode de configuration assisté
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
Les commandes show :	
show interfaces oushint	Donne une description détaillé sur les interfaces

show running-configoush run	affiche la configuration courante
Commandes	***Descriptions***
show startup-configoush star	affiche la configuration en NVRAM
show ip route ouship route	affiche la table de routage
show ip<routing-protocol> [<options>]	affiche les informations sur le protocole de routage défini
show ipprotocols	affiche des informations sur les protocoles utilisés
show ?	donne toutes les commandes show disponibles

III.6.1. les commandes basiques pour la configuration d'un firewall

Pour une première configuration, il est conseillé de ne pas oublier certains points :

- ne pas répondre aux Ping sur l'interface externe.
- établir les routes par défaut
- configurer les interfaces
- établir les règles de redirection et de contrôle d'accès

Ensuite il faut tester la connectivité et si cela réussit, sauvegarder la configuration. Détaillons à présent les commandes qui seront utiles pour cette configuration.

- hostname {nom}
- Mode de configuration globale.
- Spécifie le nom d'hôte du pare-feu.
- Exemple : hostname SupinfoPix001

domain-name {nom}
- Mode de configuration globale.
- Spécifie le nom de domaine auquel appartient le pare-feu.
- Exemple : domain-namesupinfo.lan

enablepassword {mot de passe} [encrypted]
- Mode de configuration globale.
- Mot de passe du mode privilégié.
- Sans le paramètre [encrypted], le mot de passe est écrit en clair dans le fichier de configuration.
- Exemple : enablepasswordsupersecurepwdencrypted

clock set hh:mm:ss {mois jour | jour mois} année
- Configure l'horloge du pare-feu.
- clearclock
- Reconfigure l'horloge sur l'heure GMT (nécessaire dans le cas d'utilisation d'IPSec avec des certificats).

nameif {ethernet{n°} | gb-ethernet{n°}} {nom} security{level}
- Mode de configuration globale.
- Nomme l'interface et lui assigne son niveau de sécurité.
- Exemple : nameif ethernet0 outside security0
- Exemple 2 : nameif ethernet1 inside security100

-interface {ethernet{n°} | gb-ethernet{n°}} [10baset | 10full | 100basetx | 100full | 1000sxfull | 1000basesx | aui | auto | bnc] [shutdown]
- Mode de configuration globale.
- Configure la vitesse de l'interface spécifiée en argument et l'active.
- La vitesse est optionnelle.
shutdown : permet de désactiver l'interface (par défaut toutes les interfaces sont désactivées).
- Exemple : interface ethernet0 100full

ipaddress {nom_interface} {{ip} {masque} |{dhcp}}
- Mode de configuration globale.
- Configure l'adresse IP de l'interface.
- Exemple : ipaddressinside 10.0.0.2 255.0.0.0
- Exemple 2 : ipaddressoutsidedhcp

route {nom_interface} {ip} {masque} {ip_passerelle} [metric]
- Mode de configuration globale.
- Spécifie une route statique.
- Pour spécifier la route par défaut, il faut utiliser l'ip et le masque 0.0.0.0 ou 0.
- Exemple : route outside 0.0.0.0 0.0.0.0 82.226.244.238 1
- L'interface outside enverra tous les paquets sortant vers l'ip 82.226.244.238 (un routeur par exemple).
- La métrique correspond au nombre de sauts jusqu'à la passerelle, par défaut 1

[no] rip {nom_interface} {defautl|passive} [version [1|2]] [authentication [text|md5] key {key_id}] - Dés/Active la réception des mises à jour des tables de routages RIP - icmp {permit|deny} {ip_source} [masque] {nom_interface}
- Autorise ou refuse le requête ping sur l'interface spécifié.
- Exemple : icmpdenyanyany
- Cet exemple refuse toutes les requêtes icmp.
Show interface {ethernet{n°} | gb-ethernet{n°}}
- Affiche les informations détaillées de l'interface.
- show ip
- Affiche la configuration IP des interfaces.
Show nat
- Affiche la configuration NAT : les interfaces autorisées à initier des connexions vers des interfaces moins sécurisées.

Show global
- Affiche les adresses à utiliser pour les translations.
Show xlate
- Affiche la table des adresses translatées dynamiquement. - show route
- Affiche les routes configurées.

Show access-list
- Affiche les ACL.
Show running config
- Affiche le fichier de configuration actif.

writememory
- Copie la configuration courante dans la mémoire Flash.
- Cette configuration sera utilisée au prochain démarrage.

reload
- Redémarre le PIX.

V.7. Configurer le périphérique Cisco (Switch ou routeur ou un firewall) avec HyperTerminal

V.7.1.Configuration d'HyperTerminal

- **Exemple pour la configuration d'un Switch**

Tout d'abord, vous avez besoin d'un câble console (câble RJ-45 vers Série) reliant le port série de votre ordinateur à la prise RJ-45 marqué « console » sur votre Switch comme il est donnée par la figure suivante.

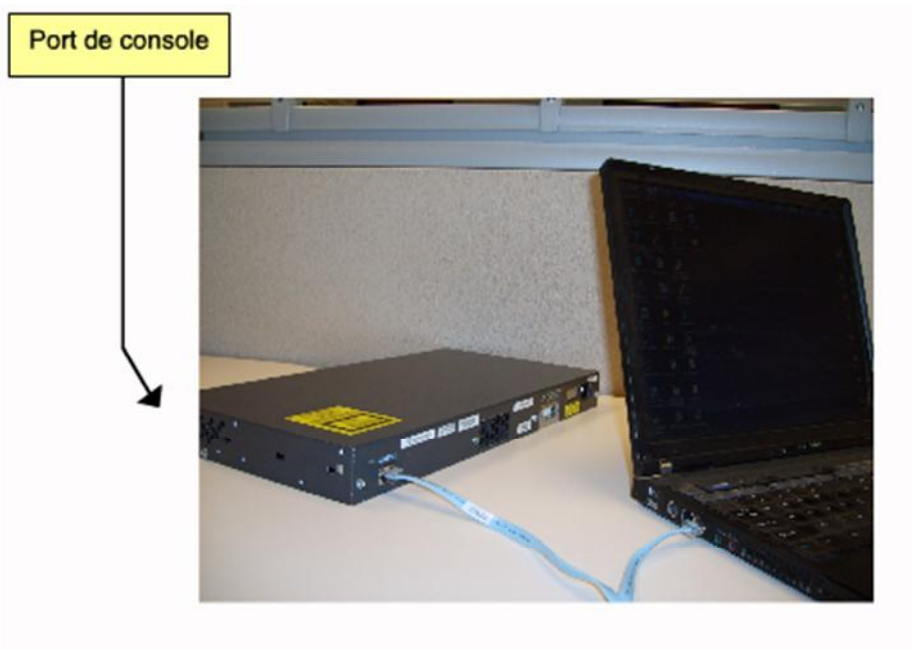
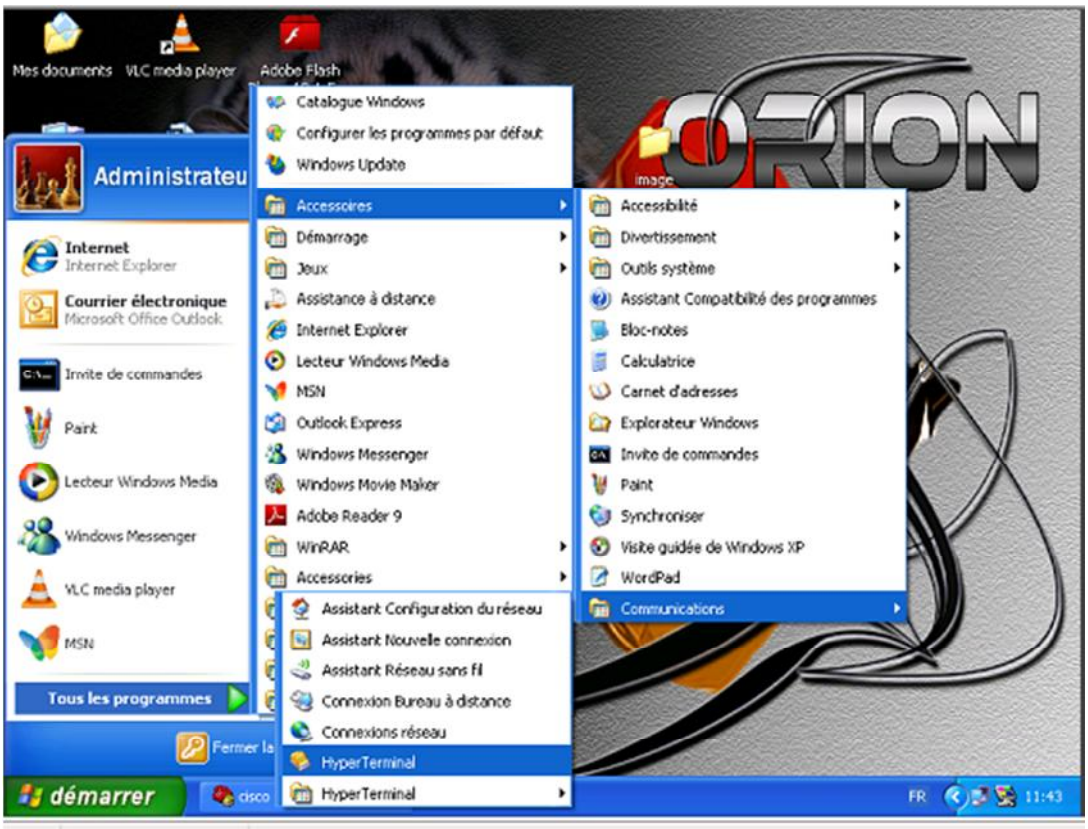


Figure 7 :L'interface de la console du Switch.

Ensuite, ouvrez Hyper-Terminal (Menu démarrer -> Tous les programmes -> accessoires -> communications ->Hyper-Terminal), puis entrez un nom pour votre nouvelle connexion ; sélectionnez le port série sur lequel est connecté le câble console et cliquez sur « paramètres par défaut » puis ok comme il est donnée par les figures (1), (2), (3), (4) et(5) successivement.



Figure(1)

Figure(2)

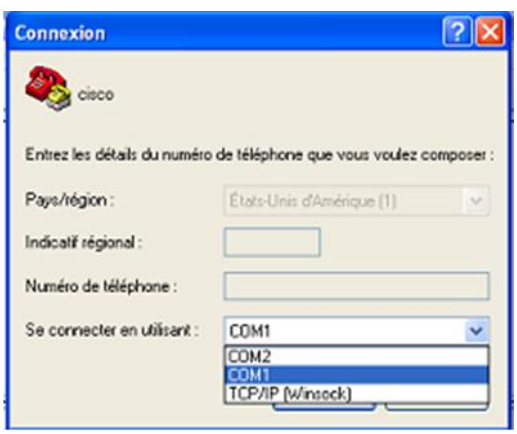
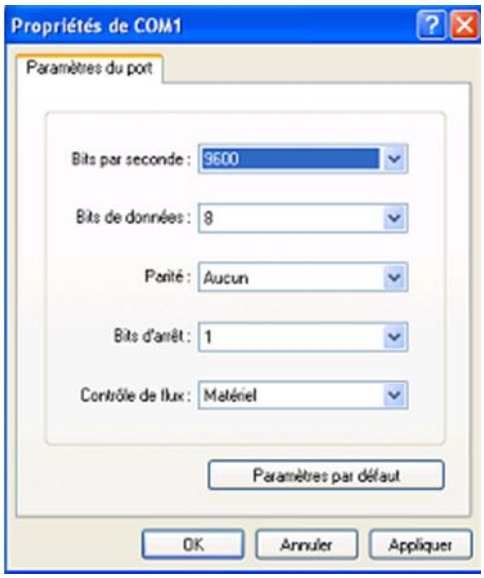
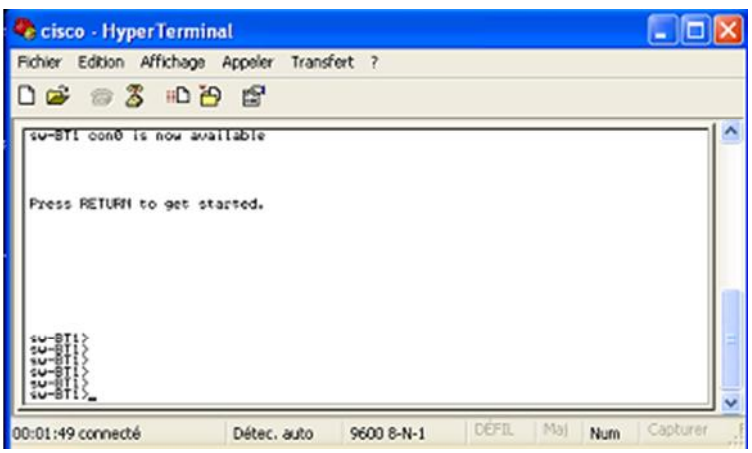


Figure (3)



Figure(4)



Figure(5)

Voilà, Nous somme connecté au Switch et à partir de maintenant nous pouvons le configurer.

Et pour la configuration d'un firewall on suit les même étapes de la configuration du Switch, mais pour la configuration d'un routeur lorsque vous terminez ces étapes, et S'il est allumé, faite un retour à la ligne, vous devriez voir apparaître une ligne vous demandant si vous voulez entrer dans outil de configuration initial, dans ce cas répondez « no » sinon, il vous affiche le nom du routeur suivi de ">" (ex: Routeur>).

S'il est allumé, faite un retour à la ligne, vous devriez voir apparaître une ligne vous demandant si vous voulez entrer dans outil de configuration initial, dans ce cas répondez « no » sinon, il vous affiche le nom du routeur suivi de ">" (ex: Routeur>) ; dans ce cas tapez "en" pour enable et entrez le mot de passe s'il y en a un. Cette fois "Routeur>" change en "Routeur#" et vous pouvez commencer à taper des commandes de configuration.

III.8. Résultat d'un Ping à partir d'une hôte

Pour voir les résultats de la commande Ping, commencer per ouvrir une fenêtre d'inviter de commande et à exécuter une commande semblable à celle reproduite ci-dessus .en spécifiant une adresse IP valide sur votre réseau comme il est donnée par la figure suivante :

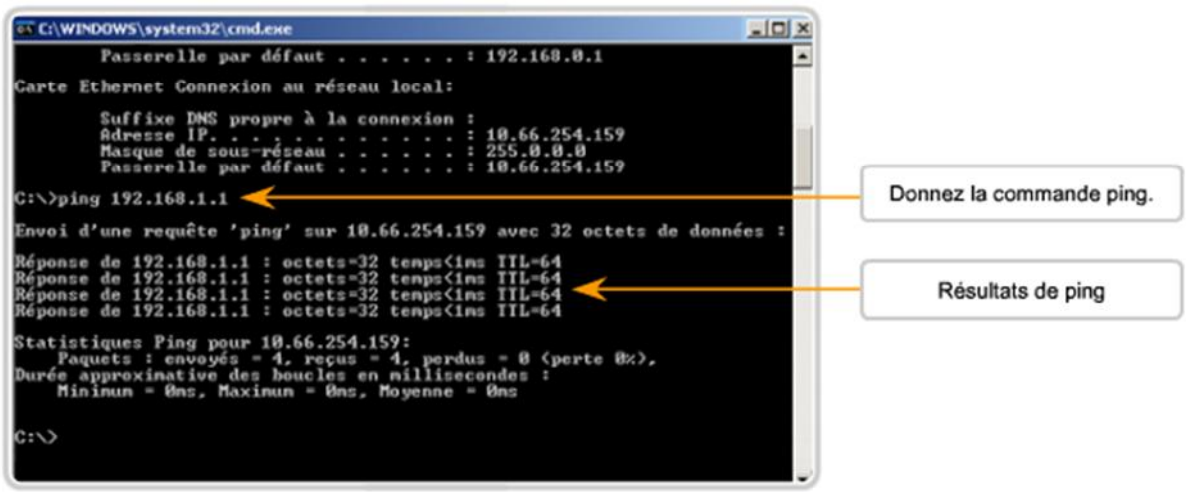


Figure 8: Résultat d'un Ping à partir d'une hôte