République Algérienne Démocratique et Populaire
Université Aboubakr Belkaid – Tlemcen
Faculté de Technologie
Département de Télécommunications

Mémoire de fin d'études

Pour l'obtention du diplôme de Master

En : *Réseaux et Télécommunications*

Thème

Implémentation de la qualité de service dans les réseaux IP

Réalisé par :

- TABET AOUL Abdelmalek
- SAHOULI Sofiane

Présenté devant le jury composé de

- HADJILA Mourad *(Président)*
- BOUABDALLAH Reda *(Encadrant)*
- BOUACHA Abdelhafid *(Examinateur)*

Année universitaire : 2018-2019

Remerciements

Nous tenons tout d'abord à remercier ALLAH le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce modeste travail.

Nous tenons à remercier notre encadreur Mr. BOUABDALLAH Reda pour son précieux conseil et son aide durant toute la période du travail.

Nos vifs remerciements vont également aux membres du jury Mr. HADJILA Mourad et Mr. BOUACHA Abdelhafid pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Nous souhaitons aussi remercier avec chaleur notre maître Mr. BACHIR BOUIADJRA Abderrazak pour ses conseils, soutiens et aides durant toute cette année universitaire.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicaces

Je dédie ce travail

À

Mes très chers parents,

Ce travail n'aura jamais pu voir le jour sans vos soutiens indéfectibles.

Aucun mot, aucune dédicace ne saurait exprimer mon respect et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien être.

Trouvez en ce travail le fruit de votre dévouement et l'expression de ma gratitude et mon profond amour.

À

Ma sœur et mes frères à qui je souhaite un avenir très brillant.

Que dieu vous protège et que la réussite soit toujours à ma portée pour que je puisse vous combler du bonheur

Sofiane

Dédicaces

C’est avec profonde gratitude et sincères mots,
Que je dédié ce modeste travail de fin d’étude à mes chers parents,
Mes premiers encadrants depuis ma naissance.
J’espère qu’un jour je peux leur rendre un peu de ce qu’ils ont fait
Pour moi.
Que dieu leur prête bonheur et longue vie.
Je dédié aussi ce travail à mes frères et sœurs, ma famille, mes amis,
À tous ceux qui j’ai chers.

Abdelmalek

Résumé

Avec l'évolution des tailles des entreprises, la croissance des systèmes d'information et la diversification des besoins des applications dans le domaine de transmission de données, la gestion des multiservices s'avère primordiale pour instaurer la notion de la Qualité de Service dans les réseaux. Cette solution de la QoS permet une utilisation optimale des équipements déployés ainsi qu'une bonne gestion des applications métiers.

Ce projet de fin d'étude consiste à optimiser les ressources réseaux de l'entité ICT-Towers par l'implémentation de la QoS avec des configurations des équipements Cisco. En premier lieu, notre travail consiste à étudier la qualité de service et l'infrastructure réseau existante au sein de ICT-Towers, et en deuxième lieu à présenter la démarche d'implémenter la QoS ainsi la supervision et le Monitoring du réseau.

Mots-clés : QoS, Intserv, Diffserv, RED, WRED, NBAR et NBAR2.

Abstract

With the evolution of the size of companies, the growth of information systems and the diversification of the needs of applications in the field of data transmission, the management of multiservice proves to be essential to establish the notion of the Quality of Service in the networks. This QoS solution allows for optimal use of deployed equipment as well as good business application management.

This end-of-study project consists in optimizing the ICT-Towers entity's network resources by implementing QoS with Cisco equipment configurations. First of all, our job is to study the quality of service and the existing network infrastructure within ICT-Towers, and secondly to present the approach to implement QoS as well as the supervision and monitoring of the network.

Key Words: QoS, Intserv, Diffserv, RED, WRED, NBAR et NBAR2.

ملخص

مع تطور حجم الشركات ونمو نظام المعلومات وتنويع احتياجات التطبيقات في مجال نقل البيانات ، أثبتت إدارة الخدمات المتعددة أنها ضرورية لتأسيس فكرة جودة الخدمة في شبكات الإتصالات و المعلومات . يتيح حل"جودة الخدمة" هذا الاستخدام الأمثل للمعدات المستعملة بالإضافة إلى الإدارة الجيدة لتطبيق الأعمال.

يقترح هذا المشروع حل لتحسين موارد شبكة تكنولوجيا المعلومات والاتصالات ICT-Towers من خلال تطبيق جودة الخدمة مع تكوينات معدات Cisco. أولاً وقبل كل شيء ، تتمثل مهمتنا في دراسة جودة الخدمة والبنية التحتية الحالية لشبكة ICT-Towers ، وثانياً تقديم النهج لتنفيذ جودة الخدمة بالإضافة إلى الإشراف على الشبكة ومراقبتها.

الكلمات المفتاحية: QoS, Intserv, Diffserv, RED, WRED, NBAR et NBAR2

Table des matières

Chapitre III : Implémentation de la QoS

Liste des figures

Liste des tableaux

Liste des abréviations

ABR	Adaptive Bit Rate
ARPANET	Advanced Research Projects Agency Network
Cap Ex	Capital Expenses
CBWFQ	Class Based Weighted Fair Queuing
CEF	Cisco Express Forwarding
CIR	Committed Information Rate
CoS	Class of Service
DNS	Domain Name System
DOD	Department Of Defense
DPI	Deep Packet Inspection
DSCP	Differentiated Service Code Point
ECN	Explicit Congestion Notification
FIFO	First In First Out
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LFI	Link Fragmentation and Interleaving
LLC	Logical Link Control
LLQ	Low Latency Queuing
NBAR	Network Based Application Recognition
Op Ex	Operation Expenditure
OSI	Open Systems Interconnection
P2P	Peer to Peer
PDLM	Protocol Description Language Module
PHB	Per Hob Behaviour
PIR	Peak Information Rate
RED	Random Early Detection
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
SCE	Service Control Engine
SNA	System Network Architecture
TCP	Transmission Control Protocol
ToS	Type of Service
UDP	User Datagram Protocol
VoIP	Voice over IP
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection

Introduction générale

Dans le but de répondre aux exigences des entreprises dans un souci d'assurer la continuité des services avec une meilleure qualité, pallier aux problèmes qui surgissent et suivre l'évolution de la clientèle, ICT-Towers accorde une grande importance à l'optimisation de son réseau par la mise en oeuvre de la Qualité de Service.

Le processus d'optimisation du réseau est indispensable afin d'aboutir à une bonne performance aux applications critiques et une qualité de service satisfaisante. C'est dans ce contexte que ICT-Towers nous a confié, dans le cadre de notre projet de fin d'études, la mise en place de la Qualité de Service qui permettra l'optimisation de ses ressources réseaux.

Le présent rapport est le fruit de notre travail réalisé dans une période de quatre mois. Il est scindé selon trois chapitres couvrant l'ensemble des axes de notre travail.

Le premier chapitre présente une introduction au réseau IP et ses contraintes qui nous dirigent vers la Qualité de Service. Le deuxième chapitre concerne l'étude théorique de la Qualité de Service, ses indicateurs et ses modèles (IntServ et DiffServ).

Quant au troisième chapitre, il décrit l'infrastructure existante à ICT-Towers et présente une étude spécifique du réseau ICT-Towers et ses équipements pour la mise en place de la Qualité de Service, ainsi la démarche que nous avons suivi pour l'implémentation de la Qualité de Service.

A la fin du troisième chapitre, nous avons décrit l'étape de la validation de notre démarche déployée, ainsi que les outils utilisés et le résultat de ce mécanisme qui est la QoS.

Chapitre I

Introduction au réseau IP

I.1 Introduction

L'Internet Protocol est issu des recherches menées par le Département de Défense Américain (DOD) pendant la guerre froide dans les années 1960, mais il n'a été standardisé qu'en 1982. Son but était de permettre l'émergence de réseaux maillés, donc décentralisés, de telle sorte qu'un unique missile nucléaire russe ne puisse pas paralyser l'ensemble des télécommunications aux États-Unis. Une multitude de réseaux différents sont interconnectés par des passerelles (les routeurs), ce qui permet à un paquet d'emprunter plusieurs chemins différents pour atteindre sa destination.
Aujourd'hui, c'est fort heureusement pour des motifs bien plus agréables qu'on utilise IP : En effet, le réseau des réseau « Internet » repose sur lui, Nous allons décrire les architectures utilisées dans les réseaux IP.

I.2 Modèles OSI et TCP/IP

Devant la diversité des matériels, des logiciels et des interfaces, il a fallu trouver un modèle couvrant tous les aspects de la communication en réseau. Un modèle universel sur lequel s'appuierait les développeurs et fabricants de matériel réseau.
Le principe c'est de décomposer en plusieurs couches. Chaque couche ayant un rôle bien défini et chaque couche servant de support à la couche supérieure.

I.2.1 Le modèle OSI

Modèle à 7 couches finalisé en 1994, normalisé par l'ISO (ISO 7498)
Open System Interconnexion : Interconnexion de systèmes ouverts : Utilisé pour modéliser toute communication entre équipements terminaux.
Le but de ce modèle est d'analyser la communication en découpant les différentes étapes en 7 couches. Chacune de ces couches répond à une des questions suivantes :
Quelles sont les informations qui circulent ?
Sous quelle forme circulent-elles ?
Quel chemin empruntent-elles ?
Quelles règles s'appliquent aux flux d'informations ?

Le **Tableau I.1** ci-dessous démontre les 7 couches du modèle OSI en détail :

Couche	Principaux services	Protocoles
7. Application	Messagerie électronique, web, transfert de fichiers, accès à distance, systèmes de fichiers distribués, téléphonie sur IP, émulation de terminal etc…	HTTP, SMTP, POP3, FTP, Telnet, NFS, VoIP, BitTorrent
6. Présentation	Format des données, chiffrement	JPEG, MPEG, MP4, MP3, AVI
5. Session	Gestion du dialogue entre les applications	OpenSSL, NetBios, ASP
4. Transport	Contrôle que les données parviennent bien à leur Destinataire	TCP, UDP
3. Réseau	Adressage et gestion de l'itinéraire suivi par les données	IP, IPsec, ICMP, EIGRP, BGP
2. Liaison	Sous-couche LLC : gestion du déplacement des données (LLC signifie Logical Link Control) Sous-couche MAC : gestion de l'accès des données au réseau physique (MAC signifie Media Access Control)	802.11 (sans-fil), Ethernet, Wi-Fi
1. Physique	Définition du matériel : cuivre, fibre ou sans-fil, débit, nombre de fils, fonction de chaque fil, forme des prises, Etc.	1000Base-T et autres normes Ethernet physiques, liaison série, etc.

Tableau I. 1 : Les couches OSI

1. Couche physique :

Se charge de la transmission des bits à l'état brut sur le canal de communication.
Son objectif est d'assurer qu'un bit à 1 envoyé sur une extrémité arrive aussi à 1 de l'autre côté, et non à 0. Elle Concerne le voltage pour représenter les états 0 et 1, la durée d'un bit, la possibilité de transmission dans les deux sens en même temps, l'établissement initial d'une connexion et sa libération lorsque les deux extrémités ont fini, le nombre de broche d'un connecteur et leur rôle. [1]

2. Couche liaison de données :

Son rôle est de faire en sorte qu'un moyen de communication brut apparaisse à la couche réseau comme étant une liaison exempte d'erreurs de transmission.
Elle décompose les données en trames de données (quelques centaines ou milliers d'octets) et envoie les trames en séquence.
S'il s'agit d'un service fiable, le récepteur confirme la bonne réception de chaque trame en envoyant à l'émetteur une trame d'acquittement. Il est important d'éviter qu'un récepteur lent soit submergé de données par un émetteur rapide.
- Utiliser des mécanismes de régulation pour que l'émetteur connaisse la quantité d'espace disponible dans le tampon du récepteur. [1]
- Intégration de mécanisme de contrôle de flux et de gestion des erreurs.
- Difficulté supplémentaire dans les réseaux à diffusion : contrôler l'accès au canal partagé. C'est la sous-couche d'accès au média qui gère ce problème.

3. Couche réseau :

Contrôle le fonctionnement du sous-réseau.
Son objectif est de déterminer comment les paquets sont routés de la source vers la destination.
- Statiquement avec des tables câblées dans le réseau et rarement modifiées.
- Dynamiquement au début du dialogue pour la session ou pour chaque paquet selon la charge actuelle du réseau. Elle doit aussi régler tous les problèmes de qualité de service (délais, temps de transit, gigue, perte de paquets…) causé par exemple par des congestions (trop de paquets en même temps sur le sous-réseau).
- Elle doit aussi gérer les problèmes concernant l'adressage (qui peut être différent entre le réseau d'origine et celui de destination), la taille des paquets (paquets trop grands), les protocoles différents. [1]

4. Couche transport :

Cette couche couvre les objectifs suivants :
- Accepter des données de la couche supérieure, de les diviser en unités plus petites si nécessaire, de les transmettre à la couche réseau et de s'assurer qu'elles arrivent correctement à l'autre bout.
- Détermine le type de service à fournir à la couche session, et au final à l'utilisateur.
- Celui qui a le plus de succès est le canal point-à-point exempt d'erreur (en réalité très faible taux d'erreur) qui remet les messages ou les octets dans l'ordre dans lequel ils ont été envoyés.
- Il existe aussi la remise de messages isolés sans garantie de l'ordre d'arrivée ou la diffusion de messages à plusieurs destinataires (multicast).

- La couche transport offre un réel service de bout-en-bout, de la source à la destination. [1]
C'est à dire qu'un programme sur la machine source entretient une conversation avec un programme similaire sûr la machine de destination en utilisant les entêtes et les messages de contrôle.
Dans les couches plus basses, les protocoles sont échangés entre chaque machine et ses voisins immédiats et non entre les machines source et de destination qui peuvent être séparées par de nombreux routeurs.

5. Couche session :

Elle permet aux utilisateurs de différentes machines d'établir des sessions
(Ouverture / Fermeture, clé publique / clé privée…). Elle gère divers services comme :
La gestion du dialogue (suivi du tour de transmission).
La gestion du jeton (empêchant deux participants de tenter la même opération critique au même moment).
La synchronisation (gestion de points de reprise permettant aux longues transmissions de reprendre là où elles en étaient suite à une interruption). [1]

6. Couche présentation :

Elle s'intéresse à la syntaxe et à la sémantique des informations transmises.

- Permettre la communication entre ordinateurs travaillant avec différentes représentations de données.
- Définition de structures d'encodage standard.

7. Couche application :

Elle contient une variété de protocoles qui sont utiles aux utilisateurs :
HTTP: Protocole du World Wide Web
POP/IMAP/SMTP : Protocoles pour le courrier électronique
FTP : Protocole pour le transfert de fichiers
NNTP : Protocole pour les news.

❖ Transmission Control Protocol

TCP est l'un des principaux protocoles de transport utilisés sur les réseaux IP. Il est décrit en détail par la RFC 793 de l'IETF. En utilisant des systèmes de séquençage des paquets et d'acquittement des émissions/réceptions de données, TCP fournit aux différents postes du réseau des informations essentielles sur la bonne transmission des paquets IP à leur destinataire.
Lorsque des paquets ont été perdus sur le réseau (ce qui peut par exemple arriver lorsque le réseau est saturé), TCP sait retransmettre les données manquantes pour reconstituer le message dans son ensemble. TCP fournit d'autres capacités intéressantes, comme la possibilité d'employer des techniques de contrôle de flux pour limiter le débit d'une connexion.
Il est à noter que TCP est le protocole de transport sous-jacent d'HTTP le protocole du Web, mais aussi de la plupart des grandes applications d'Internet. TCP est plus rarement utilisé pour les applications temps réels, pour lesquelles on lui préfère souvent un autre protocole de transport internet, UDP

La **Figure I.1** ci-dessous montre le principe du modèle OSI et l'échange entres ses couches :

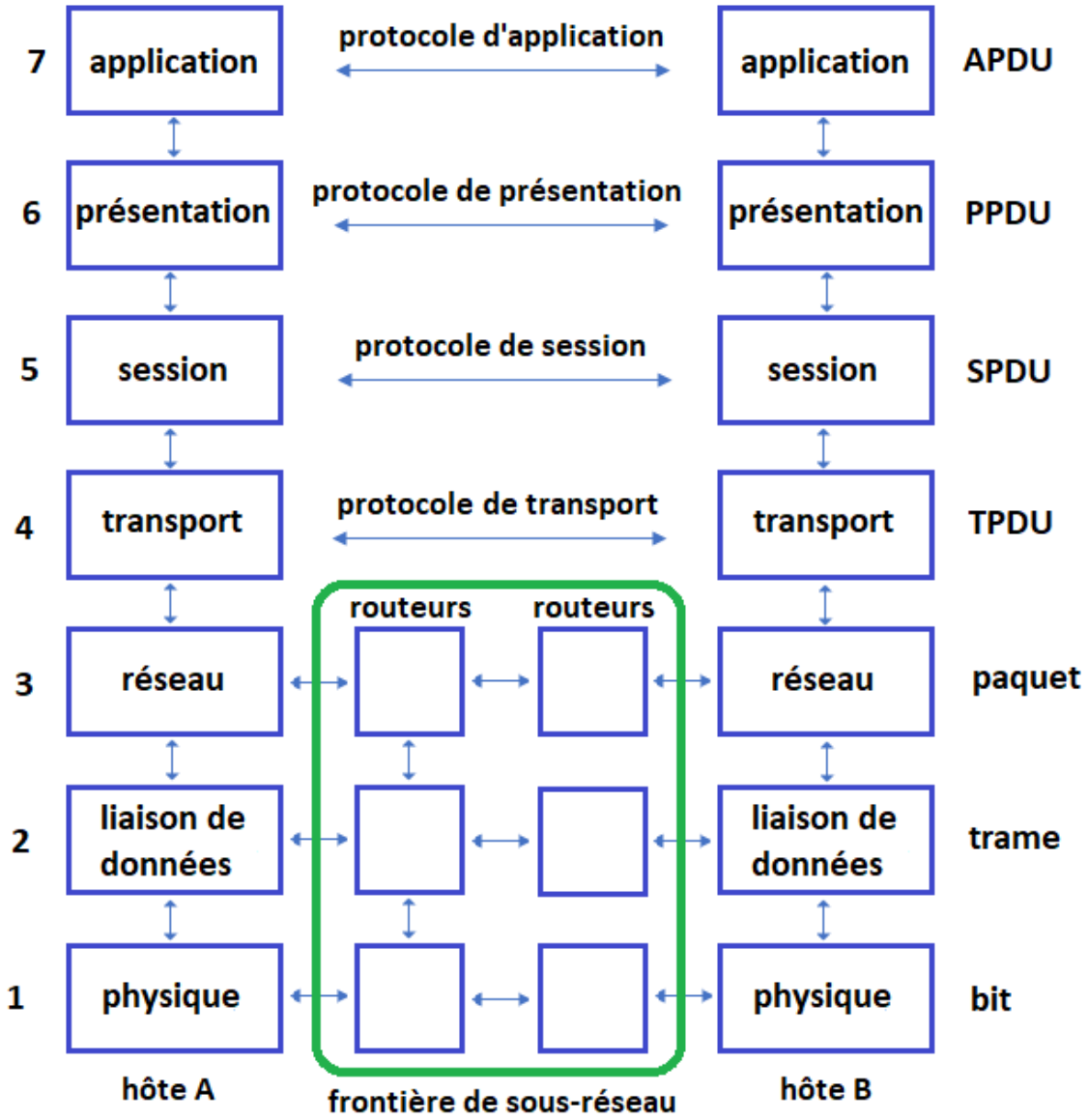

Figure I. 1 : Principe du Modéle OSI

I.2.2 Le modèle TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise « par-dessus » un protocole réseau, IP (Internet Protocol). Ce qu'on entend par « modèle TCP/IP », c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP. [1]

Le modèle TCP/IP, comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI.
Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.
L'origine du modèle TCP/IP remonte au réseau ARPANET. ARPANET est un réseau de télécommunication conçu par l'ARPA (Advanced Research Projects Agency), l'agence de recherche du ministère américain de la défense (le DOD : Departement of Defense). Outre la possibilité de connecter des réseaux hétérogènes, ce réseau devait résister à une éventuelle guerre nucléaire, contrairement au réseau téléphonique habituellement utilisé pour les télécommunications mais considéré trop vulnérable. Il a alors été convenu qu'ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergeante promettant. C'est donc dans cet objectif et ce choix technique que les protocoles TCP et IP furent inventés en 1974. L'ARPA signa alors plusieurs contrats avec les constructeurs (BBN principalement) et l'université de Berkeley qui développait Unix pour imposer ce standard, ce qui fut fait.
Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches. Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.

1. **La couche hôte réseau :**

Cette couche est assez « étrange ». En effet, elle regroupe les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

2. **La couche internet :**

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination.
Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.
Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI. La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol). Remarquons que le nom de la couche internet est écrit avec un « i » minuscule, pour la simple et bonne raison que le mot internet est pris ici au sens large littéralement (interconnexion de réseaux) même si l'Internet (avec un grand I) utilise cette couche.

3. 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 (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).

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.
UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

4. 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 (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). 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.

La **Figure I.2** nous montre le principe du modèle TCP/IP ainsi qu'une comparaison entre les couches avec le modèle OSI :

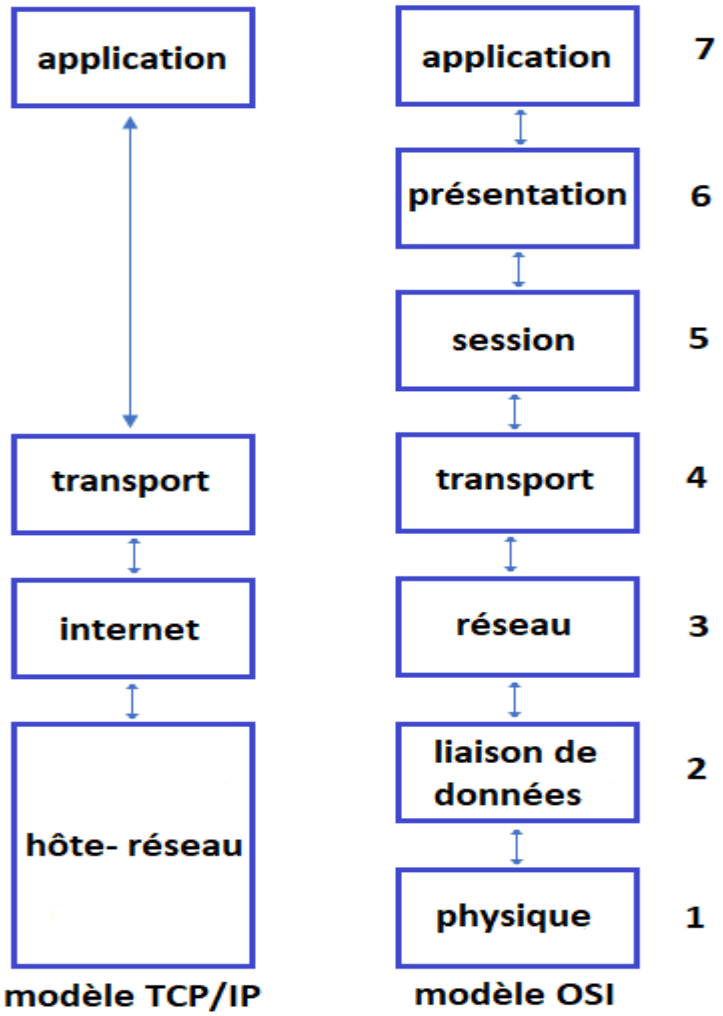

Figure I. 2 : Principe du Modéle TCP/IP

I.2.3 Le protocole UDP

User Datagram Protocol (UDP) est dit sans connexion car il n'y a pas d'établissement de connexion entre les hôtes émetteur et récepteur au niveau de la couche de transport avant qu'un segment ne soit transmis. UDP ne garantit pas la livraison des segments. De plus, les segments peuvent arriver en panne à la réception. Pour cette raison, UDP est dit peu fiable. Bien que le protocole UDP soit considéré comme un protocole non fiable, il est possible pour une application de disposer d'un transfert de données fiable lors de son utilisation, si la fiabilité est intégrée à l'application elle-même. Par exemple, DNS utilise UDP pour la communication client-serveur. [1]

Le **Tableau I.2** ci-dessous est une comparaison entre les deux concurrents TCP et UDP :

	TCP	**UDP**
Connexion	Les processus d'applications établissent une connexion avant que les messages ne puissent être échangés.	Les processus d'applications des messages sans créer de connexion.
Usage	Convient aux applications nécessitant une grande fiabilité et dont le temps de transmission est relativement moins critique.	Convient aux applications nécessitant une transmission rapide et efficace et la fiabilité est moins critique.
Utilisation par protocole de couche applications	Transfert de fichiers (FTP), courrier électronique (SMTP, POP et IMAP) et Web (HTTP/HTTPS)	Applications multimédia (VoIP, vidéo, jeux multi-joueurs en ligne) et DNS (communications client-serveur)
Fiabilité	Livraison garantie des messages d'application sans erreur et dans le bon ordre.	Aucune garantie que les messages parviendront à l'application de destination. De plus, les messages peuvent arriver en désordre.
Ordre de segments de données	Réorganise les segments de données dans l'ordre indiqué.	N'a pas d'ordre inhérent car tous les segments sont indépendants les uns des autres.
Acquittement	Les segments sont acquittés à la réception.	Pas d'acquittement à la réception.
Contrôle de flux	Mécanisme de contrôle de congestion qui régit l'émetteur de la couche de transport lorsqu'un ou plusieurs liens entre les hôtes source et destination deviennent trop encombrés.	UDP n'a pas d'option pour le contrôle de flux.
Vérification d'erreur	Les segments erronés sont retransmis de l'expéditeur au destinataire.	Les segments erronés sont ignorés. La récupération d'erreur n'est pas tentée.

Tableau I. 2 : La différence entre TCP et UDP

I.3 Equipements réseaux

Il existe plusieurs équipements réseaux qui servent à relier les machines terminales (Ordinateurs, Téléphones…). Nous allons définir les équipements qu'on va utiliser dans notre travail.

I.3.1 Les switches

a Définition

Un commutateur réseau (ou switch en anglais) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et 100). Il a donc la même apparence qu'un concentrateur (hub).[2]

Contrairement à un hub, un commutateur ne se contente pas de reproduire sur tous les ports chaque trame informatique qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs, Contrairement à un routeur, un commutateur de niveau 2 ne s'occupe pas du protocole IP. Il utilise les adresses MAC et non les adresses IP pour diriger les données. Les commutateurs de niveau 2 forment des réseaux de niveau 2 (Ethernet). Ces réseaux sont reliés entre eux par des routeurs (ou des commutateurs de niveau 3) pour former des réseaux de niveau 3 (IP). [2]

b Fonctionnement

Le commutateur établit et met à jour une table d' adresses MAC, qui lui indique sur quel port diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC source des trames reçues sur chaque port. Le commutateur construit donc dynamiquement une table qui associe des adresses MAC avec des ports correspondants.

Lorsqu'il reçoit une trame destinée à une adresse présente dans cette table, le commutateur renvoie la trame sur le port correspondant. Si le port de destination est le même que celui de l'émetteur, la trame n'est pas transmise. Si l'adresse du destinataire est inconnue dans la table, alors la trame est traitée comme un broadcast, c'est-à-dire qu'elle est transmise à tous les ports du commutateur à l'exception du port d'émission.

Un commutateur de niveau 2 est similaire à un concentrateur dans le sens où il fournit un seul domaine de diffusion. En revanche, chaque port a son propre domaine de collision. Le commutateur utilise la micro-segmentation pour diviser les domaines de collision, un par segment connecté. Ainsi, seules les interfaces réseau directement connectées par un lien point à point sollicitent le medium. Si le commutateur auquel il est connecté supporte le full-duplex, le domaine de collision est entièrement éliminé. [2]

I.3.2 Les routeurs

a) **Définition**

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets entre réseaux indépendants. Ce routage est réalisé selon un ensemble de règles formant la table de routage.

C'est un équipement de couche 3 du modèle OSI. Il ne doit pas être confondu avec un commutateur (couche 2) ou une passerelle (couche 3 et supérieures). [2]

b) **Principe de fonctionnement**

La fonction de routage traite les adresses IP en fonction de leur adresse réseau définie par le masque de sous-réseaux et les redirige selon l'algorithme de routage et sa table associée.
Ces protocoles de routage sont mis en place selon l'architecture de notre réseau et les liens de communication inter sites et inter réseaux.[2]

c) **Les protocoles de routage**

Les protocoles de routages permettent l'échange des informations à l'intérieur d'un système autonome. On retient les protocoles suivants :
- Etats de lien, ils s'appuient sur la qualité et les performances du média de communication qui les séparent. Ainsi chaque routeur est capable de dresser une carte de l'état du réseau pour utiliser la meilleure route : OSPF
- Vecteur de distance, chaque routeur communique aux autres routeurs la distance qui les sépare. Ils élaborent intelligemment une cartographie de leurs voisins sur le réseau : RIP
- Hybride des deux premiers, comme EIGRP.[1]

Parmi les protocoles de routages qui sont couramment utilisés, on cite :
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP).[1]

I.4 Adressage IP

L'adresse IP (Internet Protocol) désigne un numéro unique attribué de manière provisoire ou durable à un ordinateur connecté à un réseau informatique qui utilise l'internet protocole. Elle est constituée de 32 bits (4 octets) pour la version 4 (IPv4) comme il existe aussi la version 6 (IPv6) constituée de 128 bits (16 Octets) qui est actuellement utilisée dans les pays développés comme Les états unis, Japan, etc…

Cette suite de chiffres joue un rôle d'identification du branchement et permet l'acheminement (c'est-à-dire le routage) des paquets de données sur Internet et sur tous les supports informatiques (modem, routeur, ordinateur, smartphone, imprimante réseau, etc.), chaque interface en communication avec le réseau a besoin d'au moins une adresse IP. Cependant, il peut y avoir plusieurs adresses IP par interface, et plusieurs interfaces par ordinateur. Lors d'un échange de paquet transmis par le protocole IP, l'adresse IP de l'émetteur et du destinataire sont visibles.

Dans la majorité des cas, l'adresse IP est dite dynamique. C'est l'ordinateur qui, lorsqu'il se connecte au réseau, obtient automatiquement cette adresse grâce au protocole DHCP. Mais elle peut également être qualifiée de statique (ou fixe). C'est alors à l'utilisateur d'entrer manuellement son adresse.

Exemple adresse IPv4 : 172.16.20.3

Exemple adresse IPv6 : 2001 :0db8 :0000 :85a3 :0000 :0000 :ac1f :8001

I.5 Les listes d'accés

La liste d'accès (ACL : Access List) est un ensemble de règles définies pour contrôler le trafic réseau et réduire les attaques du réseau. Les listes de contrôle d'accès servent à filtrer le trafic en fonction de l'ensemble de règles définies pour les entrées et les sorties du réseau. [4]
Il s'agit de la liste d'accès créée à l'aide de l'adresse IP source uniquement. Ces listes de contrôle d'accès permettent ou refusent toute la suite de protocoles. Ils ne font pas la distinction entre le trafic IP tel que TCP, UDP, Https, etc. En utilisant les numéros 1-99 ou 1300-1999, le routeur le comprendra comme une liste de contrôle d'accès standard et l'adresse spécifiée comme une adresse IP source.
Il est possible de résumer le fonctionnement des ACL de la façon suivante : Le paquet est vérifié par rapport au premier critère défini. S'il vérifie le critère, l'action définie est appliquée. Sinon le paquet est comparé successivement par rapport aux ACL suivants. S'il ne satisfait aucun critère, l'action « Deny » est appliquée (Refusé).
Les critères sont définis sur les informations contenues dans les en-têtes IP, TCP ou UDP.
Des masques ont été définis pour pouvoir identifier une ou plusieurs adresses IP en une seule définition. Ce masque défini la portion de l'adresse IP qui doit être examinée.
0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés.
Deny 10.1.3.0 avec 0.0.0.255 : refus de toutes les IP commençant par 10.1.3.

- **ACL basées sur le temps**

Si nous ne souhaitons pas que les entrées de la liste d'accès prennent effet dès qu'elles sont appliquées, nous envisageons d'utiliser des listes de contrôle d'accès basées sur le temps.
Les listes de contrôle d'accès basées sur le temps nous permettent d'appliquer des règles de pare-feu basées sur des heures particulières du jour, du jour de la semaine ou du jour du mois. Ainsi, nous pouvons appliquer de manière granulaire les autorisations ou refuser les conditions que nous avons définies pour contrôler le trafic entrant et sortant de notre réseau. En d'autres termes, ils offrent plus de contrôle sur l'autorisation ou le refus d'accès aux ressources. Par exemple, nous pouvons autoriser les utilisateurs à accéder à Internet pendant le déjeuner, mais pas pendant les heures normales de bureau. Dans ce cas, les ACL temporelles nous permettront d'appliquer précisément ce type de stratégie. Nous pouvons également contrôler les messages de journalisation dans un sens que nous pouvons définir quand les entrées de la liste de contrôle d'accès doivent journaliser le trafic et par exemple, envoyer le journal à notre serveur.

I.6 Problématique

Toute entreprise quelle que soit sa taille ou sa nature a des objectifs bien définis surtout quand elle est dotée d'un système informatique et ses machines sont en réseau informatique avec une connexion Internet.
Pour les atteindre, elle doit disposer des équipements réseaux entre autres (PC, switch, routeur, câble, etc.…). C'est ainsi que pour notre part, reconnaissant le bienfondé de l'informatique surtout en réseau informatique, notre préoccupation se résumera au tour des questions suivantes :
Que faut-il faire pour administrer un réseau informatique et qui sera doté des équipements fiables ? Comment se présentera-t-il ?

I.6.1 Importance de la Qualité de Service

En s'appuyant sur des exemples réels, nous allons bien expliquer l'importance de la qualité de service.

- **Exemple 1 : Sécurité internationale**
  Dans une guerre entre deux pays, un message d'alerte n'a pas été reçu à une base militaire à un instant réel, ce qui a causé une grande défaite de l'un de ces deux pays. Cela est dû au retard dans le réseau de la boîte téléphonique ou la messagerie qui n'était pas priorisée en réseau.

- **Exemple 2 : La santé**
  Une opération cardiaque à distance à l'aide d'un robot contrôlé par un chirurgien a échoué ce qui a causé la mort du patient. Cela est dû à un très petit retard du mouvement du robot vu qu'il n'était pas favorisé ou prioritaire dans le réseau de l'hôpital.

- **Exemple 3 : Braquage de banque**
  Un voleur de banque qui s'enfuit après l'avoir braqué sans qu'il soit capturé par la caméra de surveillance, sachant qu'elle fonctionne en temps réel (RTP). La caméra devait avoir un haut débit et une classe prioritaire pour ne pas rater ces incidents.

C'est dans ces cas que réside l'importance de la qualité de service et qu'il n'y a pas d'autres moyens que de l'utilisé. Pour le comprendre, nous devons d'abord comprendre les problèmes courants du réseau.

I.6.2 Problèmes de la QoS dans les réseaux IP

Parmis les grands problèmes qui créent un encombrement, nous citons :

- Délai de bout en bout (Delay)
- Bande passante (Bandwidth)
- Variation du retard (gigue/Jitter)
- Perte de paquets (Packet Loss)

I.6.3 Spécification des besoins

En ce qui concerne les besoins, sa nécessite une étude approfondie afin de bien différencier entre les priorités des technologies (Bases de données, Voix, Vidéos…). Ces besoins varient d'une entité à une autre.

Prenant l'exemple d'une entreprise privée qu'on va appeler X. Parmi ses besoins les plus importants c'est la visioconférence.

Dans ce cas, la vidéo et la voix doivent être strictement favorisées par rapport aux autres technologies telles que (Téléchargement, Mail, Jeux vidéo, Réseaux sociaux…).

Pour ce faire, on doit utiliser le mécanisme QoS (Quality Of Service). C'est exactement son objectif :

- Assurer le bon partage des flux selon les priorités présentées.
- Eviter une grande consommation des ressources de la machine (Routeur par ex : CPU, ROM.…).

I.7 Conclusion

Au terme de ce chapitre, nous avons présenté d'une manière générale quelques informations à propos du réseau IP avec les modèles OSI et TCP/IP tels que la différence entre TCP/UDP, les protocoles de routages et les contraintes qui nous obligent à utiliser la QoS.
Dans le chapitre suivant, nous allons présenter la qualité de service dans le réseau IP.

CHAPITRE II

Etude de la QoS

II.1 Introduction de la qualité de service

Comme nous le savons, les données parcourent les réseaux sous forme de petits morceaux que nous appelons des trames. À l'intérieur, nous avons des paquets et à l'intérieur des paquets, nous avons des segments… etc. Normalement, certains paquets peuvent être envoyés plus rapidement que d'autres ou diviser notre bande passante en fonction du type de protocole de trafic utilisé.

Pour ce faire, nous devrons classifier nos paquets, les marquer de manière à définir des priorités différentes et décider de la manière dont les paquets seront traités dans les files d'attente d'interface. C'est exactement le rôle de ce mécanisme qui est la QoS.

La Qualité de service est un excellent outil malheureusement trop peu souvent utilisé qui permet de régler le routeur afin de diviser la bande passante efficacement entre les différentes applications.

La QOS correspond à la manipulation du trafic de sorte qu'un équipement réseau, tel qu'un routeur ou un commutateur, puisse transférer ce trafic conformément aux comportements requis de la part des applications à l'origine de ce trafic. En d'autres termes, la QoS permet à un équipement réseau de différencier le trafic et de lui appliquer différents comportements.
Jusqu'à présent, on utilisait des réseaux physiques différents pour transporter les trafics voix et données. Chaque réseau transportait un certain type de trafic et fournissait le niveau de qualité inhérent requis par celui-ci. Aujourd'hui, ces applications sont réunies sur des réseaux convergés (basés sur les paquets) au sein desquels les différents trafics partagent une infrastructure et des ressources réseaux communes. Ces réseaux basés sur les paquets sont conçus pour distribuer le trafic aux mieux. Ils ne disposent pas d'une QoS inhérente.
Pourtant, les abonnés aux services voix et vidéo exigent que ces services soient toujours disponibles, avec des niveaux de qualité acceptables. Les réseaux basés sur les paquets transmettent de grands volumes de trafic d'un point A à un point B, le tout en respectant les accords de service et les exigences de performance de toutes les applications à l'origine du trafic. Pour cela, ils utilisent la QoS.

Un réseau de communication constitue le pivot de toute organisation performante. Ces réseaux transportent une multitude d'applications et de données, y compris des données vidéo de haute qualité et des données sensibles aux retards telles que la voix en temps réel. Les applications gourmandes en bande passante étendent les capacités et les ressources du réseau, mais complètent et ajoutent de la valeur et améliorent chaque processus métier. Les réseaux doivent fournir des services sécurisés, prévisibles, mesurables et parfois garantis. L'obtention de la qualité de service (QoS) requise en gérant les paramètres de délai, de variation de délai (Gigue), de bande passante et de perte de paquets sur un réseau devient le secret d'une solution commerciale réussie de bout en bout. Ainsi, la qualité de service est l'ensemble des techniques permettant de gérer les ressources du réseau.

Un équipement réseau tel qu'un routeur ou un commutateur différencie le trafic comme suit :
1. Il reçoit les paquets sur son interface entrante, il examine les paquets et catégorise le trafic dans des groupes appelés classes de services (CoS).
2. Si un mécanisme de contrôle facultatif est configuré, il limite le trafic ou l'assigne à une autre classe.
3. Les paquets sont placés dans des files d'attente en attendant les ressources de transmission.
4. Le planificateur sort les paquets des files d'attente et les transmet selon l'ordre configuré pour le planificateur.
5. Si un outil de mise en forme du trafic est configuré, il met en forme le trafic en fonction du facteur de mise en forme configuré.
6. Si une fonction de marquage est configurée, l'équipement marque la valeur du champ DS de l'en-tête IP afin que le prochain équipement qui reçoit le paquet sache comment le catégoriser.

II.2 Critères de la qualité de service

II.2.1 Congestion

C'est ce qui s'est produit lorsqu'une interface a reçu une quantité de flux de données supérieure à ce qu'elle peut gérer. Cela peut arriver pour les raisons suivantes :

- Bande passante (Bandwidth) : Parfois appelé bande passante par abus de langage, il définit le volume maximal d'information (bits) par unité de temps (secondes)
- Délai (Latency) : Période prise par les paquets qui sortent de l'interface émettrice jusqu'à atteindre l'interface destinataire.
- Gigue (Jitter) : Flux de paquets de flux arrivant au récepteur dans le mauvais ordre chronologique, ce serait mauvais si les paquets de flux étaient VOIP par exemple.
- Perte de paquet (Packet Loss) : Les paquets sont abandonnés lorsque le lien est encombré.

a Points de congestion

Il existe plusieurs points dont lequel se produit la congestion. Ces points sont les zones du réseau qui subissent un encombrement de trafic, cela peut arriver pour les raisons suivantes :

- Point d'agrégation : Routeur se connectant à trop de réseaux dans une interface et effectuant l'agrégation pour eux dans une autre interface.
- Différence de vitesse : Les données passent par le routeur où elles sont entrées avec FastEthernet et sortent de l'interface Ethernet.
- LAN à WAN : Identique à la différence de vitesse, un routeur connecté à un réseau LAN à haute vitesse mais d'un autre côté, il se connecte au WAN (le WAN est toujours une liaison lente).

La **Figure II.1** ci-dessous montre les différents points de congestion cités précédemment :

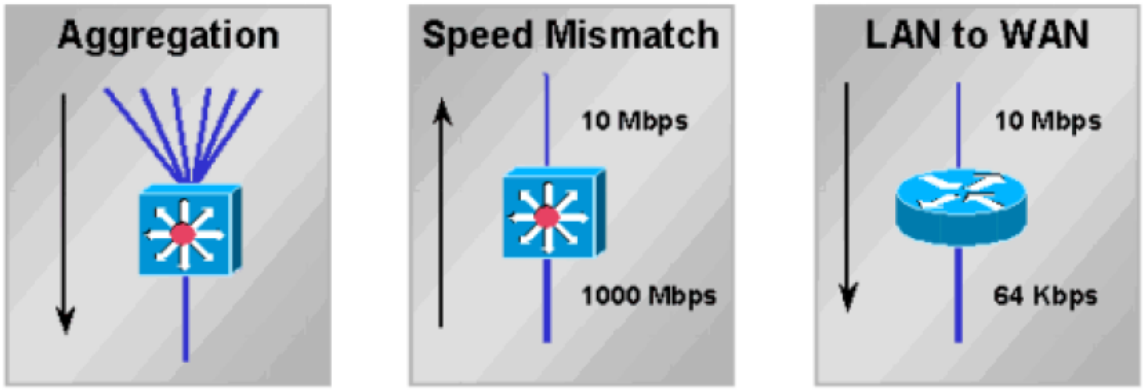

Figure II. 1 : Points de congestion classiques

❖ **Règle du lien le plus lent :**

Cette règle repose sur l'équation suivante :

La bande passante maximale disponible = La bande passante du lien le plus lent (64 Kbps dans notre cas). Cet exemple est illustré dans la **Figure II.2** ci-dessous qui est une topologie qui peut exister dans le cas réel.

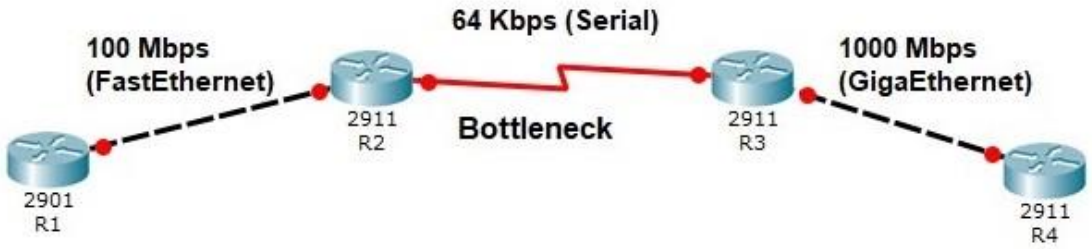

Figure II. 2 : Point de congestion

Pour résoudre ce problème, nous pouvons faire l'une des deux choses suivantes :

1. Ajouter plus de bande passante, mais cela ne coûte pas cher et peut-être que nous serions confrontés à des limitations dans les technologies utilisées dans l'infrastructure et qui nous ne permettra pas d'ajouter plus de bande passante.
2. Utiliser des techniques de QoS tel que :
   - Classer le trafic dans les classes de qualité de service et leur attribuer des priorités en fonction de leur importance.
   - Utiliser le marquage pour les paquets.
   - Utiliser des mécanismes de mise en file d'attente tels que : FIFO, WFQ, CBWFQ, LLQ.

N'oubliez pas que pour une qualité optimale du trafic vocal, nous utilisons l'en-tête RTP Compression + LLQ.

Pour le trafic de données interactif, nous utilisons l'en-tête TCP Compression + CBWFQ (Nous parlerons plus tard de ces algorithmes de file d'attente).

II.2.2 Types de retard

1. **Délai de traitement (**lié au périphérique**) :** un périphérique, tel qu'un routeur ou un commutateur de couche 3, prendra une période pour déplacer les paquets d'une interface d'entrée à une interface de sortie. [3]

Cette époque dépend de nombreux facteurs, tels que :

- Utilisation de la vitesse du processeur (CPU)
- Mode de commutation IP
- Architecture de la route
- Fonctions configurées sur les interfaces d'Entrée/Sortie

2. **Délai de files d'attente (**lié au périphérique**) :** la période sera prise par les paquets en attente ou restant dans la file d'attente de sortie du périphérique.

Cette période dépend de nombreux facteurs tels que :

- Nombre d'autres paquets en attente dans cette file d'attente
- Taille des autres paquets en attente également dans cette file d'attente
- Bande passante de l'interface où la file utilisera pour laisser les paquets entrer ou sortir
- Mécanismes de file d'attente configurés sur cette interface

3. **Délai de sérialisation (**lié au support**) :** un délai sera nécessaire pour placer les images sur un support physique afin de les sortir.

4. **Délai de propagation (**lié au support**) :** la période sera prise par les paquets à l'intérieur du lien physique (support) pendant le trajet de bout en bout. [3]

❖ **Méthodes pour prévenir les retards :**

Si nous supposons que le commutateur de routeur ou de Layer 3 est suffisamment puissant, le délai de sérialisation peut être évité à l'aide de la mise en file d'attente. Cela dépendra de :

- Number : longueur moyenne de la file d'attente
- Size : longueur moyenne de la file d'attente de paquets
- Bande passante : bande passante du lien
- Méthodes pour accélérer les paquets sensibles au délai
- Augmenter la bande passante
- Prioriser les paquets sensibles au retard en utilisant CBWFQ, WFQ, LLQ
- Réorienter les priorités des paquets en demandant au fournisseur de services Internet de le faire lorsque deux sites connectés via ce dernier.
- Compresser la charge
- Compression d'en-tête

❖ **Impact de la perte de paquets :**

En raison de la congestion importante, les images peuvent ne pas être claires, entendre le son au ralenti, la vidéo n'est pas synchronisée avec l'audio… etc.

Lorsque la file d'attente de sortie d'interface est pleine, les autres paquets qui restent dans cette file d'attente ne trouveront pas de place dessus et seront rejetés, ce qui s'appelle « Tail Drop ».

Les routeurs peuvent supprimer des paquets dans les situations suivantes :

- A cause de la file d'attente d'entrée : le processeur est occupé et ne peut pas traiter d'autres paquets
- Ignorer la raison : l'espace tampon est plein
- Raison de dépassement : le processeur est occupé et le tampon est plein
- Raison des erreurs de trame : erreurs CRC

Parmis les méthodes de prévention de la perte de paquets (paquets d'applications sensibles au rejet), nous suggérons :

- Augmenter la capacité de liaison
- Utilisez LLQ qui fournit une garantie de bande passante suffisante et fournira également un transfert prioritaire pour les paquets sensibles au largage
- Utilisez WRED qui permet de supprimer les paquets de priorité inférieure avant que la congestion ne survienne

Alors encore, quelle est la QoS ? La qualité de service est la capacité du réseau à fournir un meilleur service aux utilisateurs et aux applications et à fournir des méthodes pour empêcher la gigue, les retards et la perte de paquets des applications sensibles au facteur temps et aux applications critiques.

Le mécanisme de la qualité de service doit suivre les étapes suivantes :

- Types d'étude de votre trafic réseau et leurs exigences
- Déterminer les exigences de QoS pour chaque type
- Chaque groupe sera mis en classe
- Chaque classe sera mise en police pour répondre à ses exigences de QoS

II.3 Modéles QoS

La qualité de service peut être divisée en trois niveaux différents, également appelés services modèles. Ces modèles de service décrivent un ensemble de capacités QoS de bout en bout qui est la capacité du réseau à fournir un niveau de service spécifique pour le trafic réseau d'un bout à l'autre du réseau. Les trois services niveaux sont : **Best-effort service**, **integrated service**, and **differentiated service**. Nous allons examiner chaque modèle de service plus en détail.

II.3.1 Service meilleur effort (Best effort)

Le service Best-effort, comme son nom l'indique, est celui où le réseau fera tout son possible tentative pour livrer un paquet à sa destination. Avec le meilleur effort rien ne garantit que le paquet atteigne la destination voulue. Une application peut envoyer des données à tout prix, à tout moment, sans demander l'autorisation ou notifier le réseau. Certaines applications peuvent prospérer sous ce modèle. FTP et HTTP, par exemple, peuvent prendre en charge le service au mieux, sans trop de difficultés. [3]

Ce modèle de service n'est toutefois pas optimal pour les applications sensibles aux retards de réseau, aux fluctuations de la bande passante et aux autres conditions changeantes du réseau.

Les applications de téléphonie en réseau, par exemple, peuvent nécessiter une quantité de bande passante plus cohérente pour fonctionner correctement.

Les résultats du service Best-effort pour ces applications pourraient entraîner des échecs d'appels téléphoniques ou une interruption de la parole au cours de l'appel.

II.3.2 Service intégré (Integrated service)

Le modèle de service intégré fournit aux applications un niveau de service garanti en négociant de bout en bout les paramètres de réseau. Les applications demandent le niveau de service nécessaire à leur bon fonctionnement et à la fiabilité du système de qualité de service pour réserver les ressources réseau nécessaires avant le début du transfert de l'application. Il est important de noter que l'application n'enverra pas le trafic tant qu'elle n'aura pas reçu un signal du réseau indiquant que le réseau peut gérer la charge et fournir la qualité de service demandée de bout en bout. [4]

Pour ce faire, le réseau utilise un processus appelé contrôle d'admission.
Le contrôle d'admission est le mécanisme qui empêche le réseau d'être surchargé. Le réseau n'enverra pas de signal à l'application pour qu'elle commence à transmettre les données si la qualité de service demandée ne peut pas être livrée. Une fois que l'application commence la transmission des données, les ressources réseau réservées à l'application sont conservées de bout en bout jusqu'à ce que l'application soit terminée ou jusqu'à ce que la réservation de bande passante dépasse ce qui est autorisé pour cette application.
Le réseau s'acquittera de ses tâches de maintenance de l'état par flux, la classification, la régulation et la mise en file d'attente intelligente par paquet pour répondre à la QoS requise.
Cisco IOS dispose de deux fonctionnalités pour fournir un service intégré sous la forme de services de chargement contrôlés. [4]

Il s'agit du protocole de réservation de ressources (RSVP : Resource Reservation Protocol) et de la mise en file d'attente intelligente. RSVP est actuellement en cours de normalisation par l'IETF (Internet Engineering Task Force) dans l'un de leurs groupes de travail.
La mise en file d'attente intelligente inclut des technologies telles que la mise en file d'attente pondérée (WFQ) et la détection précoce pondérée aléatoire (WRED).
RSVP est un protocole propriétaire de Cisco utilisé pour signaler au réseau les exigences de QoS d'une application. Il est important de noter que RSVP n'est pas un protocole de routage. RSVP fonctionne conjointement avec les protocoles de routage pour déterminer le meilleur chemin à travers le réseau qui fournira la qualité de service requise. Les routeurs activés par RSVP créent en fait des listes d'accès dynamiques pour fournir la QoS demandée et s'assurer que les paquets sont livrés aux paramètres de qualité minimum prescrits.

II.3.3 Service différencié (Differentiated service)

Ce service est le dernier modèle de QoS et qui est géré par l'administrateur réseau.
Le service différencié comprend un ensemble d'outils de classification et de mécanismes de mise en file d'attente permettant de fournir certains protocoles ou applications avec une certaine priorité par rapport à un autre trafic réseau.
Les services différenciés s'appuient sur les routeurs de périphérie pour effectuer la classification des différents types de paquets traversant un réseau. Le trafic réseau peut être classifié en fonction de l'adresse réseau, des protocoles et des ports, des interfaces d'entrée ou de toute autre classification pouvant être réalisée au moyen d'une liste d'accès standard ou étendue. [3]

❖ **La configuration de QoS DiffServ :**

La configuration de QoS DiffServ se fait en suivant ces trois étapes :

1. Trier le trafic en utilisant une carte de classes (Class-map)
2. Définir une stratégie QoS à l'aide d'une stratégie-map (Policy-map)
3. Appliquer la stratégie à une interface à l'aide de la commande service-policy

Après cette étude, nous citons brièvement les caractéristiques des modèles :
Best effort = No QoS
Integrated Service avait un seul protocole qui est le RSVP
Differentiated Service contient tout le reste :

- Classification
- Marquage
- Gestion de la congestion (Algorithmes de file d'attente)
- Évitement de congestion (Congestion Avoidance)
- Maintien de l'ordre et mise en forme (Policing and Shaping)
- Efficacité du lien (Link Efficiency)

II.4 Classification

Dans le réseau IP, le trafic doit être classifié selon l'importance pour satisfaire certains besoins. Cette étape est réalisée souvent par le marquage des paquets en utilisant des bits particuliers appelés flag (Drapeaux), qui permettent de définir l'importance de chaque paquet dans le réseau et aussi d'identifier les paquets moins importants.
Cette partie présente les différentes théories de la classification du trafic et explique les mécanismes d'utilisation de ces drapeaux dans un paquet. Il y a plusieurs façons possibles dont ces drapeaux sont définis et les niveaux de classification dépendent de la méthode utilisée.
La classification peut être considérée comme insufflant dans les paquets de données, une intelligence directive concernant les périphériques réseau. L'utilisation de schémas de hiérarchisation tels que la détection aléatoire précoce (RED : Random Early Detection) et le débit adaptatif (ABR : Adaptive Bit Rate) permettent au routeur d'analyser les flux de données et les caractéristiques d'encombrement et d'appliquer ensuite des contrôles de congestion aux flux de données.
Ces applications peuvent impliquer l'utilisation de la fenêtre glissante TCP ou des algorithmes d'arrière-plan (back-off Algorithms). L'utilisation des indicateurs de classification du trafic dans le paquet supprime la fonctionnalité de décision du routeur et détermine les niveaux de service requis pour le flux de trafic particulier du paquet. Le routeur tente ensuite de fournir au paquet la qualité de service demandée.
Cette partie examine en détail la norme IP d'origine pour la classification des niveaux de service, le bit Type de service (ToS : Type of Service), la norme de remplacement actuelle, le point de code Diffserv (DSCP : Diffserv Code Point), l'utilisation de services de réservation intégrés tels que RSVP. Enfin, explorez les réseaux intégrés prenant en charge les applications utilisant la reconnaissance de réseau basée sur les réseaux (NBAR) de Cisco. Ce chapitre ne traitera pas des configurations ni des types de produits, mais d'une compréhension générale des théories et des problèmes liés à ces architectures de qualité de service différentes.

II.4.1 Deep Packet Inspection

L'inspection approfondie des paquets (DPI) permet d'examiner le paquet au-delà des informations de base de l'en-tête. Le DPI détermine intelligemment le contenu d'un paquet particulier, puis enregistre ces informations à des fins statistiques ou effectue une action sur le paquet.

Les applications activées par DPI sont les suivantes :

- Gestion du trafic ou possibilité de contrôler les applications des utilisateurs finaux telles que les applications entre homologues.
- Contrôle de la sécurité, des ressources et des entrées.
- Application de la politique et améliorations du service telles que la personnalisation du contenu ou le filtrage du contenu.

Les avantages comprennent une visibilité accrue sur le trafic réseau, ce qui permet aux opérateurs de réseaux de comprendre les modèles d'utilisation et de corréler les informations de performances du réseau tout en fournissant une facturation de base d'utilisation ou même une surveillance de l'utilisation acceptable.

DPI peut également réduire les coûts globaux sur le réseau en réduisant les dépenses de fonctionnement (OpEx : Operation Expenditure) et les dépenses en capital (Cap Ex : Capital Expenditure) en fournissant une compréhension plus approfondie de ce qui se passe sur le réseau et en offrant la possibilité de diriger ou de hiérarchiser davantage le trafic intelligemment.

Cisco dispose actuellement de deux solutions matérielles pour atteindre cette fonctionnalité DPI : la gamme de produits Cisco Service Control Engine (SCE) et le matériel PISA nouvellement introduit pour le superviseur Cisco 6500/7600. [8]

En réalité, ACL (Access List) ou la liste d'accès fait partie du DPI. Or, elle n'est pas très puissante en inspection. C'est pour cela, nous allons par la suite définir le NBAR et sa version améliorée NBAR 2.

II.4.2 Network Based Application Recognition

L'un des éléments clés des réseaux activés pour le contenu est la possibilité de classifier le trafic en fonction d'informations plus détaillées que les numéros de port ou les adresses statiques. Cisco répond à cette exigence en développant un nouveau moteur de classification appelé Network Based Application Recognition ou NBAR. NBAR est un nouveau moteur de classification qui examine dans un paquet et effectue une analyse avec état de l'information contenue dans le paquet. Bien que NBAR puisse classifier les protocoles de port statiques, son utilité est bien plus grande pour la reconnaissance des applications utilisant des numéros de port attribués de manière dynamique, classification détaillée du trafic HTTP et classification du trafic Citrix ICA par les applications publiées. [6]

Avant de poursuivre, il convient de noter que la classification NBAR pose deux problèmes importants :

- NBAR fonctionne uniquement avec le trafic IP ; Par conséquent, si vous avez du trafic SNA (System Network Architecture) ou hérité, d'autres schémas de classification et de mise en file d'attente doivent être utilisés.
- NBAR fonctionnera uniquement avec un trafic pouvant être commuté via Cisco Express Forwarding (CEF).

Si de nouvelles applications sortent, NBAR peut les reconnaître puisque Cisco fournit des fichiers PDLM (Protocol Description Language Module).

A. Fonctionnalité PDLM

Un PDLM (Protocol Description Language Module) est un fichier séparé disponible sur « Cisco.com » qui est utilisé pour ajouter la prise en charge d'un protocole actuellement non disponible dans le logiciel Cisco IOS. Un PDLM étend la liste des protocoles que NBAR peut reconnaître.

Les PDLM permettent également à NBAR de reconnaître de nouveaux protocoles sans nous obliger à installer une nouvelle image Cisco IOS ou à reconfigurer notre routeur. Les nouveaux PDLM sont uniquement publiés par Cisco et peuvent être chargés à partir de la mémoire flash.

B. Avantages NBAR

- Avec NBAR, nous pouvons classer le trafic HTTP avec une URL, un hôte ou même un type MIME.
- NBAR soutenu par CBWFQ, police, DSCP, WRED.

❖ Next Generation NBAR (NBAR 2):

NBAR2 ou Next Generation NBAR est une nouvelle architecture de NBAR basée sur le moteur de contrôle de service (SCE : Service Control Engine) avec des techniques de classification avancées, une précision et de nombreuses autres signatures. NBAR2 est rétro-compatible et est pris en charge sur les nouvelles plates-formes avancées. NBAR2 est adopté en tant que mécanisme de classification de protocole multiplateformes de Cisco. Il prend en charge plus de 1000 applications et sous-classifications, et Cisco ajoute / fournit de nouvelles signatures et mises à jour de signatures via des packs de protocole publiés chaque mois. [8]

a Avantages NBAR 2

NABR 2 offre plus d'avantages que NBAR, parmi ces avantages :

- **Techniques de classification avancées** : NBAR 2 utilise les techniques de classification de SCE, qui permettent la classification des techniques de transition IPv4, IPv6 et v6. NBAR 2 peut classifier les applications évasives telles que Skype et Tor, ainsi que les applications professionnelles telles que MS-Lync (Serveur Microsoft), les applications cloud telles que Office365, ainsi que les applications mobiles telles que Facetime, etc… à l'aide des techniques de classification avancées.

- **Prise en charge de l'extraction de champs :** Elle fournit le mécanisme permettant d'extraire des champs prédéfinis à partir des en-têtes de paquet qui peuvent être exportés via Flexible NetFlow (FNF) pour la génération de rapports.

- **Catégorisation et attributs :** Elle Fournit le mécanisme permettant de faire correspondre les protocoles ou les applications en fonction d'attributs attribués de manière statique, tels que le groupe d'applications, la catégorie, la sous-catégorie, le cryptage et le tunnel. La catégorisation des protocoles et des applications en différents groupes facilite la création de rapports et l'application de stratégies de qualité de service.

- **Bibliothèque commune des protocoles pour NBAR2 sur plusieurs plates-formes :** Elle offre des signatures indépendantes de la plate-forme pour les plates-formes prises en charge par NBAR 2.

- **Livraison des signatures via le pack de protocoles** : Un pack de protocoles est un ensemble de protocoles développés et emballés ensemble. Les packs de protocoles permettent de distribuer les mises à jour de protocole en dehors des versions du système d'exploitation Cisco et permettent un ajustement plus rapide, plus flexible et plus rapide aux tendances du marché. Les packs de protocoles peuvent être chargés sur le routeur sans remplacer l'IOS ni recharger le périphérique.

- **Protocole personnalisé utilisant l'URL HTTP et/ou le nom d'hôte :** Il fournit le mécanisme permettant de définir des protocoles personnalisés à mettre en correspondance, en fonction de l'URL HTTP et/ou du nom d'hôte. [9]

b Catégorisation du trafic dans NBAR 2

NBAR2 regroupe les applications en fonction de divers attributs, tels que :

- **Groupe d'applications :** Regroupement d'applications faisant partie de la même suite d'applications ou de la même "Marque"

Par exemple : Yahoo-Messenger, Yahoo-VoIP-Messenger et Yahoo-VoIP-over-SIP sont regroupés sous le groupe Yahoo-Messenger-group.

- **Catégorie :** regroupement d'applications prenant en charge des fonctionnalités similaires du point de vue de l'utilisateur final.

Exemple : "Email", "Jeu", "groupe de discussion" etc...

- **Technologie P2P (Peer-to-Peer) :** L'attribut indique si l'application utilise la technologie p2p.
- **Tunneling :** Attribut indique si une application tunnelise (VPN) d'autres protocoles.
- **Cryptage :** L'attribut indique si une application est cryptée. [8]

II.5 Marquage

II.5.1 Marquage couche 2

Le marquage de couche 2 peut être réalisé pour une variété de types de trames :

- Ethernet : En utilisant le champ de classe de service (CoS) 802.1p.
- Frame Relay : En utilisant le bit Discard Eligible DE (bit dans l'en-tête de relais de trames pour contrôler la vitesse CIR, 1 = oui 0 = non).
- ATM : En utilisant la priorité de perte de cellules.
- MPLS : En utilisant le champ EXP (Similaire à CoS). Il contient aussi 3 bits et qui est un champ qui marque les classes dans MPLS. [6]

❖ **CoS :** Class of service=3bits (En-tête de couche 2). Son inconvénient c'est qu'il vérifie que 3bits. C'est pour cela quand il y a des classifications de niveau 3 (dans les routeurs), sa nécessite un champ plus défini de 6 bits (DSCP). [6]

Le marquage des trames Ethernet est réalisé à l'aide du champ CoS (Class of Service) 3 bits 802.1p. Le champ CoS fait partie du champ 802.1Q de 4 octets dans un en-tête Ethernet et n'est donc disponible que lorsque le marquage de trame VLAN 802.1Q est utilisé.

La signalisation d'appel est celle qui permet au téléphone de sonner ou de regarder la qualité de celui-ci ; elle est donc moins prioritaire, tandis que l'appel vocal (5) est plus important car c'est le paquet qui transporte l'ensemble de l'audio.

a Priorité IP (IP Precedence/IPP)

La priorité IP utilise les trois premiers bits (pour un total de huit valeurs) du champ ToS afin d'identifier la priorité d'un paquet. Les paquets avec une valeur IP Precedence supérieure doivent être fournis avec un meilleur niveau de service. Les valeurs de priorité IP sont comparables aux valeurs Ethernet COS. [6]

b Définition des sept niveaux de priorité IP (IP Precedence) /CoS

Le **Tableau II.1** ci-dessous représente les champs CoS et IP Precedence qui fournissent 8 valeurs de priorité :

Type	Décimal	Binaire	Application Générale
Routine	**0**	**000**	Meilleur effort de transmission
Priorité	**1**	**001**	Transmission à priorité moyenne
Immediate	**2**	**010**	Renvoi hautement prioritaire
Flash	**3**	**011**	Renvoi de signalisation d'appel VoIP
Flash-Override	**4**	**100**	Transfert de vidéo-conférence
Critique	**5**	**101**	Transfert de voix sur IP
Internet	**6**	**110**	Contrôle inter-réseau (réservé)
Contrôle Internet	**7**	**111**	Contrôle réseau (réservé)

Tableau II. 1 : Les niveaux IPP/CoS

Par défaut, tout le trafic a une priorité IP de 000 (routine) et est transmis aux mieux. Le trafic réseau normal ne doit pas (dans la plupart des cas) et ne peut pas être paramétré sur 110 (contrôle inter-réseau) ou 111 (contrôle réseau), car il pourrait interférer avec des opérations réseau critiques, telles que les calculs STP (Spanning Tree) ou les mises à jour de routage.

II.5.2 Marquage couche 3

Le marquage de couche 3 est réalisé à l'aide du champ du type de service (ToS) 8 bits, une partie de l'en-tête IP. Une marque dans ce champ restera inchangée car elle se déplace de saut en saut, sauf si un périphérique de couche 3 est explicitement configuré pour écraser ce champ. [6]

Deux méthodes de marquage utilisent le champ ToS :

- Priorité IP (IP Precedence/IPP) : Utilise les trois premiers bits du champ ToS.
- DSCP (Differentiated Service Code Point) : Utilise les six premiers bits du champ ToS. Lorsque nous utilisons DSCP, le champ ToS est souvent appelé le champ Services différenciés (DS).

a Point de code de service différencié (DSCP)

DSCP utilise les six premiers bits de l'en-tête de type de service pour identifier la priorité d'un paquet. Les trois premiers bits identifient le sélecteur de classe (Class Selector) du paquet et sont rétro-compatibles avec la priorité IP. Les trois bits suivants identifient la priorité précédente (Drop Precedence) du paquet. Le **Tableau II.2** explique particulièrement le champ DSCP et ses répartitions.

7	6	5	4	3	2	1	0
IP Precedence			**CU**				
DSCP						**Flow Control**	

Tableau II. 2 : Differentiated Code Point

DSCP : Differentiated services code point.

CU : Currently unused (Actuellement non utilisé).

Flow Control : Contrôle de flux.

IP Precedence: Priorité IP.

b PHB (Per Hop Behaviour)

Ce qui signifie Comportement par saut. Il peut être 3 choses :

- Expedited Forwarding EF (Expédition accélérée) : transfert attendu est égale à 5.
- Assured Forwarding AF (Expédition assurée) : valeur = 1,2,3,4 et égale aux niveaux de précédence IP de 1 à 4.
- Best Effort : Priorité minimum, PHB par défaut, bits de valeur 000000 (CS0)

1. Assured Forwarding :

La RFC 2597 définit le PHB « Assured Forwarding (AF) » et le décrit comme un fournisseur d'un domaine DS (Diffserv Field) pour offrir différents niveaux d'assurance de transfert pour les paquets IP reçus d'un domaine DS client. Le PHB Assured Forwarding garantit une certaine bande passante à une classe AF et permet l'accès à une bande passante supplémentaire, le cas échéant. Il existe quatre classes AF, de AF1x à AF4x. Dans chaque classe, il existe trois probabilités de chute (drop). En fonction de la politique d'un réseau donné, les paquets peuvent être sélectionnés pour un PHB en fonction du débit requis, du délai, de la gigue, de la perte ou en fonction de la priorité d'accès aux services réseau. Les classes 1 à 4 sont appelées classes AF. [5]

2. Expedited Forwarding :

La RFC 2598 définit le PHB « Expedited Forwarding (EF) » : "Le PHB EF peut être utilisé pour créer un service de faible perte, faible temps de latence, faible gigue, bande passante assurée, via des domaines DS (Diffserv). Un tel service apparaît sur les terminaux comme une connexion point à point ou une "ligne louée virtuelle". Ce service a également été qualifié de service Premium. " Le Code point 101110 est recommandé pour le PHB EF, ce qui correspond à une valeur DSCP de 46. [5]

3. Class Selector (Sélecteur de classe) : Conserve une compatibilité ascendante avec le champ de priorité IP.

Exemple : AF33 = 011 **11**0, AF31 = 011 **01**0. Quel paquet a la priorité la plus élevée pour être abandonné ? La réponse est 011 **01**0 car **01**0 < **11**0
Exemple : Que signifie 000 000 en DSCP ? cela signifiera le meilleur effort.
Le **Tableau II.3** représente les différentes classes, leur représentation DSCP en décimal, en binaire ainsi la représentation en IPP et la probabilité de la chute (Drop Precedence).

Nom de la classe	DSCP	Binaire	IPP	Drop Precedence
CS0 (BE)	**0**	000 000	**0**	
CS 1	**8**	001 000	**1**	Non utilisé
AF11	**10**	001 **01**0		Low (01)
AF12	**12**	001 **10**0		Medium (10)
AF13	**14**	001 **11**0		High **(11)**
CS 2	**16**	010 000	**2**	Non utilisé
AF21	**18**	010 **01**0		Low **(01)**
AF22	**20**	010 **10**0		Medium **(10)**
AF23	**22**	010 **11**0		High **(11)**
CS 3	**24**	011 000	**3**	Non utilisé
AF31	**26**	011 **01**0		Low **(01)**
AF32	**28**	011 **10**0		Medium **(10)**
AF33	**30**	011 **11**0		High **(11)**
CS 4	**32**	101 000	**4**	Non utilisé
AF41	**34**	100 **01**0		Low **(01)**
AF42	**36**	100 **10**0		Medium **(10)**
AF43	**38**	100 **11**0		High **(11)**
EF	**46**	101 **11**0	**5**	
CS 6	**48**	110 000	**6**	Réservé
CS 7	**56**	111 000	**7**	Réservé

Tableau II. 3 : DSCP/IPP

❖ **Classification et marquage du trafic :**

Sur le plan conceptuel, la QoS DiffServ comporte trois étapes :

1. Le trafic doit être identifié puis classé en groupes.
2. Le trafic doit être marqué sur les limites de confiance (Bordures du réseau).
3. Des stratégies doivent être créées pour décrire le PHB et cela pour un trafic classifié.

DiffServ QoS compte sur la classification du trafic pour fournir des niveaux différenciés de service basés sur le comportement par saut. Le trafic peut être classifié sur la base d'une large variété de critères appelés descripteurs de trafic qui incluent :

- Type d'application
- Adresse IP source ou de destination
- Interface entrante
- Valeur de classe de service (CoS : Class of Service) dans un en-tête Ethernet
- Valeur du type de service (ToS) dans un en-tête IP (IP Precedence ou DSCP)
- Valeur MPLS EXP (Experimental Bits) dans un en-tête MPLS

Les listes d'accès peuvent être utilisées pour identifier le trafic à classer, sur la base des adresses ou ports. Cependant, une solution plus robuste est celle basée sur le réseau de Cisco.
Le NBAR (Network Based Application Recognition) qui reconnaîtra de manière dynamique les applications standards ou personnalisées et qui peut classifier en fonction de la charge utile (payload).
Une fois la classification effectuée, le trafic doit être marqué pour indiquer le niveau requis de service QoS pour ce trafic. Le marquage peut apparaître dans l'en-tête de couche 2 ou dans l'en-tête de couche 3. Le point du réseau où le trafic est classifié et marqué et appelé limite de confiance (Trusted). Les marques de qualité de service provenant de l'extérieur de cette limite doivent être considérées comme non fiables (Untrusted) et supprimées ou modifiées. En règle générale, le trafic doit être marqué le plus près possible de la source. Dans les environnements VoIP, ceci est souvent réalisé sur le téléphone VoIP lui-même.
Note importante : La classification du trafic ne doit pas se produire dans le cœur du réseau.

II.6 Mode d'implémentation de la QoS

II.6.1 Auto QoS

AutoQoS est une fonctionnalité à valeur ajoutée de Cisco IOS. Une fois activée sur un périphérique, AutoQoS génère automatiquement des commandes de configuration QoS pour le périphérique. La version initiale d'AutoQoS (Auto QoS VoIP) s'est concentrée sur la génération de commandes permettant de préparer le périphérique à la téléphonie VoIP et IP.
Plus tard, la fonctionnalité AutoQoS Discovery a été introduite. La prochaine génération d'AutoQoS qui tire parti de la découverte AutoQoS s'appelle AutoQoS pour l'entreprise. Comme son nom l'indique, AutoQoS Discovery analyse le trafic réseau en direct aussi longtemps que nous le laissons fonctionner et génère des classes de trafic en fonction du trafic qu'elle a traité. Ensuite, nous activons la fonctionnalité AutoQoS.
AutoQoS utilise les classes de trafic (mappes de classes) formées par AutoQoS Discovery pour générer une stratégie QoS réseau (mappe de stratégie) et applique cette stratégie. En fonction du type d'interface, AutoQoS peut également ajouter des fonctionnalités telles que la fragmentation et l'entrelacement (LFI), les liaisons multiples et la mise en forme du trafic à la configuration de l'interface.

II.6.2 Modular QoS CLI

Cisco a introduit MQC pour remédier aux faiblesses de la CLI (Command Line Interface) existante et permettre l'utilisation des outils et fonctionnalités QoS les plus récents disponibles dans le Cisco IOS moderne. Avec la MQC, la classification du trafic et la définition de la politique sont effectuées séparément. Les politiques de trafic sont définies en fonction des classes de trafic. Différentes règles peuvent faire référence aux mêmes classes de trafic, tirant ainsi parti du code modulaire et réutilisable. Lorsqu'une ou plusieurs stratégies sont définies, nous pouvons les appliquer à de nombreuses interfaces, favorisant ainsi la cohérence et la réutilisation du code. [4]

Le **Tableau II.4** ci-dessous représente une comparaison entre les modes MQC et AutoQoS.

	Modular QoS CLI	**AutoQoS**
Utilisation	Facile	Simple
Temps d'implémentation	Moyenne	Courte
Modularité	Excellente	Excellente
Tuning	Excellente	Excellente
Apprentissage	Non	Oui

Tableau II. 4 : Comparaison MQC / AutoQoS

II.7 Gestion de la congestion

La gestion de la congestion est un terme général qui englobe différents types de stratégies de mise en file d'attente utilisées pour gérer les situations dans lesquelles les demandes de bande passante des applications réseau dépassent la bande passante totale pouvant être fournie par le réseau. La gestion de la congestion ne contrôle pas la congestion avant qu'elle ne survienne. Elle contrôle l'injection de trafic dans le réseau afin que certains flux du réseau soient prioritaires sur d'autres. Dans cette section, les techniques les plus élémentaires de gestion de la file d'attente pour la gestion de la congestion seront abordées à un niveau élevé. [7] Nous examinerons les techniques de gestion de la congestion suivantes :

- First in First Out Queuing (FIFO)
- Priority Queuing
- Custom Queuing
- Weighted Fair Queuing (WFQ)
- Class Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)

Plusieurs de ces stratégies de mise en file d'attente sont appliquées dans une situation où le trafic sortant d'une interface du routeur dépasse la bande passante du port de sortie et doit être hiérarchisé. Priority et Custom Queuing nécessitent une planification de base de la part de l'administration du réseau pour être correctement implémentée et configurée sur le routeur. L'administrateur réseau doit bien comprendre les flux de trafic et la hiérarchisation de ce dernier pour servir une stratégie de file d'attente efficace. Une hiérarchisation mal planifiée peut conduire à des situations plus graves que l'état congestif lui-même. [7]
La FIFO et la WFQ, d'autre part, nécessitent très peu de configuration pour fonctionner correctement.
Dans Cisco IOS, WFQ est activé par défaut sur les liaisons de vitesse E1 (2,048 Mbps) ou plus lente.
Inversement, la FIFO est activée par défaut sur les liaisons plus rapides que les vitesses E1.

❖ Algorithmes de file d'attente :

À l'intérieur du routeur, nous avons des files de logiciels (Software) dans lesquelles les paquets peuvent attendre avant d'entrer dans l'interface pour sortir par une seule file matérielle (Hardware) qui utilise l'algorithme de mise en file d'attente FIFO.
La file d'attente logicielle peut être modifiée et gérée conformément aux algorithmes de mise en file d'attente QoS que nous utilisons. Les routeurs déterminent la longueur de la file d'attente matérielle en fonction de la bande passante configurée de l'interface.

II.7.1 First in first out Queuing

La forme par défaut de mise en file d'attente sur presque toutes les interfaces est First-In First-Out. (FIFO). Cette forme de mise en file d'attente ne nécessite aucune configuration, et simplement traite et transmet les paquets dans leur ordre d'arrivée. Si la file d'attente devient saturée, de nouveaux paquets seront supprimés (chute de la queue / Tail Drop). Cette forme de file d'attente peut être insuffisante pour les applications en temps réel (RTP), surtout en période de congestion. Le FIFO ne discréditera jamais ni ne donnera préférence aux paquets de priorité supérieure. Ainsi, des applications telles que la VoIP peuvent être affamés pendant les périodes de congestion. [2]

La **Figure II.3** explique le fonctionnement de la file d'attende FIFO.

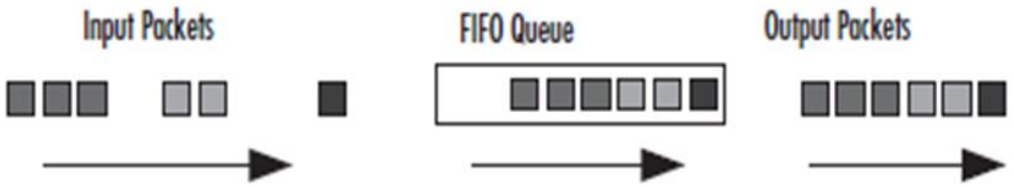

Figure II. 3 : La file d'attende FIFO [8]

II.7.2 Priority Queuing

La mise en file d'attente de priorité (PQ) est une technique de gestion de la congestion. PQ planifie le trafic de sorte que les files d'attente de priorité supérieure "toujours" soient traitées en premier. Cela peut entraîner l'affaiblissement du trafic des autres files d'attente moins prioritaires. PQ utilise 4 files d'attente différentes - Haute, Moyenne, Normale et Basse.

Si un paquet est en attente dans la file haute, le planificateur le traitera en premier. S'il n'y a pas de paquet dans la file d'attente élevée, le planificateur cherchera à traiter la file d'attente moyenne. Il faudra un paquet de la file d'attente moyenne, puis à nouveau rechercher tous les paquets en attente dans la file d'attente haute. La file d'attente basse n'est traitée que s'il n'y a pas de paquets en attente dans les files d'attente haute, moyenne et normale.

Les paquets en PQ peuvent être classés en fonction du type de protocole, interface entrante, taille de paquet et les fragments et ACL. [2]

PQ enverra les paquets de la file d'attente 1 jusqu'à ce qu'elle soit vide, puis procédera de même pour la file d'attente 2, et ainsi de suite jusqu'à la file 4. Une garantie de prévention de retard à mais pour une file seulement. Cependant, il n'existe pas de garantie de bande passante.

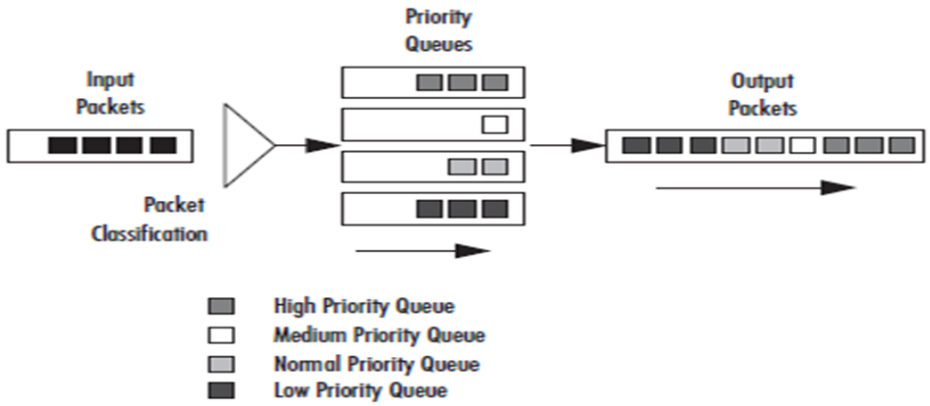

Figure II. 4 : La file d'attende Priority Queuing [8]

La **Figure II. 4** explique le fonctionnement de la file d'attende PQ.

II.7.3 Custom Queuing

La mise en file d'attente (CQ) est une forme moins stricte de mise en file d'attente, qui utilise une méthodologie pondérée de file d'attente à la ronde. Chaque file d'attente est traitée dans l'ordre, mais chaque file d'attente peut avoir un poids différent ou taille (mesurée en octets ou en nombre de paquets). Chaque file d'attente traite tout son contenu à son tour. CQ prend en charge un maximum de 16 files d'attente. La **Figure II.5** explique le fonctionnement de la file d'attende CQ avec un nombre d'octets personnalisé (Custom Byte Count).

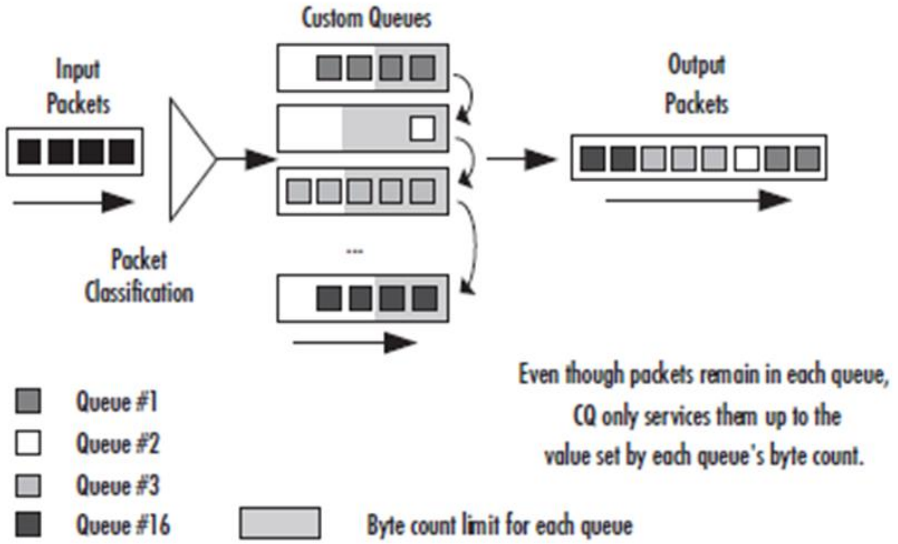

Figure II. 5 : La file d'attende Custom Queuing [8]

Cet algorithme (CQ) se divise en deux types :

1. Round Robin RR
2. Weighted Round Robin WRR

Aucune garantie de retard. Or, la garantie de bande passante peut être garantie en déterminant le nombre d'octets envoyés dans la file d'attente.

a) Round Robin (RR)

Les paquets sortent de chaque file d'attente de la même manière, ce qui signifie qu'un paquet sort de la file d'attente 1, un paquet sort de la file d'attente 2 et ainsi de suite jusqu'à la file 3, puis redémarre à partir de la file d'attente 1. La **Figure II.6** explique le fonctionnement de cette file d'attende.

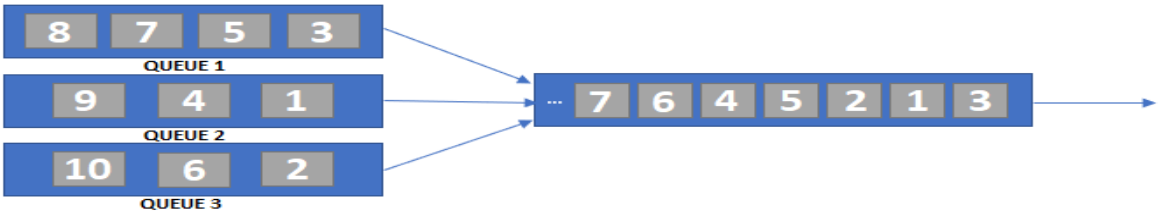

Figure II. 6 : La file d'attente Round Robin

b) Weighted Round Robin (WRR)

Il fonctionne comme RR mais nous allons donner du poids (Weight) à chaque file d'attente. Trois paquets sortent de la file 1, deux paquets sortent de la file 2, un paquet de la file 3, puis repartent de la file 1. La **Figure II.7** explique le fonctionnement de la file d'attende WRR.

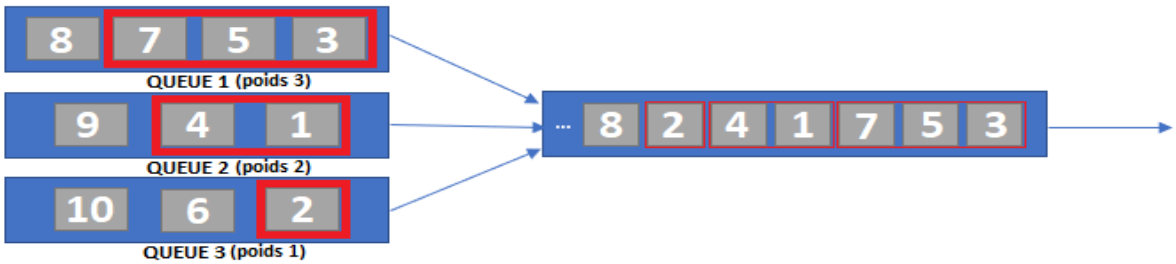

Figure II. 7 : La file d'attente Weighted Round Robin

II.7.4 Flow-based weighted fair Queuing

Weighted Fair Queuing (WFQ) crée de manière dynamique des files d'attente basées sur les flux de trafic. Les flux de trafic sont identifiés avec une valeur de hachage générée à partir des champs d'en-tête suivants :

- Adresse IP source et de destination
- Port TCP source (ou UDP)
- Numéro de protocole IP
- Valeur du type de service (IP Precedence ou DSCP) [2]

Les trafics du même flux sont placés dans la même file d'attente. Par défaut, un maximum de 256 files d'attente peut exister, bien que cela puisse être augmenté à 4096. Si la priorité (basée sur le champ ToS) de tous les paquets est la même, la bande passante est divisé également entre toutes les files d'attente. Cela se traduit par des flux à faible trafic avec un minimum de retard, alors que des flux de trafic élevés peuvent connaître une latence. Les paquets avec une priorité supérieure sont planifiés avant les paquets de priorité inférieure arrivés en même temps. Ceci est accompli en assignant une séquence numéro à chaque paquet qui arrive, calculé à partir de la dernière séquence nombre multiplié par un poids inverse (basé sur le champ ToS). En d'autres mots, une valeur de ToS plus élevée donne un numéro de séquence inférieur, et les paquets de priorité supérieure seront traités en premier. [7]

La **Figure II. 8** explique le fonctionnement de la file d'attende WFQ.

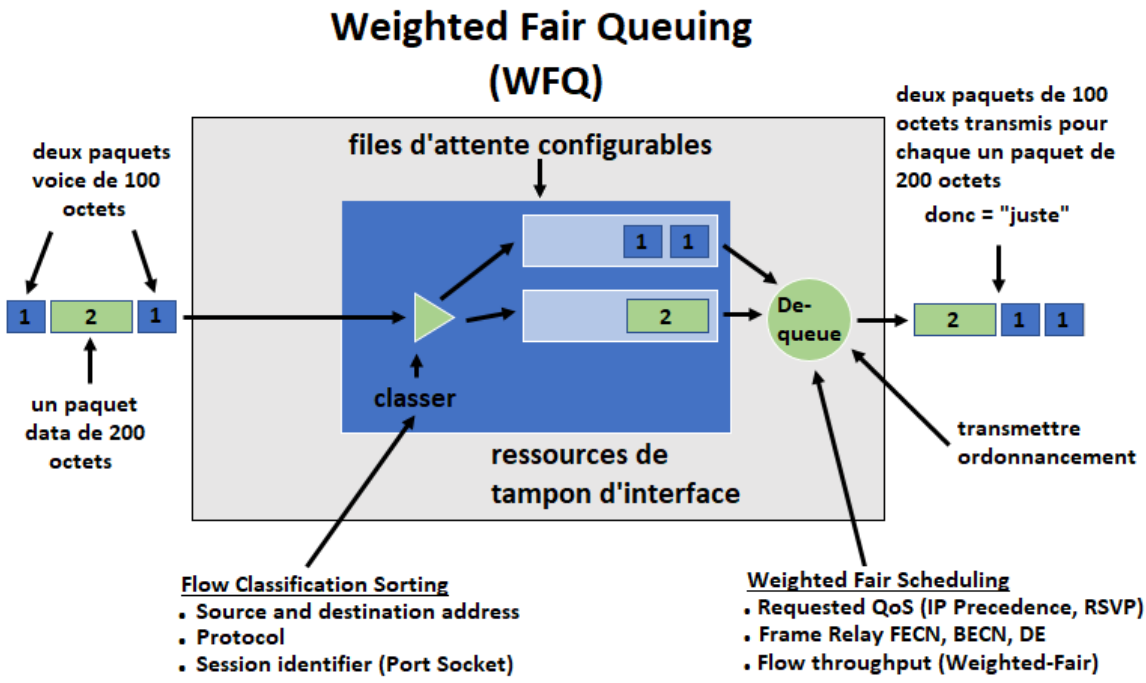

Figure II. 8 : La file d'attente Weighted Fair Queuing

Dans cet exemple, nous avons deux différents paquets : Voix et Data.
Paquet Data= 200 Octets.
Paquet Voix= 100 Octets.
Le WFQ va les traiter selon le poids le plus faible, et comme la voix est la plus importante, il va la classifier dans la première queue. Puis, le paquet Information (Data) sera de suite classifier dans la deuxième queue. Mais en prenant en considération la taille des deux différents paquets. La condition implique qu'il ait une équivalence entre les deux différents paquets. Le WFQ envoie deux paquets Voix et un paquet Data en respectant la priorité des types de paquets.

❖ **Principe du WFQ :**

Le WFQ peut être défini par les caractéristiques suivantes :

- Il crée 8 files d'attente de paquets système, 1000 files d'attente pour RSVP, 256 files d'attente dynamiques, de 16 à 4096 files d'attente par flux (conversations).
- Il donne la priorité aux locuteurs avec de petites quantités de données que les locuteurs avec de grandes quantités de données.
- Introduit pour résoudre les problèmes avec FIFO & PQ
- Ne supporte pas le cryptage ou le tunneling.
- C'est la valeur par défaut pour les interfaces série, elle n'est prise en charge que sur les liaisons inférieures ou égales à 2 Mo.
- Aucune garantie de retard.
- Aucune garantie de bande passante. [2]

II.7.5 Class-Based weighted fair Queuing

WFQ souffre de plusieurs inconvénients clés :

- Le trafic ne peut pas être mis en file d'attente en fonction de classes définies par l'utilisateur.
- WFQ ne peut pas fournir de garanties de bande passante spécifiques à un flux de trafic.
- WFQ n'est pris en charge que sur des liaisons plus lentes (2,048 Mbps ou moins).
- Ces limitations ont été corrigées avec WFQ basé sur les classes (CBWFQ). [7]

CBWFQ fournit jusqu'à 64 files d'attente définies par l'utilisateur. Le trafic dans chaque file est traité avec FIFO. Chaque file d'attente est dotée d'un minimum configurable garantie de bande passante, qui peut être représentée de trois façons :

1. Sous forme de montant fixe (en utilisant la commande Bandwidth).
2. En pourcentage de la bande passante totale de l'interface (à l'aide de la commande bande passante pour cent).
3. En pourcentage de la bande passante non allouée restante (à l'aide de la commande de pourcentage de bande passante restante). [7]

Les files d'attente CBWFQ ne sont tenues de respecter leur garantie minimale de bande passante que pendant les périodes d'encombrement et peuvent donc dépasser ce minimum lorsque la bande passante est disponible. La **Figure II. 9** explique le fonctionnement de la file d'attende CBWFQ.

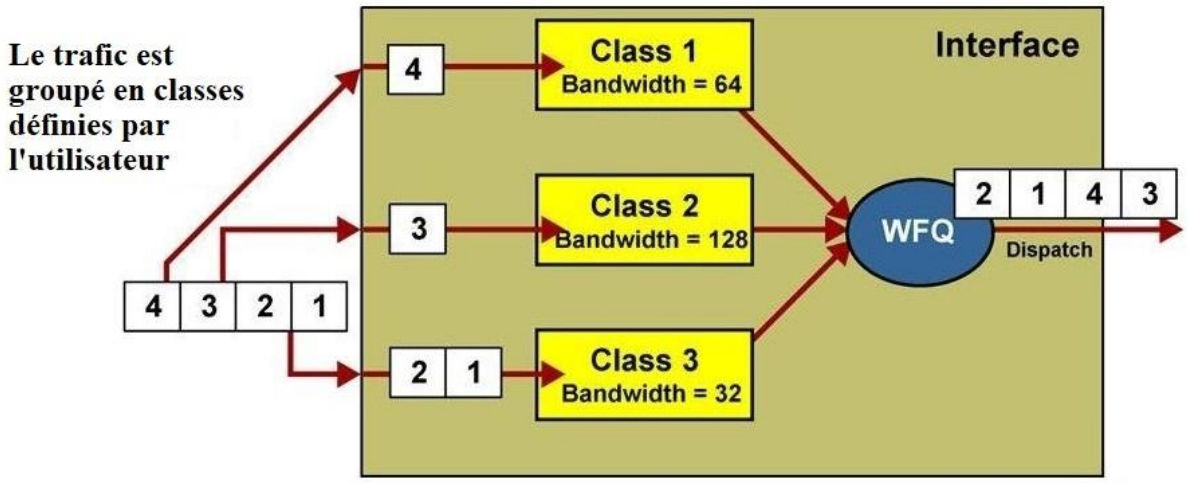

Figure II. 9 : La file d'attente Class Based Weighted Fair Queuing

II.7.6 Low-latency Queuing

La section précédente a démontré que CBWFQ peut donner des garanties de bande passante à différentes classes de trafic. Bien que CBWFQ puisse fournir ces garanties de bande passante, une transmission à faible temps de latence peut ne pas être fournie aux paquets dans des situations de congestion, car tous les paquets sont transmis équitablement en fonction de leur poids. Cela peut poser des problèmes pour des applications telles que la VoIP sensibles aux retards, notamment les variations dans les retards. La variation du temps de retard entre les paquets individuels qui constituent un flux de voix est généralement appelée Gigue. Bien que la plupart des applications vocales puissent tolérer un certain délai, la gigue peut causer des saccades dans les transmissions vocales et dégrader rapidement la qualité globale de la voix. La mise en file d'attente à faible latence (LLQ) étend CBWFQ pour inclure la possibilité de créer une file d'attente à priorité stricte. La mise en file d'attente à priorité stricte permet une transmission à faible temps de latence vers des applications à débit constant (CBR : Constant Bit Rate) telles que la voix. [4]

- **Comment fonctionne LLQ ?**

Une fois que nous savons comment fonctionne CBWFQ, LLQ est facile à comprendre. LLQ crée une priorité stricte que nous pouvons imaginer reposer sur toutes les autres queues. Cette priorité est vidée avant toute autre file d'attente. Une priorité stricte est souvent appelée une file d'attente exhaustive, car les paquets continuent d'être retirés de la file d'attente et transmis jusqu'à ce qu'elle soit vide. Ce n'est que lorsque la file d'attente à priorité stricte est totalement vide que les autres files d'attente sont desservies dans l'ordre déterminé par la pondération configurée des instructions de bande passante CBWFQ.

Si des paquets entrent dans la file d'attente prioritaire alors qu'une autre file d'attente est en cours de traitement, les paquets en attente dans la file d'attente prioritaire seront les prochains paquets envoyés à l'interface, après la transmission du paquet actuel.

De cette manière, le délai entre les paquets envoyés à partir de la file d'attente prioritaire est minimisé et un service à faible latence est fourni. Le délai maximum entre les paquets prioritaires arrivant à l'extrémité distante se produit dans le cas où un paquet arrive dans la file d'attente prioritaire précédemment vide dès que le routeur commence à transmettre un paquet volumineux. Le plus grand paquet possible est appelé unité de transmission maximale (MTU), soit 1 500 octets sur Ethernet.

Le paquet prioritaire devra attendre la fin du paquet non prioritaire. Ainsi, le délai le plus long possible entre les paquets de priorité entrants est limité au temps de sérialisation du MTU plus le temps de sérialisation du paquet de priorité lui-même.

Le temps de sérialisation est calculé par : $\frac{\textbf{Taille du paquet}}{\textbf{Vitesse de la liaison}}$

La **Figure II. 10** explique le fonctionnement de la file d'attente LLQ qui est un ensemble des deux algorithmes PQ+CBWFQ.

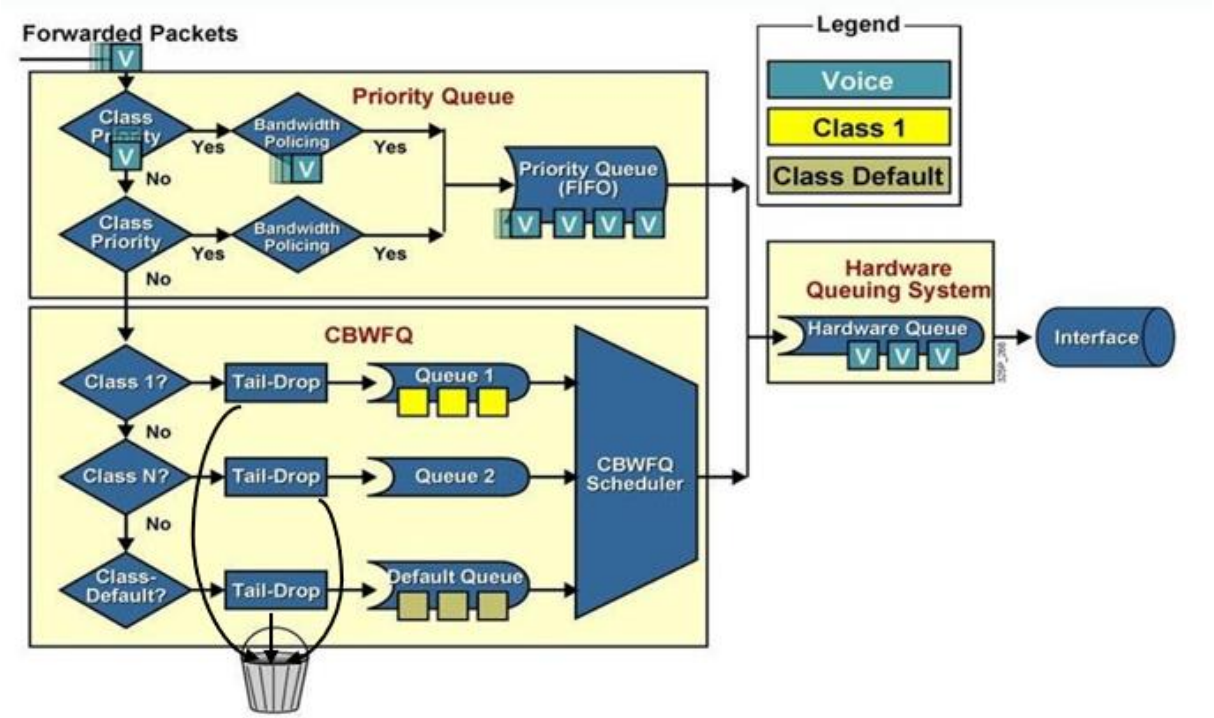

Figure II. 10 : Architecture LLQ

Après cette étude sur l'algorithme LLQ, on peut le simplifier par les caractéristiques suivantes :

- LLQ c'est tout simplement CBWFQ mais nous ajoutons un fichier d'attente prioritaire à CBWFQ pour un trafic en temps réel tel que la VOIP, c'est pourquoi il est préféré pour la VoIP.
- Nous aurons donc 1 PQ avec une priorité élevée et des fichiers d'attente restants seront CBWFQ avec une priorité inférieure.
- Garantie de délai dans le fichier d'attente PQ, Garantie de bande passante.
- Peut fonctionner avec tout type de support, y compris les supports série et Ethernet, etc.
- Un courrier prioritaire en cas de congestion.
- Les classes sont contrôlées et la limite du taux individuel.

II.8 Outils d'évitement de la congestion

II.8.1 Buckets

a Leaky Bucket (Seau percé)

Le seau percé (Leaky Bucket) est un concept clé pour comprendre la théorie de la mise en file d'attente. Une file d'attente réseau peut être comparée à un seau dans lequel les paquets du réseau sont versés. Le seau comporte un trou au bas qui permet aux paquets de s'écouler à un débit constant.

Dans un environnement réseau, le taux d'égouttement (Drip Rate) correspond à la vitesse de l'interface desservie par cette file d'attente ou ce compartiment. Si les paquets tombent dans le seau plus rapidement que le trou ne peut les laisser s'écouler, le seau se remplit lentement. Si trop de paquets tombent dans le seau, celui-ci peut éventuellement déborder. Ces paquets sont perdus car ils ne s'écoulent pas hors du seau. [8]

La **Figure II.11** illustre l'analogie avec un seau qui fuit. Ce mécanisme est bien adapté pour gérer un trafic réseau trop important. Si les paquets tombent par paquets, le seau se remplit et fuit lentement à une vitesse constante. De cette façon, la vitesse à laquelle les paquets tombent dans le seau n'est pas importante tant que le seau lui-même peut les contenir. Cette analogie est utilisée pour décrire les files d'attente réseau. Les paquets entrent dans une file d'attente à un débit donné, mais la quittent à un débit constant, qui ne peut pas dépasser la vitesse de l'interface de sortie.

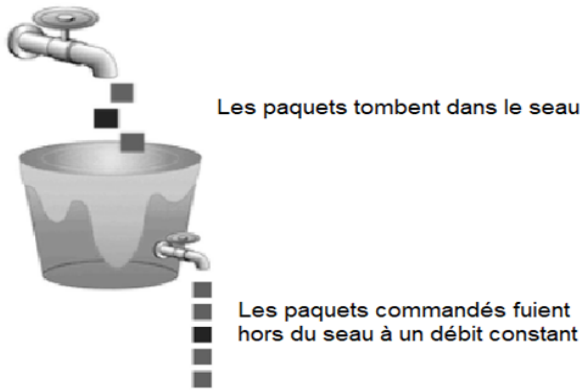

Figure II. 11 : Fuite du seau

b Token Bucket (Seau à jetons)

Le seau à jetons est un autre mécanisme utilisé dans QoS. Il représente un pool de ressources pouvant être utilisées par un service à tout moment. Contrairement au seau percé (Leaky Bucket), le seau à jetons ne laisse rien couler par le bas. Ce qui se passe dans le seau doit sortir par le haut. Au fil du temps, les jetons sont ajoutés au compartiment par le réseau. Lorsqu'une application doit envoyer quelque chose au réseau, elle doit supprimer le nombre de jetons égal à la quantité de données qu'il lui faut transmettre. S'il n'y a pas assez de jetons dans le seau, l'application doit attendre que le réseau ajoute d'autres jetons au compartiment. Si l'application n'utilise pas ses jetons, celui-ci peut éventuellement déborder.

Les jetons renversés sont alors perdus et l'application ne peut pas les utiliser. Cela signifie que chaque seau de jetons a une capacité de jeton maximale clairement définie.

Les seaux à jetons sont utilisés dans la mise en forme du trafic (Trafic Shaping) et dans d'autres applications où le trafic se produit en rafales.
Le seau à jetons autorise les rafales en permettant à l'application de supprimer un grand nombre de jetons de son compartiment pour envoyer des informations, mais limite la taille de ces rafales en ne permettant qu'un certain nombre de jetons dans le seau.

II.8.2 Tail drop

Que se passe-t-il quand le seau se remplit ? Bien sûr, lorsqu'il s'agit de files d'attente réseau, une certaine quantité de mémoire du routeur est allouée à ces seaux. Cela signifie que ces files d'attente ne sont pas infinies. Elles ne peuvent contenir qu'une quantité d'informations prédéterminée. Les administrateurs réseau peuvent normalement configurer les tailles de file d'attente si nécessaire, mais l'IOS (Cisco Inter network Operating System) permet normalement des valeurs de taille de file d'attente par défaut assez équilibrées.
Lorsqu'une file d'attente est saturée, les paquets sont placés dans la file d'attente dans l'ordre où ils ont été reçus. Lorsque le nombre de paquets entrés dans la file d'attente dépasse la capacité de la file d'attente pour les contenir, le seau déborde. Dans la terminologie de mise en file d'attente, la file d'attente subit une perte de charge. Ces pertes de queue représentent des paquets qui ne sont jamais entrés dans la file d'attente. Elles sont simplement rejetées par le routeur.
Les protocoles de couche supérieure utilisent leur processus d'accusé de réception et de retransmission pour détecter ces paquets abandonnés et les retransmettent. Les abandons en queue ne sont pas une indication directe d'un dysfonctionnement du réseau. [8]
Par exemple, il est normal qu'une interface FastEthernet à 100 Mbps envoie trop d'informations à une interface T1 à 1,544 Mbps. Ces paquets abandonnés sont souvent utilisés par les protocoles de couche supérieure pour limiter le débit d'envoi d'informations au routeur. Certains mécanismes de QoS tels que la détection précoce aléatoire (RED) et la détection précoce aléatoire pondérée (WRED) utilisent ces principes pour contrôler le niveau de congestion du réseau. [8]
Les chutes de queue peuvent évidemment avoir un impact sur la réponse de l'utilisateur. Les paquets perdus entraînent des demandes de retransmission. Avec de plus en plus d'applications utilisant le protocole TCP / IP, les chutes automatiques peuvent également introduire un autre phénomène appelé synchronisation globale. La synchronisation globale provient de l'interaction d'un mécanisme de couche supérieure de TCP / IP appelé fenêtre glissante (sliding window).
En termes simples, la fenêtre de transmission d'une communication TPC/IP unique représente le nombre de paquets que l'expéditeur peut transmettre dans chaque bloc de transmission. Si le bloc est envoyé avec succès sans erreur, la taille de la fenêtre "glisse" vers le haut, ce qui permet à l'expéditeur de transmettre plus de paquets par intervalle. Si une erreur survient dans la transmission, la taille de la fenêtre diminue progressivement.
Lorsque plusieurs conversations TCP / IP a lieu simultanément, chaque conversation augmente la taille de la fenêtre à mesure que les paquets sont transmis. En fin de compte, ces conversations utilisent toute la bande passante disponible, ce qui entraîne la perte de paquets par la file d'attente de l'interface. Ces paquets rejetés sont interprétés comme des erreurs de transmission pour toutes les conversations, ce qui réduit simultanément la taille de leur fenêtre pour envoyer moins de paquets par intervalle. [8]

Cette synchronisation globale provoque une fluctuation de l'utilisation du réseau visible dans la **Figure II.12** ci-dessous :

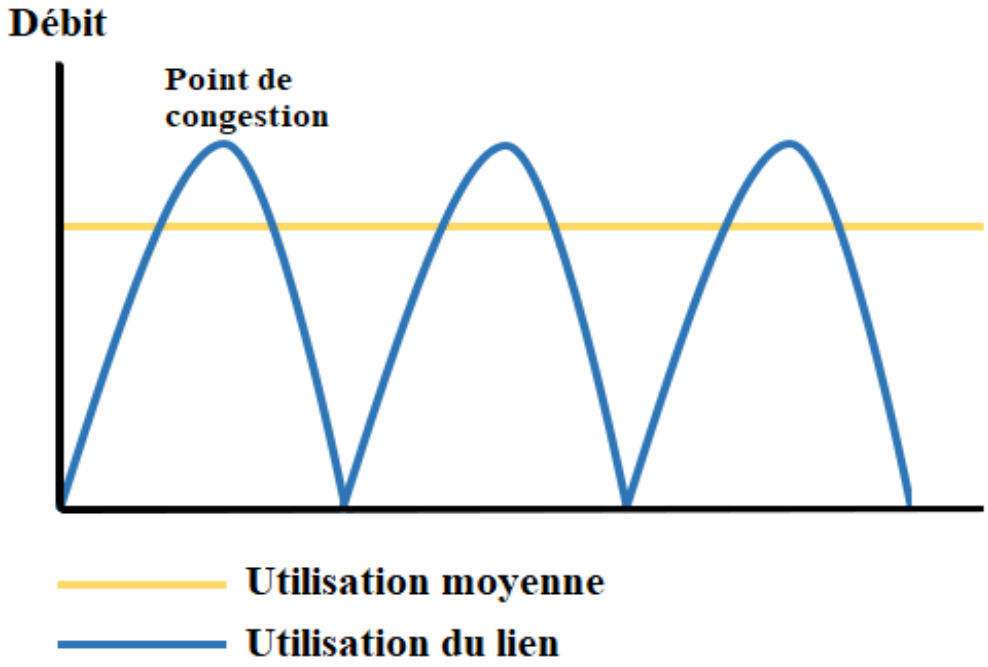

Figure II. 12 : Chute de la queue

II.8.3 Mécanismes RED, WRED

Les techniques d'évitement de congestion surveillent les charges de trafic sur le réseau afin d'anticiper et d'éviter les encombrements au niveau des goulots d'étranglement du réseau commun (Bottlenecks). L'évitement de la congestion est réalisé par la chute de paquets (Tail drop). Parmi les mécanismes les plus couramment utilisés pour éviter les encombrements, on trouve la détection aléatoire précoce (RED) qui est optimale pour les réseaux de transit à grande vitesse. La qualité de service Cisco IOS inclut une implémentation de RED qui, lorsqu'elle est configurée, contrôle le moment où le routeur supprime les paquets.

Si vous ne configurez pas la détection précoce pondérée aléatoire (WRED), le routeur utilise le mécanisme de dépôt de paquets par défaut plus grossier appelé retrait final.

a RED (Random Early Detection)

La détection aléatoire précoce est un mécanisme qui évite les situations d'encombrement en traitant les communications réseau lorsque la liaison commence à montrer les premiers signes d'encombrement. En conséquence, si RED est activé, une liaison ne doit jamais atteindre le point de congestion, car le mécanisme RED réduira le flux de paquets avant que cela ne se produise. Cela a également pour effet de normaliser l'utilisation de la bande passante d'une liaison et de la maintenir à sa capacité maximale. La **Figure II.13** représente les différents seuils de la chute.

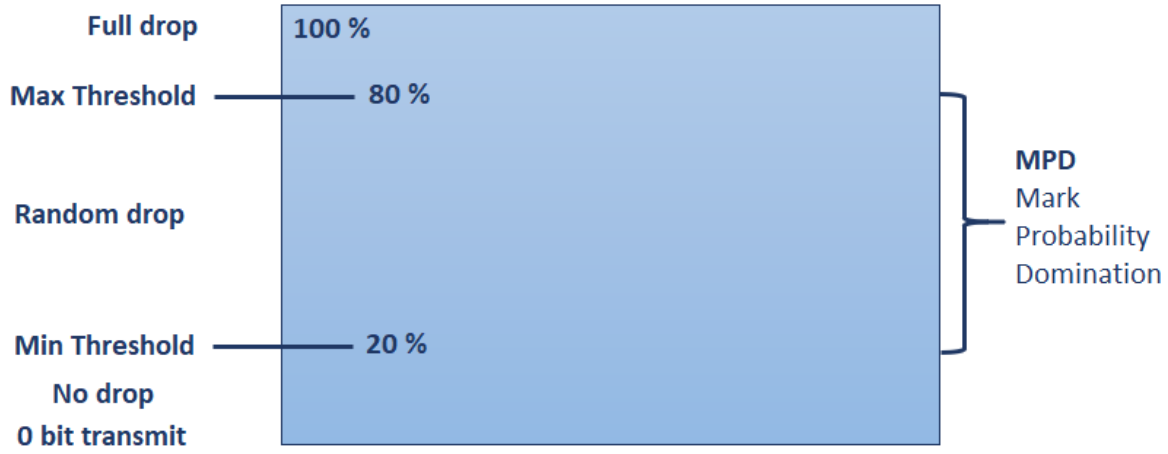

Figure II. 13 : Les différents seuils de la chute

Les trois paramètres suivants influent sur le rejet d'un paquet qui arrive :

1. Seuil minimum (Max Threshold)
2. Seuil maximum (Min Threshold)
3. Marqueur Dénominateur de Probabilités ➔MPD=$\frac{\mathbf{MaxTh}}{\mathbf{MinTh}}$

Le seuil minimum spécifie le nombre de paquets dans une file d'attente avant que celle-ci n'envisage de supprimer les paquets. La probabilité d'élimination augmente jusqu'à ce que la profondeur de la file d'attente atteigne le seuil maximal. Une fois que la profondeur de la file d'attente dépasse le seuil maximal, tous les autres paquets tentant d'entrer dans la file d'attente sont supprimés.

Cependant, la probabilité que des paquets soient ignorés lorsque la profondeur de la file d'attente est égale au seuil maximal est de 1 / (MPD). Cela est présenté dans la **Figure II.14**.

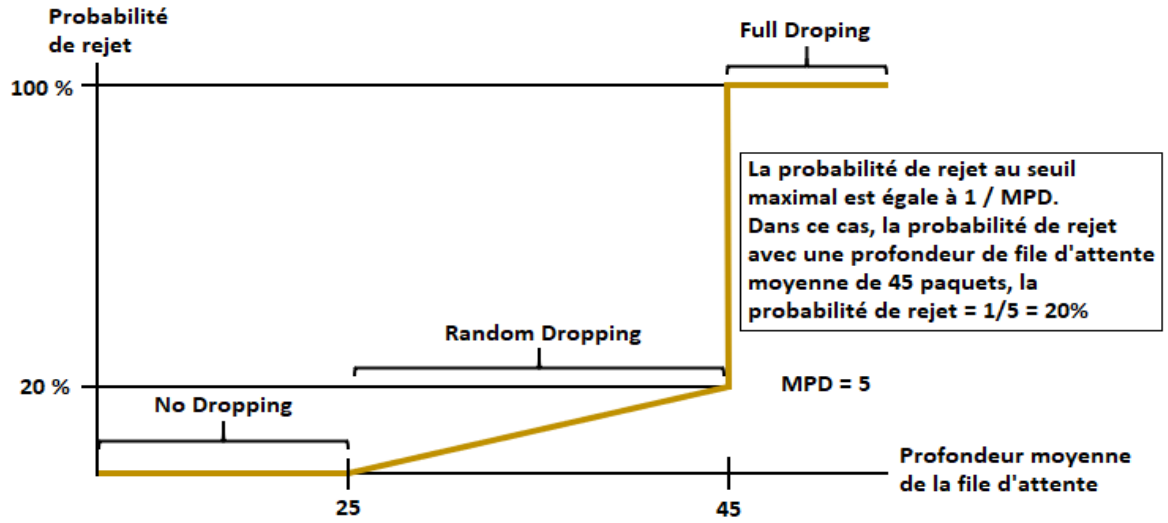

Figure II. 14 : Probabilité de la chute en RED

❖ **Comment fonctionne la détection précoce aléatoire ?**

RED fonctionne en éliminant de manière aléatoire les paquets de différentes conversations. Il utilise la fenêtre glissante de TCP / IP et des mécanismes de récupération rapide pour forcer la communication à réduire la vitesse à laquelle il transmet les paquets, réduisant ainsi l'utilisation de la bande passante pour cette conversation particulière.

En appliquant ce principe au hasard à diverses communications en cours, RED peut ralentir les choses car il détecte qu'un lien se rapproche d'un état congestif. RED n'est pas approprié dans les situations où le trafic UDP est prédominant, car RED n'a aucun effet appréciable sur dernier.

b WRED (Weighted Random Early Detection)

La détection précoce pondérée aléatoire (WRED) est une extension de l'algorithme RED afin de promouvoir une politique avec plusieurs niveaux de priorité. Un routeur fonctionnant en WRED doit posséder autant de files implémentées en RED que de niveaux de priorité désirés. Chaque file s'occupe des paquets pour lesquels elle est désignée, chaque paquet se trouve ainsi classé dans la file correspondante. On utilise fréquemment le champ TOS (Type Of Service) du header IP pour classer les paquets. Chaque file étant elle-même gérée par un module RED différent avec des valeurs différentes de minth, maxth et maxP, chacune d'elle permet une politique différente suivant la priorité du paquet. [10]

Le **Tableau II.5** ci-dessous est un exemple de la classe 1 AF (AF11, AF12, AF13), les valeurs sont choisies par l'administrateur afin de déterminer pour chaque sous-classe sa probabilité de rejet (%) et sa profondeur moyenne de la file (°).

	Minimum (%)	**Maximum (%)**	**Pourcentage de Drop (%)**
AF11	45	90	25
AF12	30	60	55
AF13	20	45	70

Tableau II. 5 : Probabilité de la chute en WRED

Le résultat du Tableau ci-dessus peut être représenté sous la forme de la **Figure II.15** suivante :

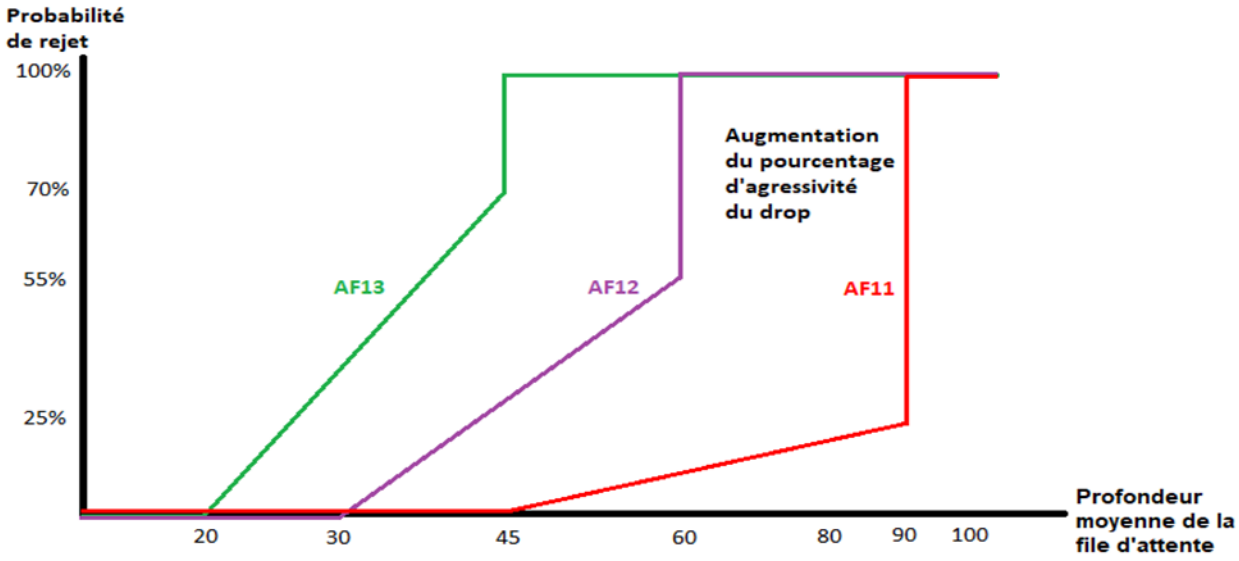

Figure II. 15 : Les profils WRED

II.8.4 Explicit Congestion Notification

La Notification explicite de congestion est définie par les points suivants :

- Le contrôle de congestion TCP n'est pas adapté aux applications sensibles au retard ou à la perte de paquets.
- ECN (défini dans le document RFC 3168) élimine la nécessité de recourir à la perte de paquets en tant qu'indicateur de congestion.
- ECN marque les paquets au lieu de les supprimer lorsque la longueur moyenne de la file d'attente dépasse une valeur de seuil spécifique.

Les routeurs et les hôtes finaux peuvent utiliser le marquage ECN pour signaler que le réseau est encombré et envoyer des paquets plus lentement. La **Figure II.16** nous montre la composition du champ Explicit Congestion Notification.

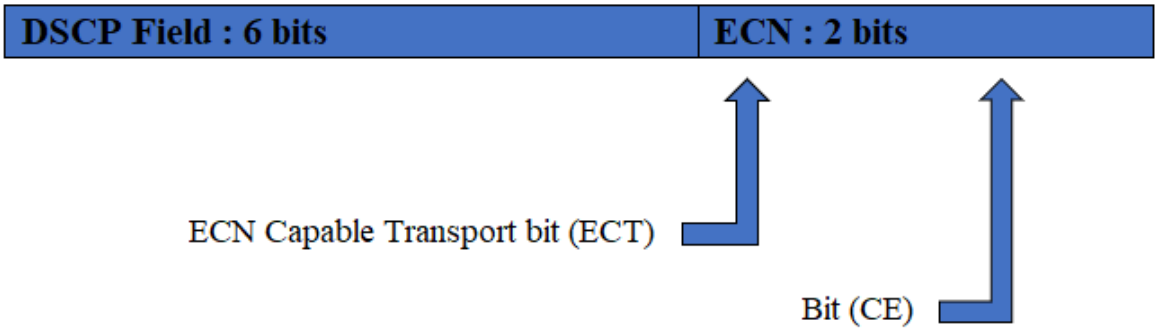

Figure II. 16 : Le champ Explicit Congestion Notification

Le **Tableau II.6** suivant représente la probabilité ECN composée d'un Bit ECT (ECN Capable Transport) et CE (Congestion Experienced). Il existe seulement deux cas pour qu'il ait un transport ECN comme démontré ci-dessous :

Bit ECT	CE Bit	Résultat
0	0	Transport non compatible ECN
0	1	ECN Capable Transport (1)
1	0	ECN Capable Transport (0)
1	1	Congestion experimentée

Tableau II. 6 : Probabilité ECN

II.9 Policing and shaping

II.9.1 Policing

La politique du trafic nous permet de contrôler le débit maximal du trafic envoyé ou reçu sur une interface et de partitionner un réseau en plusieurs niveaux de priorité ou classe de service (CoS).

La fonctionnalité de gestion du trafic gère le taux de trafic maximal via un algorithme de seau à jetons. L'algorithme de compartiment à jetons peut utiliser les valeurs configurées par l'utilisateur pour déterminer le débit maximal de trafic autorisé sur une interface à un moment donné. L'algorithme de seau à jetons est affecté par tout le trafic entrant ou sortant (selon l'endroit où la politique de trafic avec Traffic Policing est configurée) et est utile pour gérer la bande passante du réseau dans les cas où plusieurs gros paquets sont envoyés dans le même flux de trafic. [11]

a One Rate Policy

Un régulateur à double taux : Un compartiment de jetons avec deux actions pour chaque paquet (une action de conformité et une action de dépassement). La **Figure II.17** est une démonstration du Policing à un seul taux.

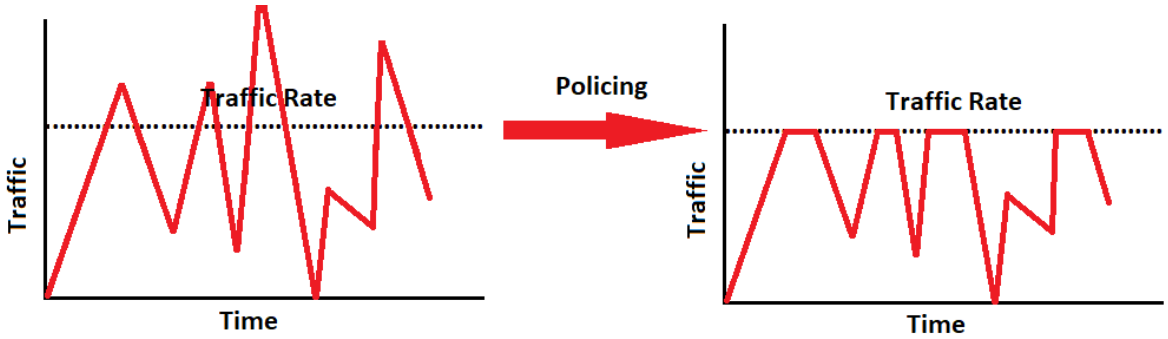

Figure II. 17 : One Rate Policing

b Two Rates Policy

Le régulateur à deux taux gère le taux de trafic maximal en utilisant deux compartiments de jetons : le compartiment de jetons engagé et le compartiment de jetons de crête.
L'algorithme de compartiment à double jeton utilise des valeurs configurées par l'utilisateur pour déterminer le débit maximal de trafic autorisé sur une file d'attente à un moment donné.
De cette manière, le régulateur à deux débits peut mesurer le trafic à deux débits indépendants :

1. Le débit d'information garanti (CIR : Committed Information Rate)
2. Le débit d'information de pointe (PIR : Peak Information Rate)

Le compartiment de jetons validé peut contenir des octets allant jusqu'à la taille de la rafale validée (bc : Committed burst) avant le débordement.
Ce compartiment de jetons contient les jetons qui déterminent si un paquet est conforme au CIR ou le dépasse, comme décrit ci-après :
• Un flux de trafic est conforme lorsque le nombre moyen d'octets sur une période donnée ne provoque pas de débordement du compartiment de jetons validé. Lorsque cela se produit, l'algorithme de compartiment à jetons marque le flux de trafic en vert.
• Un flux de trafic dépasse le seuil lorsque le compartiment de jetons engagé déborde dans le compartiment de jetons de pointe. Lorsque cela se produit, l'algorithme de compartiment à jetons marque le flux de trafic en jaune. Le compartiment de jetons de pointe est rempli tant que le trafic dépasse le taux de la police.

Le compartiment de jetons de crête peut contenir des octets jusqu'à la taille de la rafale de crête (be : Excess Burst) avant de déborder. Ce compartiment de jetons contient les jetons qui déterminent si un paquet viole le PIR. Un flux de trafic viole lorsqu'il provoque le dépassement du compartiment de jetons de crête. Lorsque cela se produit, l'algorithme de compartiment à jetons marque le flux de trafic en rouge.

L'algorithme de compartiment de jetons fournit trois actions pour chaque paquet comme le montre le **Tableau II.7** ci-dessous :

Action	Etat des paquets	
Violate action : Une action facultative de violation	**Drop :** Configurés pour être abandonnés	
Exceed action : Une action de dépassement	**Remark :** Envoyés avec une priorité réduite	**PIR :** Peak Information Rate 
Conform action : Action de conformité	**Forwarding :** Transmis	**CIR :** Committed Information Rate 

Tableau II. 7 : Two Rates Policing

La surveillance du trafic est souvent configurée sur des interfaces à la périphérie d'un réseau pour limiter le débit du trafic entrant ou sortant du réseau. Dans les configurations de gestion du trafic les plus courantes, le trafic conforme est transmis et le trafic dépassant est envoyé avec une priorité réduite ou est abandonné. Les utilisateurs peuvent modifier ces options de configuration pour répondre aux besoins de leur réseau. [11]

II.9.2 Shaping

La mise en forme du trafic nous permet de contrôler le trafic sortant d'une interface afin de l'adapter à la vitesse de l'interface cible distante et de nous assurer que le trafic est conforme aux politiques qui lui ont été contractées. La **Figure II.18** est une démonstration du Shaping ou la mise en forme.

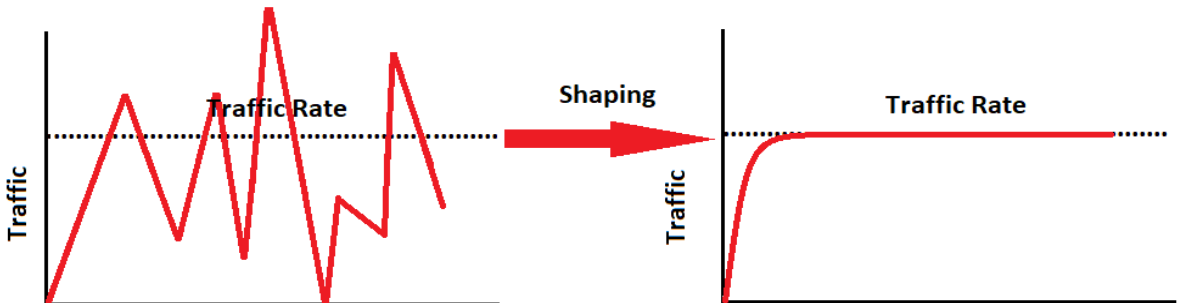

Figure II. 18 : Shaping

Ainsi, le trafic adhérant à un profil particulier peut être configuré pour répondre aux exigences en aval, éliminant ainsi les goulots d'étranglement (Bottlenecks) dans les topologies présentant des inadéquations de débit de données. [11]
Le **Tableau II.8** suivant est un tableau comparatif entre Policing et Shaping.

	Policing	**Shaping**
Direction	Direction entrante et sortante	Direction sortante uniquement
Marquage et Remarquage	Oui	Non
Utilisation de la mémoire	Moins d'utilisation de la mémoire	Nécessite un système de file d'attente de mise en forme supplémentaire

Tableau II. 8 : Comparaison Policing/Shaping

❖ **Terminologies Policing & Shaping:**

TC : Mesure du temps en millisecondes (Spécifié par ISP dans son accord avec le client).
BC (Committed Burst) : C'est la mesure en bits de la quantité totale de trafic pouvant être envoyée par TC.
BE (Excess Burst Size) : C'est le plus grand nombre de bits en bc pouvant être envoyé après une période d'arrêt.
Shaping rate : C'est la quantité de bits par seconde que nous mettons en mise en forme (Shaping).
CIR (Committed Information Rate) : C'est la vitesse de liaison du client autorisée par le ISP.
$\boldsymbol{TC = BC / Shaping\ rate}$

II.10 Efficacité du lien

C'est un mécanisme utilisé pour améliorer l'efficacité des liaisons et utiliser au maximum la bande passante qui se trouve. Il existe deux façons pour le faire :

1. **Compression**

Cela signifie simplement que la donnée est compressée pour qu'elle ait une petite taille. Or faut savoir spécialement ce qui doit être compresser. Par exemple, nous pouvons compresser les classes importantes, l'entête du paquet, Payload (Charge utile).

2. **Link Fragmentation Interleaving (Fragmentation de lien entrelacé/LFI)**

Dans le délai de sérialisation, nous pouvons voir qu'un paquet de1500 octets sort de la file d'attente matérielle et qu'il y a un paquet VOIP de 64 octets derrière.
La solution est de diviser (fragmenter) ce paquet de 1500 octets en petits paquets et placer le paquet VOIP (64 octets) juste derrière le premier petit paquet fragmenté pour pouvoir partir rapidement.

En conséquence, nous devons réécrire les en-têtes, il est donc préférable de l'utiliser avec des liens lents = ou inférieurs à 768kbps.
Si la largeur de bande de liaison est supérieure à cela, l'utilisation de LFI sera considérée comme une efficacité anti-liaison. La **Figure II.19** explique comment travaille LFI.

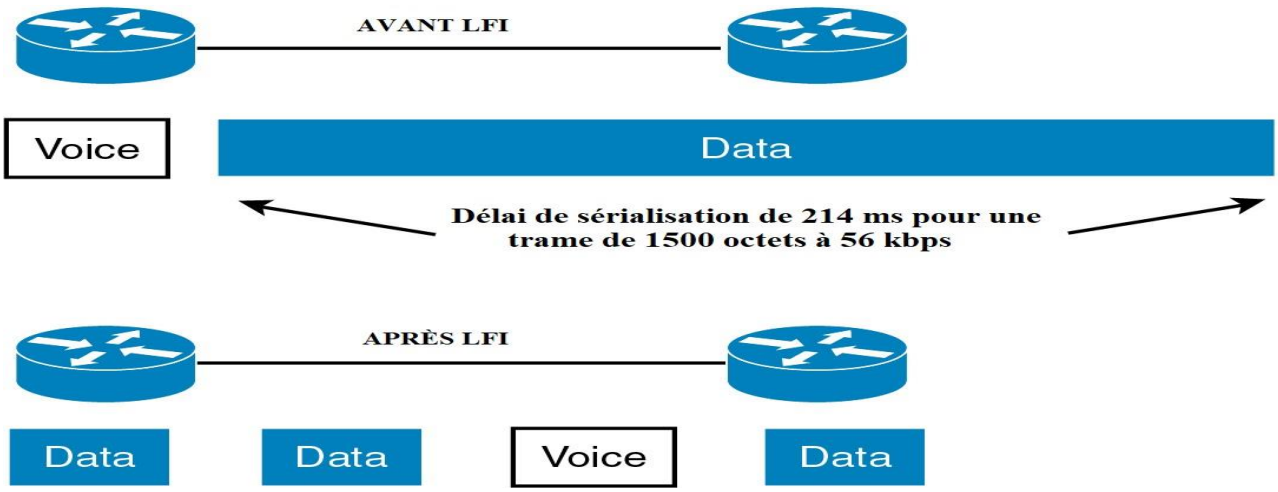

Figure II. 19 : Link Fragmentation and Interleaving

❖ **P2P App (Peer to Peer Applications):**

Un réseau pair-à-pair dans lequel les nœuds interconnectés "pairs" partagent les ressources entre eux sans avoir recours à un système administratif centralisé comme le montre la **Figure II.20** ci-dessous :

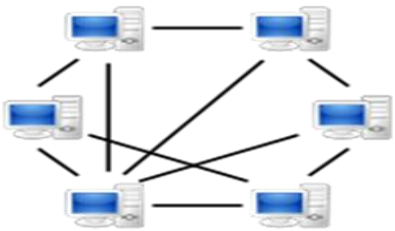

Figure II. 20 : Un réseau pair-à-pair

II.11 Conclusion

Dans ce chapitre, nous avons décrit les bases théoriques de la Qualité de Service, à savoir sa définition, son principe et aussi une présentation des modèles. Ce chapitre relève ainsi d'une utilité majeure pour ce qui suit puisqu'il détaille des notions exploitées dans la phase de la mise en place de notre projet. Dans le prochain chapitre, nous allons implémenter la qualité de service dans une entité professionnelle.

CHAPITRE III

Implémentation de la QoS

III.1 Définition et présentation de l'entreprise ICT-Towers

III.1.1 Introduction

Dans le cadre de notre dernière année d'ingénierie en Réseaux de Télécommunications à l'université de Aboubakr Belkaid Tlemcen, nous avons effectué un stage de fin d'études d'une durée de 2 mois. Ce stage vise à clôturer notre cursus. Il nous a permis d'être formés au sein d'une entreprise dans le but d'acquérir des connaissances sur le secteur d'activité, tout en permettant de mettre en pratique les connaissances théoriques ainsi que pratiques lors de notre cursus. Dans ce dernier chapitre, nous présentons l'environnement de travail ainsi que la mission principale qu'on a réalisé au sein de la société ICT-Towers, à savoir la réalisation de la qualité de service. La **Figure III.1** représente le logo de cette entité.

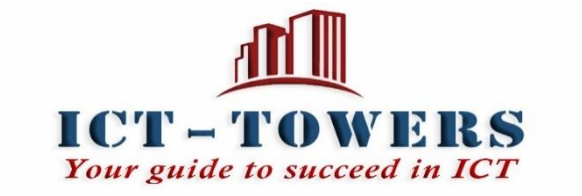

Figure III. 1 : Logo de l'entreprise ICT-Towers

III.1.2 Présentation de la société

ICT Towers est une société mère 100% Algérienne et entièrement indépendante (non franchisée). Fondée en 2014 par Monsieur A. Bachir Bouiadjra, située à Sidi Belabess et Alger. Elle réunit un ensemble varié d'experts des nouvelles technologies de l'information et de la communication NTIC disposant de l'expérience professionnelle et des compétences requises pour en faire un pôle d'expertise, d'excellence, et d'innovation dans le domaine des TIC.
ICT Towers contribue au développement du niveau d'expertise du personnel NTIC et assiste les entreprises lors de l'implémentation des différentes solutions NTIC ; à leur fournir les meilleurs conseils et recommandations afin d'assurer non seulement leur utilité et utilisabilité, mais aussi un niveau très élevé de leur performance, fiabilité, sécurité, haute disponibilité, et évolutivité.

III.1.3 Les activités d'ICT Towers

Les activités d'ICT-Towers peuvent se découper en trois entités différentes :

1. Les formations et le transfert de compétences.
2. Le consulting et le déploiement des solutions.
3. La recherche et le développement des solutions.

a Formation et Transfert de Compétences

ICT-Towers accorde une importance particulière à la participation et à l'amélioration du capital humain qui recouvre l'ensemble des connaissances, qualifications, compétences et caractéristiques individuelles.

b Audit et conseil

Les experts-auditeurs de ICT-Towers interviennent périodiquement sur le terrain (chacun dans son domaine de spécialité), à travers les différentes étapes liées au cycle de vie des solutions du domaine des NTIC. L'objectif est de préserver et surtout d'améliorer continuellement leur niveau d'expertise au double plan théorique et pratique.

L'objectif étant d'offrir à leurs clients le plus riche « Portefeuille de Services » lié aux différents champs mentionnés ci-dessous, selon la classification suivante :

Ingénierie : Spécification des besoins, dimensionnement & architecture, étude comparative des différentes solutions.

Réalisation : Préparation & planification, implémentation & déploiement, test & évaluation, documentation.

Support : Maintenance & dépannage, supervision & reporting, assistance & support.

Audit : Évaluation organisationnelle, évaluation physique et architecturale, évaluation de la commutation et du routage, évaluation du management et de la supervision, évaluation de la sécurité et de la haute disponibilité, évaluation de la qualité et de la performance.

La **Figure III.2** représente les entreprises et les entités qui ont fait confiance à ICT-Towers :

Figure III. 2 : Partenariat ICT-Towers

c Recherche & Développement

ICT-Towers se distingue par sa spécificité, en se différenciant des concurrents par la mise en place d'une structure entière et R&D chargée de la conduite des travaux de recherche scientifiques nécessaires, au développement des solutions les plus appropriées.
L'objectif principal étant de lancer et de conduire des travaux de recherche scientifiques, de procéder au développement expérimental afin de traduire les objectifs stratégiques en projets informatiques tout en garantissant les aspects suivants :

- L'utilité et l'utilisabilité des solutions proposées.
- Leur adéquation aux besoins et contraintes des clients.
- Leur sécurité, leur confiance et leur haute disponibilité.

d Environnement du stage

Le stage s'est déroulé au sein de la société ICT-Towers à Sidi Belabess, le choix de l'entreprise comme pôle d'expertise, d'excellence et d'innovation dans le domaine des NTIC est fondé sur le fait que : la qualité de ses prestations et services est garantie, et que son personnel est spécialisé, hautement qualifié, expérimenté, et justifiant de certifications de très haut niveau, conformément aux exigences posées par les différentes firmes (leaders mondiaux) dans le domaine des NTIC.
Être entouré par des experts et des instructeurs hautement qualifiés sur le plan technique et pédagogique, au contenu enrichi, avec des plates-formes matérielles.

III.2 Business Audit ICT-Towers

Dans cette partie, nous devions connaitre la hiérarchie de ICT-Towers. Le responsable nous a informé que l'entité est divisée en 3 secteurs. Chaque secteur a son propre Vlan qui recouvre des tâches spécifiées et limitées, nous citons :

1. Le Directeur de l'entreprise & Pearson Vue.
2. Bureau Administratif & Financier.
3. Service clientèle et visiteurs.

Note : Pearson Vue est une société internationale et un Leader mondial des examens de certifications. Cela signifie que la nécessité de ce dernier est strictement prioritaire vu que les examens se passent en ligne.

- Nous avons trouvé qu'il existe plusieurs types de trafic gérés au sein de ICT-Towers dont peu est très important en termes de nécessité par rapport au reste qui devait être classifié du plus prioritaire au moins utile.

- Le Directeur nous a mentionné qu'une configuration QoS est déjà implémentée et qui nécessite une comparaison avec ses besoins désirés. Ces besoins doivent être ordonnés du plus prioritaire au moins important. Les étapes suivantes l'expliquent brièvement :

- Vlan du VoIP : Voice over IP
- Vlan du Directeur & Pearson Vue
- Vlan des employés
- Vlan des étudiants et stagiaires
- Le dernier Vlan est réservé aux visiteurs

III.3 Audit du réseau ICT-Towers

III.3.1 Topologie et structure du réseau ICT-Towers

La **Figure III.3** représente l'infrastructure globale de ICT-Towers au niveau de Sidi Belabess et Alger en montrant les liaisons avec les fournisseurs d'accés Internet.

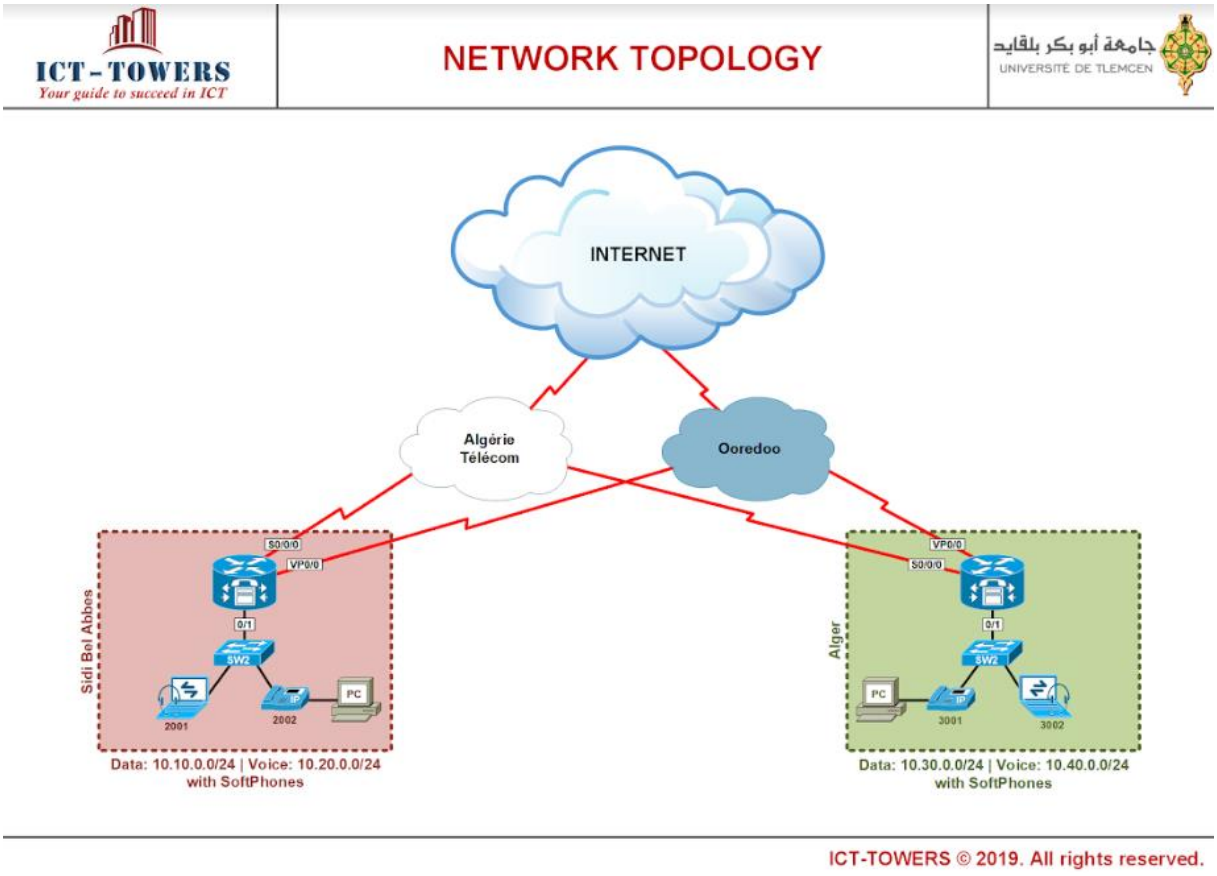

Figure III. 3 : Infrastructure ICT-Towers

Dans cette partie, nous avons d'abord dû étudier tout le trafic du réseau. Pour cela, nous nous sommes réunis avec le directeur de l'entreprise pour faire un audit approfondi du réseau et les contraintes qui y existent.

En résultat, nous avons rencontré des problèmes techniques tels que les protocoles de routage et un mauvais adressage IP. En outre, il y avait une configuration QoS mais qui était mal implémentée, et qui devait être parfaitement adaptée aux besoins de l'entité.
La qualité de service (QoS) ne fonctionne parfaitement que lorsque le réseau est bien configuré.

ICT-Towers est une entreprise qui travaille totalement avec des équipements Cisco, ce qui impose une configuration avec des commandes pures Cisco. Tandis qu'il existe d'autres entreprise telles que Algérie Télécom, Ericsson, Djezzy etc.… qui utilisent les produits de vendeurs Huawei, Juniper, Palo Alto etc…

III.3.2 Les types de trafic ICT-Towers

Les éléments suivants définissent les types de trafic du réseau ICT-Towers :

- **Protocoles de routage :** OSFP, EIGRP
- **Pearson Vue :** Examen de certification en ligne
- **Management :** SNMP, ICMP…
- **VoIP :** Voix sur IP
- **Base de données :** SQL
- **Mise à jour logiciel (Software updates)**
- **Système de sauvegarde (Backup) :** Modification sur la machine
- **Mail :** Gmail, Yahoo, Outlook…
- **Téléchargement (File Transfer) :** Torrent, Emule…
- **Web :** Google, Yahoo Recherche
- **Video Over http:** Vidéo sur Facebook, Twitter…
- **Application de messagerie :** WhatsApp, Viber, Skype
- **Video :** YouTube
- **Tunneling :** Tor, VPN
- **Gaming :** Jeux vidéo
- **Anonymizers :** Piratage / Hackers

Lors de la supervision de la qualité de service qui existait dans le réseau, nous avons rencontré plusieurs problèmes et contraintes qui d'un côté ne respectaient pas les standards de la QoS et de l'autre côté ne vérifient pas les besoins de la société. Parmi ces problèmes nous citons :

- Le Vlan du Pearson Vue est négligé en termes d'importance.
- La liste d'accès est appliquée sur un seul Vlan seulement.
- Le marquage est complétement non identifié.
- Contrainte de classes entre les switches et les routeurs.
- Il existait une Policy pour VoIP ce qui n'est pas du tout nécessaire.

A l'aide d'autres ingénieurs réseaux, nous avons amélioré la configuration réseau en travaillant sur son infrastructure et en supervisant le développement technique et le comportement du réseau.

Au cours de cette partie, nous avons décrit les étapes nécessaires pour pourvoir implémenter la QoS dans notre prototype, à savoir l'audit des applications existantes et leur classification. Dans la partie suivante, nous allons discuter notre implémentation de QoS.

III.4 Configuration de la QoS

III.4.1 Phase 1 : Étape préparative

Après qu'on a fait un audit du réseau, le directeur de ICT-Towers nous a cité ses besoins et ses nécessités désirées. Ce qui nous a permis de structurer et d'ordonner les types de trafic dont chaque type est intégré dans sa classe selon sa priorité. Nous nous sommes arrivés à un résultat qui est affiché dans le **Tableau III.1** suivant :

Nom de la classe	Contenu	Priorité	Identification
Routing Protocols	OSPF, EIGRP…	**CS7**	▪ Routing Protocol
Management	SNMP, ICMP…	**CS6**	▪ Network-management
Voice	Voice Over IP	**EF**	▪ Voice, SIP
Premium	Base de données	**AF41**	▪ SQL
	Mail	**AF42**	▪ Email
	Système de Sauvegarde	**AF43**	▪ Backup-and-storage
Critique	Pearson Vue	**AF31**	▪ Access List
	Média	**AF32**	▪ YouTube ▪ Video-over-http
	(Vide)	**AF33**	▪ (Réservé)
Normal	Téléchargement	**AF21**	▪ File-Transfer
	Mise à jour de logiciel	**AF22**	▪ Software-updates
	Web	**AF23**	▪ HTTP ▪ Secure-http
Best Effort	Réseaux Sociaux	**AF11**	▪ Social-networking ▪ Social-Media
	Flux indésirable 1	**AF12**	▪ Peer to Peer ▪ Gaming
	Flux indésirable 2	**AF13**	▪ Tor ▪ Anonymizers ▪ Tunnel

Tableau III. 1 : Configuration désirée

Dans ce tableau, nous avons laissé un champ vide **AF33**. Cela est appelé le remarquage ; C'est quand la file d'attente d'un flux très important tel que **AF41** est saturée, le trafic venant subira une chute de la queue 'Tai drop'. Pour cela on remarque **AF41** dans un champ vide tel que **AF33.**

Nous avons séparé le trafic en 3 catégories de classes de service :

a **Catégorie CS:**

- **CS7 :** Les protocoles de routages sont la base pour que le réseau puisse transmettre et recevoir les paquets.

- **CS6 :** La gestion du réseau est aussi indispensable et elle doit être strictement favorisée.

b **Catégorie EF :** Destinée à véhiculer les trafics en temps réel d'un client de type signalisation de la voix (délai d'acheminement constant et très court).

c **Catégorie AF:**

- **Une classe de trafic 4 (Premium) :** Destinée à véhiculer les trafics des applications importantes telles que mail, Base de données et le système de sauvegarde.

- **Une classe de trafic 3 (Critique) :** Destinée à véhiculer les trafics des applications critiques comme : Pearson Vue et les médias.

- **Une classe de trafic 2 (Normal) :** Destinée à véhiculer les trafics des applications non critiques comme : Mise à jour logiciel, Web et Téléchargement.

- **Une classe de trafic 1 (Best Effort) :** Destinée à véhiculer les trafics des applications non prioritaires qui ne disposent aucune garantie particulière comme : Les réseaux sociaux, les jeux vidéo, VPN.

❖ **Note importante :**

Nous devions prendre en considération que les deux liaisons d'entrée et sortie sont des liaisons Giga Ethernet (1 Giga chacune). Alors, nous avons dû fixer la bande passante de la liaison sortante vers Internet à 400 Mbps pour qu'il ait une congestion et pour pousser le routeur à faire son travail de QoS. Tandis qu'on a gardé la liaison entrante vers le réseau ICT-Towers à 1 Gbps.

La **Figure III.4** est une capture qui a été prise avant de commencer l'implémentation. Nous avons lancé plusieurs flux pour voir le comportement du réseau.

	Input	Output
	-----	------
Protocol	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
youtube	62217	56280
	88980628	46454400
	1285000	77000
	1285000	77000
secure-http	62370	45969
	79257012	39971120
	1004000	58000
	1112000	75000
voip	12626	11316
	17276388	10992524
	288000	17000
	2100000	89000
backup-and-storage	90558	89821
	78664571	47132874
	99000	27000
	1290001	78000
anonymizers	35461	33524
	44431637	33827347
	98000	10000
	980000	130000
whatsapp	90172	74297
	74906994	63228114
	327000	20000
	354000	64000
viber	43942	41046
	35357359	30322340
	2000000	260000
	2010000	270000
http	42641	40685
	48087063	34553346
	70000	20000
	603000	170000
bittorrent	66608	58082
	62356549	61836236
	123000	90000
	169000	230000
gmail	30057	11440
	63485676	35552786
	56000	16000
	660000	122000
video-over-http	24184	12471
	58310977	48424026
	129500	13100
	2014000	1629000
tor	22170	10750
	29570090	20362520
	37000	2000
	390000	25000

Figure III. 4 : Résultat flux avant QoS

La **Figure III.5** représente un histogramme des paquets générés en sortie et en entrée avant l'implémentation de la QoS.

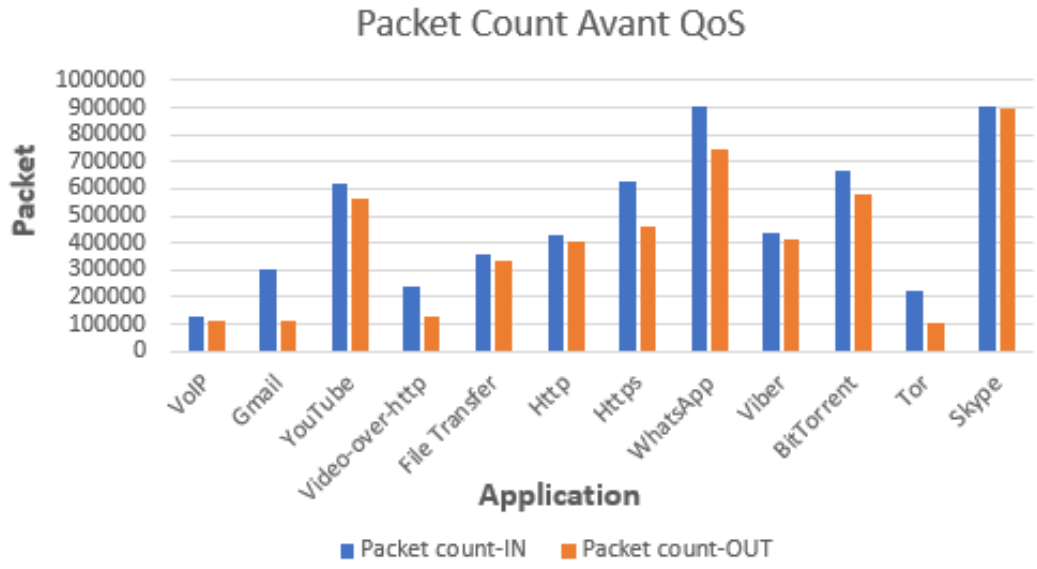

Figure III. 5 : Nombre de paquets avant QoS

La **Figure III.6** représente un histogramme de la bande passante consommée en sortie et en entrée par les applications avant l'implémentation de la QoS.

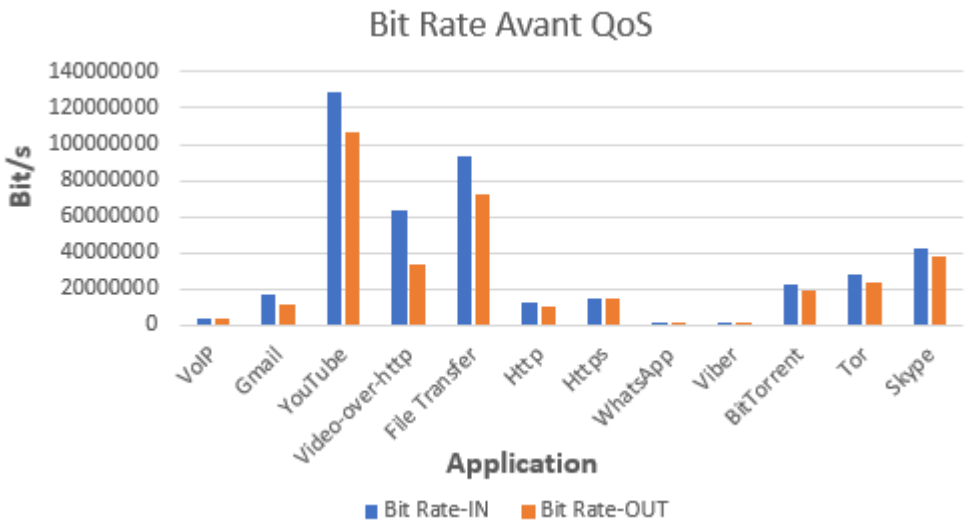

Figure III. 6 : La bande passante avant QoS

Nous remarquons dans la **Figure III.6** que les flux qui circulent en entrée et en sortie sont presque les mêmes. Ceci implique que la notion des priorités n'est pas appliquée car l'implémentation de la qualité de service n'est pas encore injectée.

En regardant dans la **Figure III.5** le flux des paquets générés des trafics non importants tels que BitTorrent, Https, WhatsApp etc.… on déduit que la bande passante est consommée que par ces flux moins utiles. Cela cause les problèmes suivants :

- Un retard dans la VoIP
- Perte de paquets des trafics importants (YouTube, Gmail…)
- Un retard pendant les examens de certification (Pearson Vue)

❖ Matériel Utilisé

- Router Cisco 1921 ISR
- Switch Cisco Catalyst 2960-24TT-L

❖ Outil utilisé

Wireshark

Wireshark est un analyseur de protocoles (sniffer). Celui-ci utilise directement l'interface Ethernet de la machine pour réaliser la capture de toutes les informations circulant sur le réseau local sur lequel nous sommes connectés. Il sera utilisé comme sonde réseau pour analyser les protocoles des flux générés.

La **Figure III.7** ci-dessous est une capture **Wireshark** qui nous montre les flux lancés allant du réseau ICT-Towers vers Internet et Vice-versa :

No.	Source	Destination	Protocol	Length	Info
328	10.10.45.3	172.16.1.2	SSL	78	Continuation Data
329	172.16.1.2	10.10.45.3	TCP	54	sip-tls > 49322 [ACK] Seq=1 Ack=25 Win=65536 Len=0
330	10.10.45.3	172.16.1.2	SSL	1506	[TCP Previous segment not captured] Continuation Data
331	172.16.1.2	10.10.45.3	TCP	66	[TCP Dup ACK 329#1] sip-tls > 49322 [ACK] Seq=1 Ack=25
332	10.10.45.3	172.16.1.2	SSL	1506	Continuation Data
334	10.10.45.3	172.16.1.2	SSL	1506	[TCP Retransmission] Continuation Data
336	10.10.45.3	172.16.1.2	SSL	1506	[TCP Retransmission] Continuation Data
337	172.16.1.2	10.10.45.3	TCP	66	sip-tls > 49322 [ACK] Seq=1 Ack=1477 Win=64000 Len=0 S
338	10.10.45.3	172.16.1.4	ICMP	1492	Echo (ping) request id=0x0001, seq=506/64001, ttl=123
339	10.10.45.3	172.16.1.2	SSL	590	Continuation Data
340	10.10.45.3	172.16.1.2	SSL	590	Continuation Data
342	10.10.45.3	172.16.1.2	SSL	1506	[TCP Retransmission] Continuation Data
343	172.16.1.2	10.10.45.3	TCP	66	sip-tls > 49322 [ACK] Seq=1 Ack=2937 Win=65536 Len=0 S
344	10.10.45.3	172.16.1.2	SSL	1506	Continuation Data
345	10.10.45.3	172.16.1.2	SSL	1506	Continuation Data
346	172.16.1.2	10.10.45.3	TCP	66	[TCP Dup ACK 343#1] sip-tls > 49322 [ACK] Seq=1 Ack=29
347	10.10.45.3	172.16.1.4	TCP	66	49323 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
348	172.16.1.4	10.10.45.3	TCP	66	http > 49323 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MS
349	10.10.45.3	172.16.1.4	TCP	54	49323 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
350	10.10.45.3	172.16.1.4	HTTP	463	GET /Base HTTP/1.1
351	10.10.45.3	172.16.1.2	SSL	1506	[TCP Retransmission] Continuation Data
353	10.10.45.3	172.16.1.4	HTTP	463	[TCP Retransmission] GET /Base HTTP/1.1
354	172.16.1.4	10.10.45.3	TCP	54	http > 49323 [ACK] Seq=1 Ack=410 Win=15680 Len=0
355	172.16.1.4	10.10.45.3	HTTP	584	HTTP/1.1 301 Moved Permanently (text/html)
356	172.16.1.4	10.10.45.3	TCP	54	http > 49323 [FIN, ACK] Seq=531 Ack=410 Win=15680 Len=
357	c0:00:06:a0:00	c0:00:06:a0:00	LOOP	60	Reply
358	10.10.45.3	172.16.1.4	TCP	54	49323 > http [FIN, ACK] Seq=410 Ack=531 Win=65168 Len=
359	10.10.45.3	172.16.1.4	TCP	54	49323 > http [ACK] Seq=411 Ack=532 Win=65168 Len=0
360	172.16.1.4	10.10.45.3	TCP	54	http > 49323 [ACK] Seq=532 Ack=411 Win=15680 Len=0
361	10.10.45.3	172.16.1.4	TCP	66	49324 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
362	172.16.1.4	10.10.45.3	TCP	66	http > 49324 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MS
363	10.10.45.3	172.16.1.4	TCP	54	49324 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0

Figure III. 7 : Capture des différents trafics avec Wireshark

La **Figure III.8** ci-dessous est une capture Wireshark prise avant QoS d'un trafic aléatoire pour montrer que le marquage n'est pas encore identifié, on remarque que le champ DSCP est fixé à CS0 (Best Effort) pour tous les trafics qui circulent dans le réseau.

```
Wireshark · Paquet 42809 · Ethernet
Ethernet II, Src: CompalIn_c8:3f:4c (20:89:84:c8:3f:4c), Dst: Cisco_ae:f0:c4 (08:17:35:ae:f0:c4)
  > Destination: Cisco_ae:f0:c4 (08:17:35:ae:f0:c4)
  > Source: CompalIn_c8:3f:4c (20:89:84:c8:3f:4c)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.20.48, Dst: 85.154.176.209
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0x7c24 (31780)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.20.48
    Destination: 85.154.176.209
Transmission Control Protocol, Src Port: 52840, Dst Port: 53152, Seq: 1192, Ack: 122061, Len: 0
```

Figure III. 8 : Capture Wireshark d'un trafic aléatoire avant QoS

A. Classification des flux

Pour établir une qualité de service, il faut tout d'abord sélectionner les flux qu'on veut différencier.

i. Classification du trafic réseau

Une classe de trafic contient trois éléments essentiels :

- Le nom de la classe
- Une série de commandes **match**
- Evaluation des commandes **match**

Les commandes match sont utilisées pour spécifier divers critères de classification des paquets. Les paquets sont vérifiés pour déterminer s'ils appartiennent ou non à ces critères spécifiés par la commande match.

En utilisant la classification des paquets on peut par la suite partitionner notre réseau en plusieurs niveaux de priorités ou en classes de services (**Class-map**)

ii. Paramètres des class-map

1- On associe un nom à une classe-map pour mieux la designer par la suite :

Routeur(config)# class-map *nom-de-la-classe*

2- On spécifie que TOUS les critères doivent être vérifiés pour que le paquet appartienne à la classe.

Routeur(config)# class-map **match-all** *nom-de-la-classe*

3- On spécifie qu'au moins un des critères doit être vérifié pour que le paquet appartienne à la classe

Routeur(config)# class-map **match-any** *nom-de-la-classe*

B. Création d'une politique de service

Maintenant qu'on a différencié le trafic, on doit partager la bande passante de notre routeur. C'est pourquoi on doit utiliser des politiques de priorité (**Policy-map**). C'est à partir du moment où on utilise les **policy-map** qu'on met en place la Qualité de Service voulue.

Une **policy-map** contient trois éléments :

1. Le nom de la politique
2. Les classes associées
3. Les commandes de qualité de service

III.4.2 Phase 2 : Classification et Marquage

a Marquage

Après qu'on a classifier et marquer chaque flux dont il appartient dans le **Tableau III.1**, nous avons injecté la configuration en commençant par le marquage de chaque flux : comme le montre la **Figure III.9** suivantes :

```
Policy Map conf-IN
  Class voice
    set dscp ef
  Class database
    set dscp af41
  Class mail
    set dscp af42
  Class backup
    set dscp af43
  Class pearsonvue
    set dscp af31
  Class media
    set dscp af32
  Class file-transfer
    set dscp af21
  Class software-updates
    set dscp af22
  Class http/https
    set dscp af23
  Class social-media
    set dscp af11
  Class routing-prtocols
    set dscp cs7
  Class management
    set dscp cs6
  Class undiserable
    set dscp af12
  Class undiserable2
    set dscp af13
  Class class-default
    set dscp default
  interface g0/0   [1]
  service-Policy input conf-in
```

[1] : Après avoir créé une politique de service, il faut l'appliquer sur une interface (ou plusieurs) du routeur. Suivant le flux du trafic, il est possible de l'attacher soit à l'interface entrante soit à l'interface sortante. Dans notre cas, on l'attache à l'interface entrante (Input).

Figure III. 9 : Marquage

b Classification

Tout d'abord, nous avons injecté les listes d'accés. La **Figure III.10** montre l'affichage des commandes injectées.

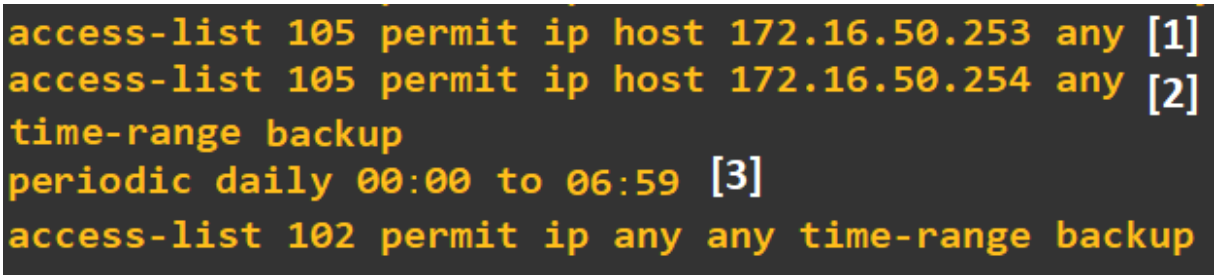

Figure III. 10 : Affichage des listes d'accés

- **Explication**

[1] : Permettre l'@ IP de la machine du Directeur d'accéder à tous sans exception.
[2] : Permettre l'@ IP de la machine du Pearson Vue d'accéder à tous sans exception.
[3] : Permettre les @ IP du groupe 102 (Source ou Destination) de stocker les nouvelles modifications entre minuit et 7h du matin.

La **Figure III.11** illustre l'injection des commandes de classification :

```
Class Map match-all social-media (id 19)
  Match access-group  104
  Match class-map social-networking

Class Map match-any routing-prtocols (id 13)
  Match protocol attribute sub-category routing-protocol

Class Map match-any http/https (id 14)
  Match protocol http
  Match protocol secure-http

Class Map match-any media (id 15)
  Match protocol video-over-http
  Match protocol youtube

Class Map match-all voice (id 16)
  Match packet length min 64 max 200
  Match   dscp ef (46)

Class Map match-any undiserable (id 17)
  Match protocol attribute p2p-technology p2p-tech-yes
  Match protocol attribute sub-category p2p-networking
  Match protocol attribute sub-category p2p-file-transfer
  Match protocol attribute category gaming

Class Map match-any file-transfer (id 9)
  Match protocol attribute sub-category file-transfer

Class Map match-any class-default (id 0)
  Match any

Class Map match-any social-networking (id 10)
  Match protocol skype
  Match protocol viber
  Match protocol whatsapp

Class Map match-any software-updates (id 11)
  Match protocol attribute category software-updates

Class Map match-any undiserable2 (id 12)
  Match protocol tor
  Match protocol attribute category anonymizers
  Match protocol attribute tunnel tunnel-yes

Class Map match-any database (id 2)
  Match protocol attribute category database

Class Map match-any mail (id 3)
  Match protocol attribute category email

Class Map match-all backup (id 5)
  Match protocol attribute category backup-and-storage
  Match access-group  102

Class Map match-all pearsonvue (id 6)
  Match access-group  105

Class Map match-any management (id 7)
  Match protocol attribute sub-category network-management
```

Figure III. 11 : Classification

Note 1 :

Ici, nous observons la puissance du NBAR 2 vu qu'il peut identifier le trafic d'une manière très profonde.

Router (conf)# Class-map match-any media

Router (conf)# Match Protocol Video-over-http

➔ Cette dernière commande peut bloquer entièrement une vidéo sur Facebook ou sur Twitter… en augmentant son agressivité de drop.

Note 2 :

La classe-map Voice (id16) est représentée par la commande suivante :
Match packet length min 64 max 200

Note 3 :

Tout le trafic restant qui n'est pas identifié dans les classes sera automatiquement affilié vers la classe Default.

III.4.3 Phase 3: Remarquage + Policing & Shaping + Drop Probability

Tout d'abord, nous devions regrouper les sous classes (Media, Mail, File Transfer…) dans les classes principales (Voice, Premium, Critique, Normal, Best effort) comme le montre la **Figure III.12** ci-dessous :

```
Class Map match-any premium
  Match   dscp af43          [1]
  Match   dscp af42
  Match   dscp af41

Class Map match-any critique
  Match   dscp af33
  Match   dscp af32
  Match   dscp af31

Class Map match-any normal
  Match   dscp af23
  Match   dscp af22
  Match   dscp af21

Class Map match-any besteffort
  Match   dscp af13
  Match   dscp af12
  Match   dscp af11

Class Map match-all voice
  Match   dscp ef
```

Figure III. 12 : Regroupement des sous-classes

- **Explication**

[1] : La mise en place des sous-classes Mail, Base de données et Backup dans la classe Premium, même chose pour tout le reste.

Tout de suite, nous devions remarquer la classe Premium dans le champ AF33. Par la suite nous avons identifié chaque flux par son Policy et sa mise en forme (Shaping) et en affectant à chacune une probabilité de drop. La **Figure III.13** montre la configuration de la phase 3 :

```
Router#sh policy-map
  Policy Map conf-OUT
    Class voice
      priority 100 (kbps)  [1]
    Class premium
      bandwidth 40 (%)  [2]
     police cir 160000000 pir 180000000   [3]
       conform-action transmit
       exceed-action set-dscp-transmit af33  [4]
       violate-action drop
       packet-based wred, exponential weight 9
      random-detect ecn  [5]

      dscp    min-threshold    max-threshold    mark-probablity
      ----------------------------------------------------------
      af41 (34)     90               100              1/10 [6]
      af42 (36)     80               95               1/15
      af43 (38)     70               85               1/20
      default (0)   -                -                1/10
    Class critique
      bandwidth 30 (%)
     police cir 140000000  [7]
       conform-action transmit
       exceed-action drop
       packet-based wred, exponential weight 9
      random-detect ecn

      dscp    min-threshold    max-threshold    mark-probablity
      ----------------------------------------------------------
      af31 (26)     55               65               1/35
      af32 (28)     40               50               1/40
      af33 (30)     35               45               1/45
      default (0)   -                -                1/10
    Class normal
      bandwidth 15 (%)
      Average Rate Traffic Shaping 60000000    [8]
      cir 4000000   (bps)
       packet-based wred, exponential weight 9

      dscp    min-threshold    max-threshold    mark-probablity
      ----------------------------------------------------------
      af21 (18)     33               40               1/50
      af22 (20)     27               35               1/55
      af23 (22)     23               30               1/60
      default (0)   -                -                1/10
    Class besteffort
      bandwidth 10 (%)
     police cir 10000000
       conform-action transmit
       exceed-action drop
       packet-based wred, exponential weight 9

      dscp    min-threshold    max-threshold    mark-probablity
      ----------------------------------------------------------
      af11 (10)     17               25               1/65
      af12 (12)     13               20               1/70
      af13 (14)     10               15               1/80
      default (0)   -                -                1/10
    Class class-default
      fair-queue
       packet-based wred, exponential weight 9

      dscp    min-threshold    max-threshold    mark-probablity
      ----------------------------------------------------------
      default (0)   -                -                1/10
```

Figure III. 13 : Configuration Remarquage + Policing & Shaping + Drop Probability

- **Explication**

[1] : La classe Voice est caractérisée par « Priority 100 ».

[2] : La classe Premium utilise 40% de la bande passante : $\mathbf{400} * \frac{\mathbf{40}}{\mathbf{100}} = \mathbf{160}\ \boldsymbol{Mbps}$

[3] : La classe Premium est identifiée par une Policy 2 rates et est limitée [160-180] Mbps.

[4] : Le remarquage de la classe Premium en AF33.

[5] : ECN utilisé seulement dans les deux classes les plus importantes (4 et 3), et cela pour fournir un meilleur service de compression et de LFI à ces deux classes vu leur importance.

[6] : Représente les profils WRED, prenant l'exemple de la sous classe AF41, le seuil minimum de la probabilité de rejet est fixé à 90 %, le seuil maximum est fixé à 100% d'agressivité (Augmentation du flux), et son degré d'inclinaison est de 10% ce qui va assurer aux files d'attente de AF41 un évitement total de congestion.

[7] : La classe Critique est identifiée par une Policy 1 rate vu qu'elle est moins importante.

[8] : La classe Normale est identifiée par une mise en forme / Shaping car elle est la plus négligée et indésirable. Utilisation de 15 % de la bande passante pour cette classe, ce qui vaut : $\mathbf{400} * \frac{\mathbf{15}}{\mathbf{100}} = \mathbf{60}\ \boldsymbol{Mbps}$

En ce qui concerne le pourcentage qui reste de la bande passante (5%= 20Mbps). Elle sera prise par la classe Default.

III.4.4 Phase 4 : Monitorage et évaluation du travail

Après la configuration, nous avons lancé le trafic de nouveau pendant une période de deux heures. Et puis nous l'avons supervisé pour voir l'effet de la qualité de service. La **Figure III.14** montre les nouvelles valeurs affichées après l'implémentation de toutes les configurations précédentes de la QoS.

	Input	Output
	-----	------
Protocol	Packet Count	Packet Count
	Byte Count	Byte Count
	5min Bit Rate (bps)	5min Bit Rate (bps)
	5min Max Bit Rate (bps)	5min Max Bit Rate (bps)
----------	----------	----------
youtube	561732	456321
	7055781364	4033751966
	102849600	99763200
	114859300	110895170
secure-http	731952	527630
	900973518	622576389
	19548960	10582640
	21572070	13746900
voip	146813	146813
	209763485	209763485
	4246730	4246730
	4268640	4268640
skype	954310	908275
	891255843	732956324
	47726100	3986540
	43676850	4462150
ftp	247691	152378
	294729186	213900689
	57376250	39716830
	62875600	48623190
whatsapp	937264	513946
	86773892	31353782
	997300	329340
	1196590	636700
viber	468315	249238
	38995420	13951267
	1956300	627500
	2387650	1026780
http	596327	32465
	7056782389	371559612
	21183400	9016470
	29827180	18675500
bittorrent	701396	34762
	770037936	23763515
	27386000	918430
	41157000	1238540
gmail	281458	240124
	601763895	539234710
	16097620	14787530
	18376650	17998100
video-over-http	223154	197265
	469311768	413497280
	43524960	40869750
	52860520	49178640
tor	303709	137050
	467813750	157601788
	33786420	7624150
	45825300	10875600

Figure III. 14 : Résultat flux après QoS

La **Figure III.15** ci-dessous définit un histogramme qui représente le nombre de paquets après QoS.

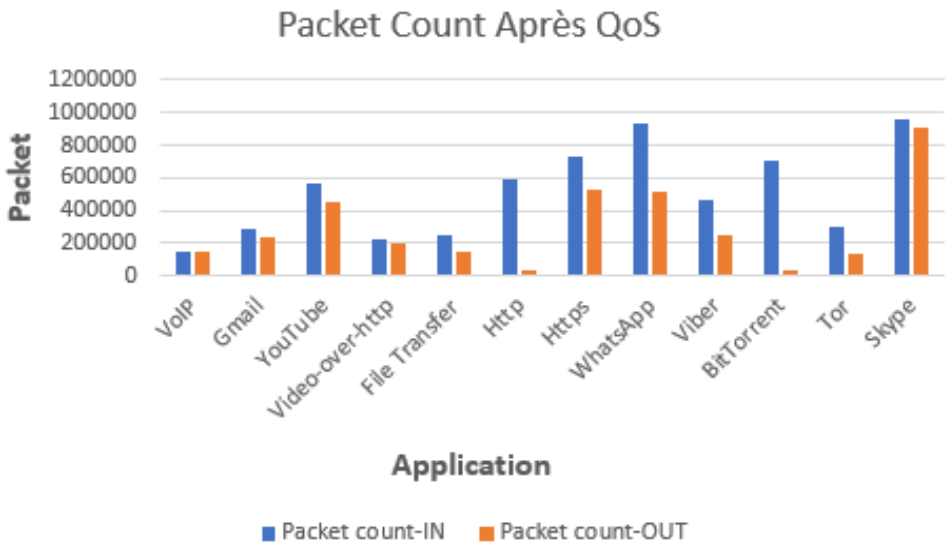

Figure III. 15 : Le nombre de paquets après QoS

La **Figure III.16** représente un histogramme de la bande passante consommée par les applications en sortie et en entrée après l'implémentation de la qualité de service.

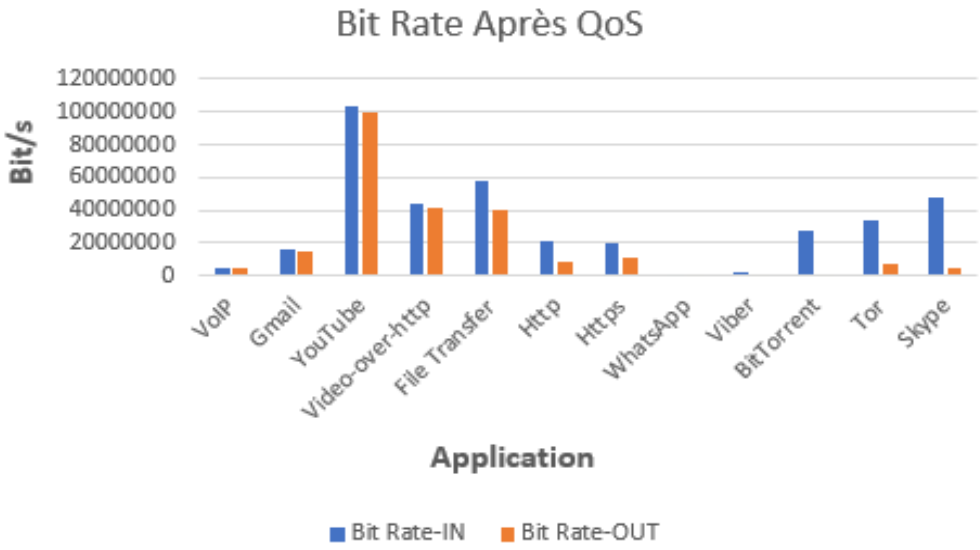

Figure III. 16 : La bande passante après QoS

L'implémentation de la QoS a justifié un bon résultat. Nous remarquons que les flux qui circulent en entrée et en sortie après l'injection de la configuration ne sont plus les mêmes. En résultat, le routeur a appliqué le mécanisme de la qualité de service ce qui a imposé la liaison de sortie (fixée à 400 Mbps) de fournir aux différentes classes de trafics leur critères et politique de comportement.

La **Figure III. 17** est une capture Wireshark d'une trame de réception de la sous-classe AF42 (Gmail).

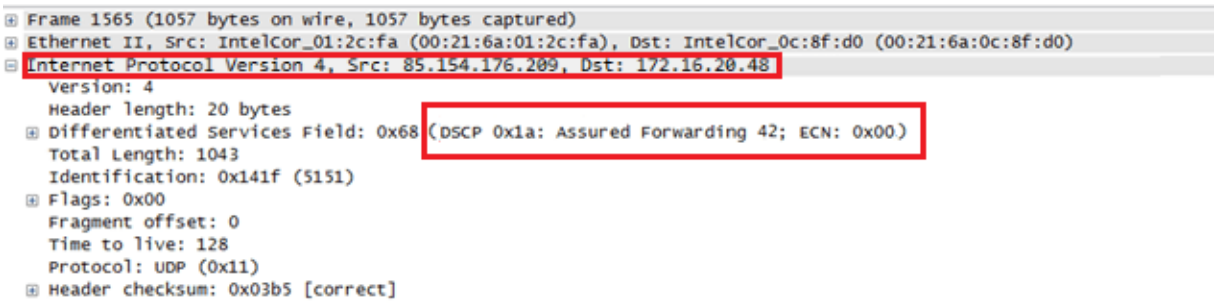

Figure III. 17 : Capture trame Gmail avec Wireshark

La **Figure III. 18** est une capture Wireshark d'une trame VoIP (EF) vers l'extérieur du réseau.

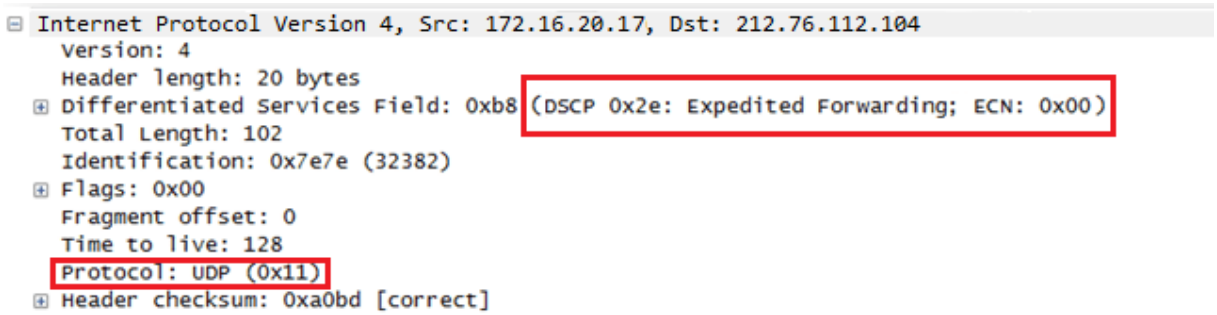

Figure III. 18 : Capture trame VoIP avec Wireshark

Grâce à l'analyseur Wireshark, nous avons vérifié la qualité de service rendue pour la voix ainsi que pour les emails. Nous observons donc que les priorités définies en termes de classes sont respectées et que le marquage joue bien son rôle dans le contrôle du trafic.

Conclusion

Dans ce chapitre, nous avons décrit l'environnement matériel et logiciel durant notre travail. Nous avons mis en place notre implémentation comme nous avons aussi effectué des simulations sur le trafic avant et après activation de toutes les configurations nécessaires de la qualité de service sur le site administratif.

Conclusion générale

Notre projet de fin d'études est un travail réalisé au sein de ICT-Towers ayant pour objectif l'optimisation des ressources réseaux par l'implémentation de la Qualité de Service (QoS). Nous avons entamé ce projet par présentation générale du projet. Pour cela, nous avons présenté dans le premier chapitre le monde du réseau IP et ces contraintes ainsi une introduction sur la qualité de service.

Dans le deuxième chapitre, nous avons expliqué les principaux mécanismes de gestion de la QoS, ainsi que les deux modèles IntServ, DiffServ. Ensuite nous avons consacré le troisième chapitre à l'étude et à l'analyse de l'existant.

Cette étude théorique nous a permis de mener à bien la démarche et la réalisation de la QoS, à savoir les applications existantes et la classification de Cisco menu sur ces applications.

En effet, nous nous sommes basés sur la politique de Cisco pour implémenter la qualité de service dans les routeurs Cisco des sites administratifs afin de garantir une QoS de bout en bout que nous avons montré par l'implémentation de notre étude de QoS.

Enfin, ce stage fut une expérience très enrichissante pour nous sur les deux plans personnels et professionnels. En effet, il a été l'occasion de renforcer nos connaissances théoriques et de les appliquer pratiquement, aussi qu'étendre nos compétences techniques. Ainsi c'était une expérience qui nous a permis d'avoir un esprit d'équipe, d'être appliqué et de découvrir le milieu professionnel.

Avec QoS, les administrateurs réseau peuvent ajuster avec précision les vitesses de trafic et l'utilisation de la bande passante sur leurs réseaux. Lorsqu'elles sont correctement configurées, les communications et le trafic réseau critiques garantissent les vitesses et la bande passante dont ils ont besoin pour fonctionner sans ralentissement, tandis que les services moins critiques peuvent attendre pour faire leur travail jusqu'à ce que le réseau soit moins encombré. La QoS est un outil précieux que tous les administrateurs réseau devraient utiliser pour optimiser les capacités et la fiabilité de leur réseau.

Références bibliographies

[1] Jean-François Susbielle : Internet Multimédia et temps réel, Edition Eyrolles,2000

[2] BOUBEKRI Sara, MEBARKI Ryma : La haute disponibilité des réseaux campus, Mémoire De Fin d'Etude, Université A/Mira de Béjaïa, 2015/16

[3] Chai-Ben Dania : gestion de qualité de service dans les réseaux NGN, Mémoire Master Professionnel, Université Kasdi Merbah-Ouargla, 2014/15

[4] Cisco Systems: QOS Implementing Cisco Quality of Service, volume 1-2, version 2.2, guide de formation Cisco

[5] L.Toumi : Algorithmes et mécanismes pour la qualité de service dans des réseaux Hétérogènes, Institut National Polytechnique de Grenoble - INPG, France, 2002.

[6] Aaron Balchunas: QoS Classification and Marking, Volume1, version32, 2010

[7] Aaron Balchunas: QoS and Queuing, Volume1, version31, 2010

[8] Syngress Publishing: Inc. Administering Cisco QoS in IP Networks, 2001

[9] https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_c67-697963.html (Consultation : 17/03/2019)

[10] https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconav .html (Consultation : 24/04/2019)

[11] https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpolsh.pdf (Consultation : 14/02/2019)

Annexe

Cisco Express Forwarding (CEF) : C'est une technique de commutation de paquets utilisée dans les routeurs Cisco. L'objectif principal de CEF est d'optimiser la transmission des paquets et d'augmenter la vitesse de commutation des paquets.

Service Control Engine (SCE) : C'est une solution de surveillance et de contrôle DPI puissante et flexible, dédiée à l'utilisation du réseau, conçue pour analyser, consigner et conditionner les transactions réseau au niveau de l'application. Il permet aux fournisseurs de services de créer de nouvelles sources de revenus rentables tout en capitalisant sur leur infrastructure existante. Grâce à la puissance de HCL SCE, les fournisseurs de services peuvent analyser, facturer et contrôler le trafic réseau IP à des vitesses filaires.
HCL SCE fournit également les outils nécessaires pour identifier et cibler les services à contenu à forte marge et permettre leur distribution. Il répond aux besoins des établissements d'enseignement et des entreprises grâce à son riche ensemble de fonctionnalités telles que le filtrage des URL, la mise en liste noire, la surveillance et le contrôle de la bande passante basée sur les applications. Il est indépendant de l'accès et peut être déployé dans n'importe quel environnement de réseau câblé, filaire ou IP mobile.

SNA: Systems Network Architecture (SNA) is IBM's proprietary networking architecture, created in 1974. It is a complete protocol stack for interconnecting computers and their resources. SNA describes formats and protocols and is, in itself, not a piece of software.

Op Ex ou dépenses d'exploitation (Operational Expenditure) sont les charges courantes pour exploiter un produit, une entreprise, ou un système.

Cap Ex ou dépenses d'investissement (Capital Expenditure) se réfèrent aux immobilisations, c'est-à-dire aux dépenses qui ont une valeur positive sur le long terme.

Flexible NetFlow : Cisco IOS Flexible NetFlow est la technologie de flux de nouvelle génération. Il optimise l'infrastructure du réseau, réduit les coûts d'exploitation et améliore la planification de la capacité et la détection des incidents de sécurité avec une flexibilité et une évolutivité accrue. La possibilité de caractériser le trafic IP et d'identifier sa source, sa destination, son minutage et ses informations d'application est essentielle pour la disponibilité, les performances et les solutions du réseau. La surveillance des flux de trafic IP augmente la précision de la planification de la capacité et garantit que l'allocation de ressources est conforme aux objectifs de l'organisation. Flexible NetFlow aide les clients de Cisco à déterminer comment optimiser l'utilisation des ressources, planifier la capacité du réseau et identifier la couche d'application optimale pour la qualité de service (QoS). Il joue un rôle essentiel dans la sécurité du réseau en détectant les attaques par déni de service (DoS : Denial of Service) et les vers transmis par le réseau.