This QoS solution allows an optimal use of equipment and made a good management to the business applications.

The aim of our final project is to optimize the network resources at Poste Maroc by implementing Quality of Service (QoS) with Cisco configurations.

Our PFE contains the study of the Quality of Service (QoS), and the existing network infrastructure in the Poste Maroc, we have also deal with the present approach to implement QoS and setting implement QoS in our test model.

Table des matières

Liste des abréviations 8
Liste des tableaux 10
Liste des figures 10
Introduction générale 12
Chapitre 1: Présentation générale du projet 13
I. Présentation de Poste Maroc 14
1.1. Historique de Poste Maroc 14
1.2. L'organigramme de Poste Maroc 15
1.3. L'organigramme de la direction des systèmes d'information 16
1.4. Activités de Poste Maroc 17
II. Cahier des charges 18
2.1. Contexte du projet 18

2.2. Objectifs....18
2.3. Architecture WAN de la Poste Maroc....18
2.4. Les besoins....20
III. Planning du projet....20
Chapitre 2:Etude de la QoS....21
I. Introduction....22
1.1. Définition de la Qualité de Service....23
1.2. But de la Qualité de service....23
II. Les indicateurs de la QoS....24
III. Les niveaux de la QoS....24
IV. Les modèles de la qualité de service....25
4.1. Le modèle d'IntServ....25
a. Le protocole RSVP....25
b. Limites du protocole RSVP....26
4.2. Le modèle DiffServ....26
a. L'Objectif du DiffServ....26
b. Définition du champ DSCP....27
c. Le comportement par saut : PHB (Per Hop Behaviour)....28
V. Les mécanismes de gestion de la QoS....29
Chapitre 3:Etude de l'existant....31
I. Architecture....32
II. Description de l'existant....33
III. Analyse de l'existant....34
3.1. Accès des sites critique vers le siège via MPLS....34
3.2. Accès des sites Administratifs....34
3.3. Les Agences Normales....34
3.4. Accès Internet....34
3.5. Outil StreamCore....35
a. Présentation....35
b. Gamme et Architecture....35
c. Implémentation de la QoS sur StreamCore....36
3.6. Analyse de la QOS au sein de Poste Maroc....36

IV. Critique de L'existant 39
V. Etude comparative 41
5.1. Méthodologie adoptée 41
5.2. Tableaux comparatifs 42
5.3. Solutions envisagée 44
Chapitre 4:Démarche d'implémenter la QoS 46
I. Etude des applications existantes 46
1.1. Audit du système 46
a. Audit du Réseau 47
b. Audit du Busines 47
1.2. Matrice de flux de Poste Maroc 48
II. Classification de flux 50
Conclusion 51
Chapitre5:Mise en place de l'application QoS et tests 51
I. Les outils utilisés 52
1.1. Simulateur GNS3 52
1.2. JPerf: Générateur de trafic 52
1.3. Wireshark 52
1.4. VMware Workstation 10.0.1 53
II. La Maquette de test 53
1.1. Adressage et configuration 54
III. Mise en place de la QoS 54
IV. Simulation de la QoS 56
a. Envoi de Ping de l'agence critique vers le siège 56
b. Après activation de tous les services 57
Conclusion 61
Annexe A 62
Annexe B 63
Annexe C 70
Bibliographie &Webographie ..... **Erreur ! Signet non défini.**

LISTE DES ABREVIATIONS

Abréviation	Désignation
QoS	Quality of Service
WAN	Wide Area Network
MPLS	MultiProtocol Label Switching
ITU	International Telecommunication Union
IETF	Internet Engineering Task Force
RFC	Request For Comments
IntServ	Integrated Services
DiffServ	Differenciated Services
RSVP	Resource Reservation Protocol
ToS	Type of Service
DSCP	Differentiated Service Code Point
PHB	Per Hop Behaviour
CU	Currently Unused
CBR	constant bit rate
EF	Expedited Forwarding
AF	Assured Forwarding
CS	Class Selector

BA	Behavior Agregate
ACL	Access Control List
ICMP	Internet Control Message Protocol
SIP	Session Initiation Protocol
Http	HyperText Transfer Protocol
QSOS	Qualification and Selection of Open Source
RTCP	Real-time Transport Control Protocol
Https	HyperText Transfer Protocol Secure
IMCP	Internet Message Access Protocol
DNS	Domain Name System
ICA	Independent Computing Architecture
LDAP	Lightweight Directory Access Protocol
SMTP	Simple Mail Transfer Protocol
POP3	Post Office Protocol
SNMP	Simple Network Management Protocol
IMAP	Internet Message Access Protocol
VRF	Virtual Routing and Forwarding
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
CE	Customer Edge
PE	Provider Edge
P	Provider

LISTE DES TABLEAUX

Tableau 1: Les classes de priorité.....28
Tableau 2: Les sélecteurs de classe. 29
Tableau 3: Evaluation pour StreamCore. 43
Tableau 4: Evaluation pour Cisco. 44
Tableau 5:Les applications existantes. 47
Tableau 6: Matrice de flux. 49
Tableau 7:Les classes de la Qualité de service. 50
Tableau 8: Adressage IP. 54

LISTE DES FIGURES

Figure 1: Organigramme de Poste Maroc 16
Figure 2: Organigramme de la DSI 17
Figure 3: Architecture réseau de Poste Maroc. 19

Figure 4: Diagramme de Gantt.....20
Figure 5: Problématique.....22
Figure 6: Fonctionnement du protocole RSVP. 26
Figure 7: Composition du champ ToS. 27
Figure 8:Composition du champ DSCP. 27
Figure 9: Mécanismes de gestion de la QoS. 29
Figure 10: Réseau WAN de Poste Maroc. ..... **Erreur ! Signet non défini.**
Figure 11:Réseau LAN de Poste Maroc. 33
Figure 12: StreamGroomers SG1600. 36
Figure 13: Le flux services communs sous StreamCore. 37
Figure 14: Les flux applicatifs sous StreamCore. 37
Figure 15: Taux d'utilisation WAN vers Siège-Siège vers WAN. 38
Figure 16: Débit maximal -siège vers WAN. 39
Figure 17:Schéma générale de la méthode QSOS. 41
Figure 18:Barème de la méthode QSOS. 42
Figure 19:Réseau WAN implémentée sous GNS3. 53
Figure 20:Ping Agence vers Siège. 57
Figure 21:Capture trame ICMP avec Wireshark. 57
Figure 22: Configuration Jperf en mode serveur. 58
Figure 23: Configuration du Jperf en mode client. 59
Figure 24:Capture pour tous type de trafic avec Wireshark. 60
Figure 25:Ping après activation des Services. 60
Figure 26:Capture trame SIP avec Wireshark. 61

INTRODUCTION GENERALE

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, Poste Maroc accorde une grande importance à l'optimisation de son réseau par la mise en œuvre de la Qualité de Service.

Le processus d'optimisation des réseaux WAN est indispensable afin d'aboutir à une bonne performance aux applications critiques et une qualité de service satisfaisante.

C'est dans ce contexte que Poste Maroc 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 troismois. Il est scindé selon cinq chapitres couvrant l'ensemble des axes de notre travail. Le premier chapitre présente l'organisme d'accueil, l'élaboration de cahier des charges, et la planification du projet.

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 Poste Maroc et présente une étude comparative de deux équipements pour la mise en place de la Qualité de Service : Outil StreamCore et Cisco. Le quatrième chapitre montre la démarche que nous avons suivie pour l'implémentation de la Qualité de Service. Alors que le dernier décrit l'étape de la validation de notre démarche déployée, ainsi que les outils utilisés et la simulation.

Université Sidi Mohammed Ben Abdellah
Faculté Des Sciences et Techniques Fès
Département de Génie Electrique

CHAPITRE 1: PRESENTATION GENERALE DU PROJET

L'objectif de ce présent chapitre est de mettre notre travail dans son contexte général. Tout d'abord, nous présentons l'organisme d'accueil « Poste Maroc ».Ensuite, nous détaillons le cahier des charges proposé et le planning suivi tout au long de la réalisation de ce projet.

I. PRESENTATION DE POSTE MAROC

1.1. Historique de Poste Maroc

L'existence de **Poste Maroc** remonte à l'époque du Sultan Hassan 1 qui a pris en charge l'organisation d'un secteur sporadique et entretenu par des étrangers notamment.

- **En 1892**, le sultan donna ses ordres aux responsables des ports po… …te marocaine. Cette organisation embryonnaire a englobé 13 villes marocaines qui étaient reliées par lignes définies chacune par des cachets spécifiques.

- **En 1911**, la compagnie marocaine du télégraphe est chargée d'organiser la poste nationale mais surtout de commencer à utiliser dorénavant des timbres postaux au lien des cachets.

- **En 1912**, La compagnie commence son activité sous le nom de la direction Chérifienne de la poste, du télégraphe et du téléphone qui va mettra le premier timbre poste marocain le 22 mai 1912.

- **En 1956**, année de l'indépendance du Maroc, Feu Sa Majesté le RoiMohammed V instaura, à la place de l'Office Chérifien, un département ministériel de plein droit sous l'appellation du Ministère des PTT. Ce dernier mena une politique de développement soutenue du secteur.

- **En 1984**, une réforme a transformé le Ministère en un établissement publicsous la dénomination de l'Office National des Postes et Télécommunications (ONPT).

- **En 1998**, Poste Maroc voit le jour suite à la séparation des secteurs «Poste et Télécommunications», en tant qu'établissement public, doté de la personnalité morale et de l'autonomie financière, soumis à la tutelle de l'Etat.

- **En 2010**, Poste Maroc connait la transformation de son statut, en Société Anonyme et la filialisation de ses services financiers via la création d'Al Barid Bank, qui joue un rôle incontournable dans la bancarisation au Maroc.

- **En 2011**, Poste Maroc a obtenu l'agrément de l'ANRT en tant que 1er opérateur de certification électronique pour les échanges dématérialisés. Ce nouveau service a reçu d'ailleurs le prix spécial jury de l'administration électronique «e-mtiaz 2011», décerné par le Ministère de la Modernisation des Secteurs Publics.

- **En 2012**, Poste Maroc célèbre le centenaire des timbre-poste marocains, qui fut marqué par l'édition des timbres-poste audio, une première dans le monde arabe et africain, car à l'échelle internationale il n'y avait que la Chine et les pays bas qui avaient précédé le Maroc dans l'utilisation de cette nouvelle technologie.

- **En 2013**, Poste Maroc acquiert 100% des parts Sociales de la SDTM, en pour suivant ainsi son positionnement dans son activité Messagerie – Colis – Logistique [1].

1.2. L'organigramme de Poste Maroc

Poste Maroc repose sur la structure organisationnelle présenté dans la figure 1 pour assurer sa mission au Maroc [1] :

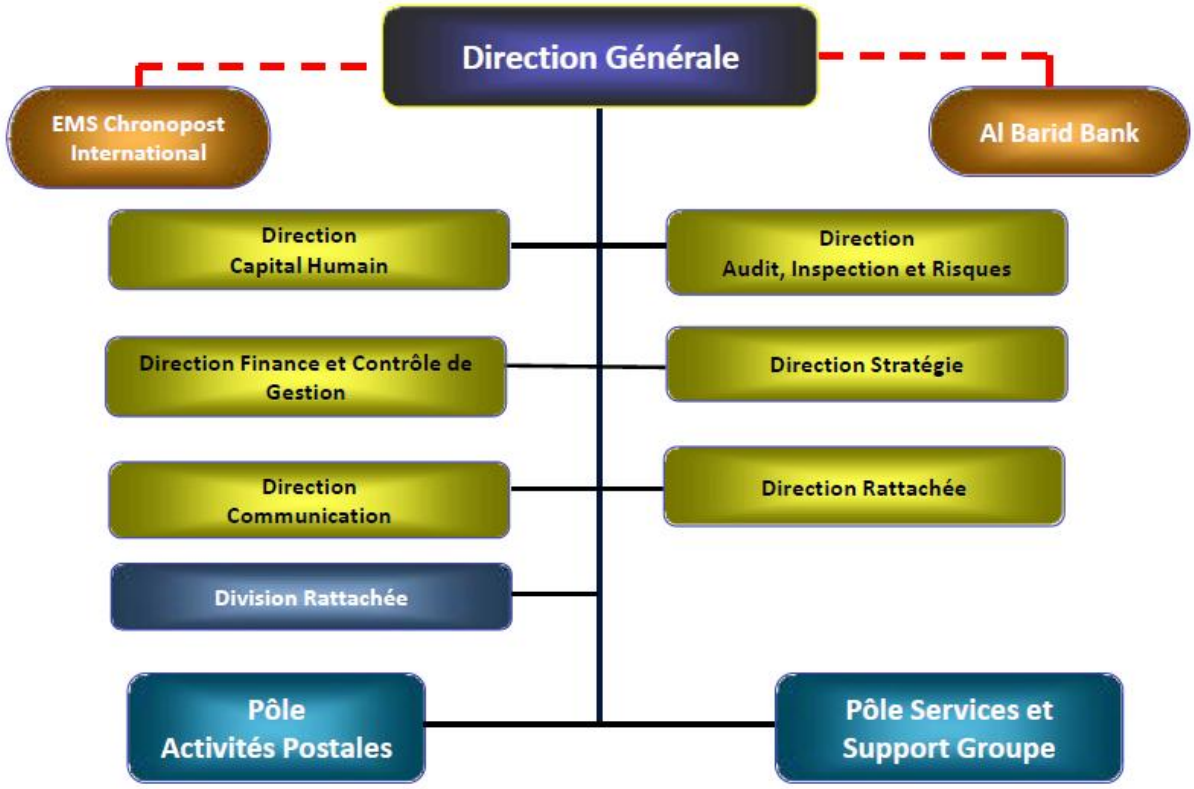


Figure 1: Organigramme de Poste Maroc

1.3. L'organigramme de la direction des systèmes d'information

Notre stage s'est déroulé au sein de la direction des systèmes d'information.LaDSIa pour mission de développer le système réseau avec le maximum d'efficacité et d'économie afin de fournir une meilleure qualité de service, d'élaborer un plan général d'informations et de suivre son exécution en collaboration avec les services intéressés. En plus, elle veille sur la sauvegarde de l'intégrité et la sécurité des données et des programmes du poste Maroc conformément à la législation en vigueur.

L'organigramme ci-après donne un aperçu général sur la structure de la direction des systèmes d'information (DSI):

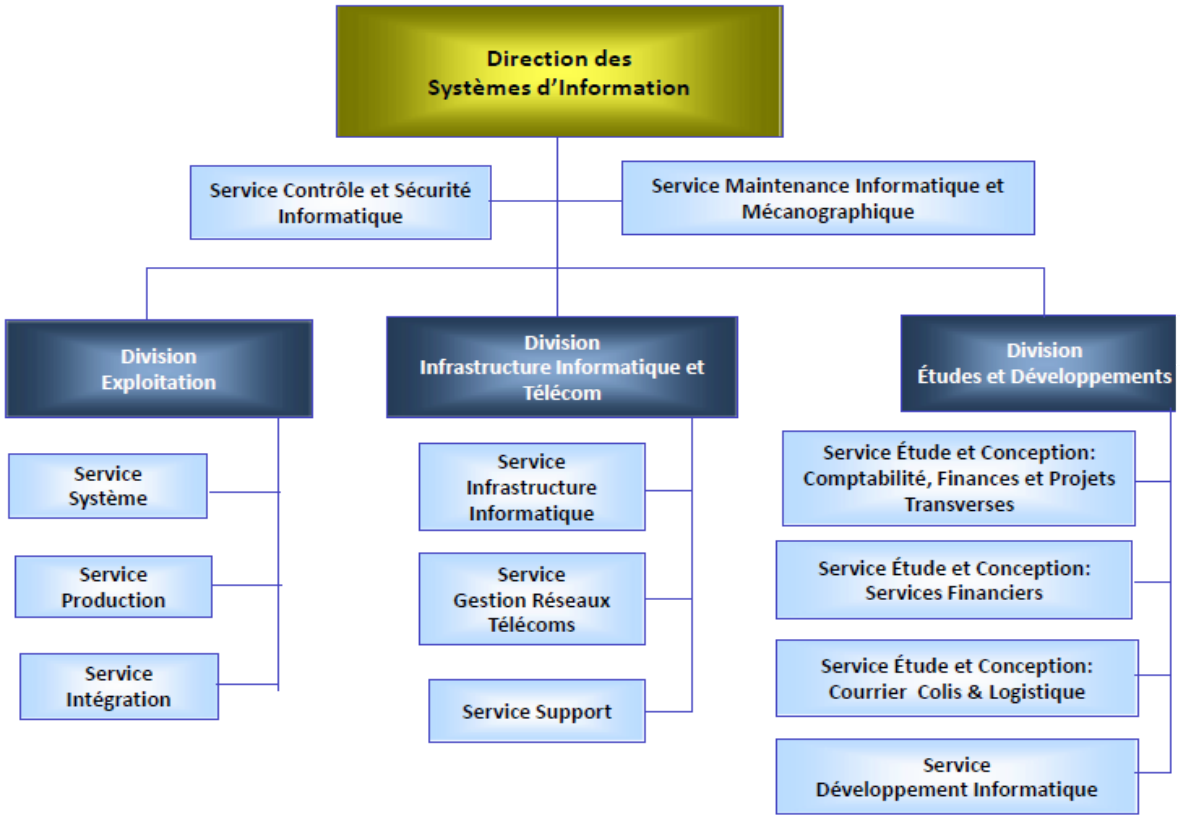


Figure 2: Organigramme de la DSI

1.4. Activités de Poste Maroc

Parmi ses activités, on trouve:

- Le traitement du courrier postal national et international,
- La collecte de l'épargne à travers la Caisse d'épargne nationale (CEN);
- La gestion du service des comptes courants des chèques postaux (CCP).
- La gestion d'un réseau de bureaux de poste qui distribuent, outre les produits postaux, des produits financiers et des assurances de sociétés filiales [1].

II. CAHIER DES CHARGES

2.1. Contexte du projet

En mode Best effort, lorsqu'un lien réseau est surchargé, tous les flux arrivant en entrée de l'équipement sont rejetés sans distinction. Un des concepts de la Qualité de Service est donc de hiérarchiser le trafic transitant dans le réseau en modifiant le comportement de l'équipement pour que les paquets rejetés ne soient pas confondus avec ceux considérés critiques et prioritaires par l'administrateur réseau. C'est dans ce contexte que s'inscrit notre projet de fin d'études, qui est l'optimisation des ressources réseaux, par l'implémentation de la QoS.

2.2. Objectifs

Dans l'objectif d'optimiser les ressources réseaux, on doit mettre en œuvre la Qualité de Service (QoS) au sein de l'infrastructure réseau Poste Maroc.

Les objectifs de notre projet sont :

- Améliorer la QoS dans l'infrastructure réseau de Poste Maroc.
- Fournir un système de priorisation des flux réseaux en un cas de saturation de réseau.
- Donner la priorité aux applications critiques en concurrence avec d'autres types de trafic.
- Optimiser la bande passante selon les besoins métiers de poste Maroc.

2.3. Architecture WAN de la Poste Maroc

Le réseau de Poste Maroc se compose de mille agences reliées au siège via le réseau MPLS de l'operateur IAM.

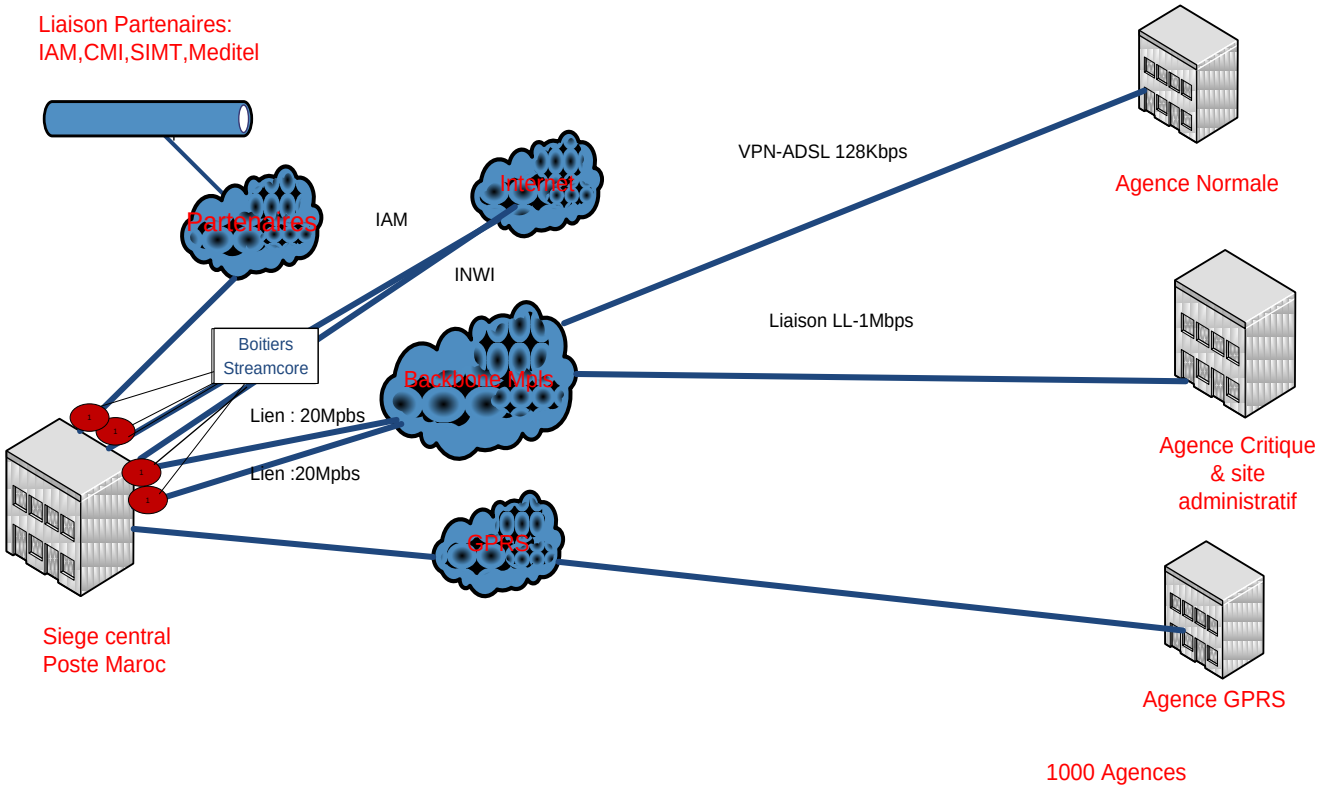


Figure 3: Architecture réseau de Poste Maroc.

Les lignes d'interconnexion WAN utilisées au sein de Poste Maroc sont de trois types :

- Des liaisons Spécialisées(LS) via MPLS
- Des Lignes VPN-ADSL
- Des lignes GPRS

- Deux liaisons spécialisées entre le siège et l'opérateur IAM de « 20Mbps »pour chacune reliant le Backbone MPLS.
- Des liaisons spécialisées entre les agences critiques et l'opérateur de « 1Mbps ».
- Liaison VPN_ADSL entre les agences normales et l'opérateur.
- Des boitiers STREAMCORE au niveau du siège pour le monitoring et l'implémentation de la QoS.
- La majorité des équipements réseaux de Poste Maroc sont de marque Cisco.

2.4. Les besoins

Les outils et les matériels requis :

- Deux ordinateurs personnels.
- Des équipements de type routeur « **Cisco 2660** » et Switch « **Cisco 2960** ».
- Le simulateur de réseau GNS3 sera utilisé pour nostests.
- Un générateur de trafic réseau **JPerf** pour pouvoir saturer le réseau.
- Autres logiciels vont être utilisés comme **VMware** et **Wireshark**.

III. PLANNING DU PROJET

Afin de mener à bien notre projet, nous avons planifié les différentes tâches en accordant à chacune une durée précise. La figure ci-dessous présente le planning prévisionnel du projet selon le diagramme de Gantt.

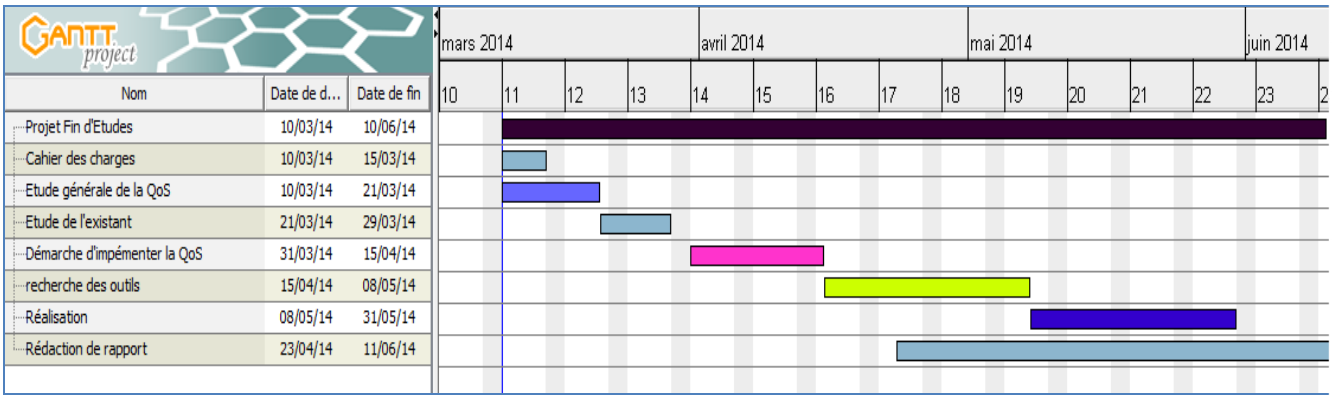


Figure 4: Diagramme de Gantt

Conclusion

Tout au long de ce chapitre, nous avons pu situer le cadre général de notre projet de fin d'études, à savoir la présentation de l'entreprise d'accueil, le cahier des charges proposé ainsi que le planning suivi pour la réalisation des différentes étapes du projet.

Dans le chapitre suivant, nous donnerons une étude théorique de la QoS.

Université Sidi Mohammed Ben Abdellah
Faculté Des Sciences et Techniques Fès
Département de Génie Electrique

CHAPITRE 2:ETUDE DE LA QOS

La réalisation de notre projet nécessite une étude approfondie sur certaines notions qui touchent non seulement le cadre général du projet, mais aussi son implémentation. Pour bien assimiler ces différentes notions, nous détaillons, dans un premier lieu, la définition et le principe de la Qualité de Service (QoS). Nous terminons ce chapitre avec présentation détaillée sur les modèles liés à la QoS.

I. INTRODUCTION

À ses débuts, les réseaux informatiques étaient destinés à transporter des données d'un point A à un point B. Au fil du temps les réseaux informatiques grandissaient, parallèlement, les types de protocoles traversant le biais de ces réseaux étaient de plus en plus transformés. Il en est de même pour la demande des nouvelles applications en temps réel, comme la téléphonie ou la visioconférence. Il n'y avait aucun moyen d'établir ces services en temps réel et de séparer le trafic jusqu'à la naissance de la qualité de service qui couvre d'un bout à l'autre tout le réseau. À l'aide de la QoS, on pourrait potentiellement appliquer diverses politiques qui auraient des retombées positives sur notre trafic agissant différemment pour différents types de services.

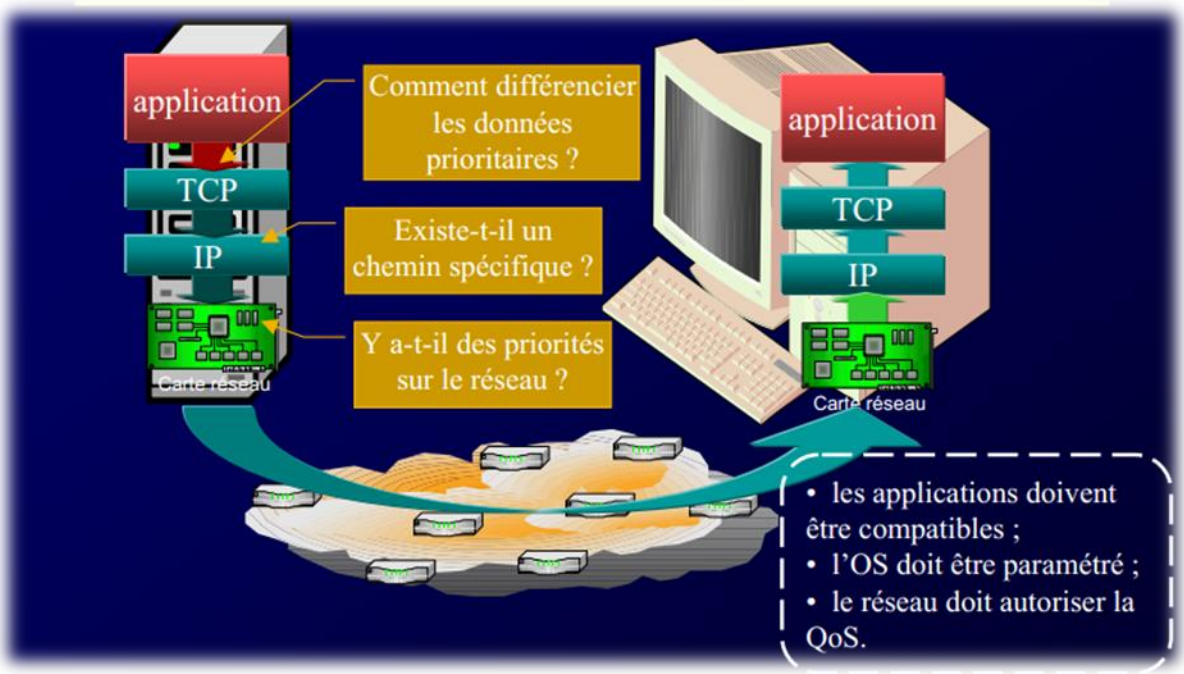


Figure 5: Problématique.

1.1. Définition de la Qualité de Service

La QoS est un sigle qui signifie « Quality of Service » en anglais, que l'on traduit par « qualité de service » en français.

La Qualité de Service est la capacité à véhiculer dans de bonnes conditions un type de trafic, en termes de disponibilité, débit, délais de transmission, taux de perte de paquets…

D'après l'IUT**:** La QoS est l'Ensemble des effets portant sur les performances d'un service de communication et qui détermine le degré de satisfaction d'un utilisateur de ce même service.

1.2. But de la Qualité de service

Le but de la QoS est donc d'optimiser les ressources du réseau et de garantir des bonnes performances aux applications critiques. La Qualité de Service sur les réseaux permet de hiérarchiser les applications ainsi que d'offrir aux utilisateurs des débits et des temps de réponse différenciés par application suivant les protocoles mis en œuvre au niveau de la couche réseau.

Elle permet ainsi aux fournisseurs de services (départements réseaux des entreprises, opérateurs…) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport applicatives sur leurs infrastructures IP. Selon le type d'un service envisagé, la qualité pourra résider dans:

- Le débit (téléchargement ou diffusion vidéo).
- Le délai (pour les applications ou la téléphonie).
- La disponibilité (accès à un service partagé).
- Le taux de pertes de paquets.

II. LES INDICATEURS DE LA QOS

Les principaux critères permettant d'apprécier la qualité de service sont les suivants [10] :

- **Débit** (en anglais bandwidth): parfois appelé bande passante, il définit le volume maximal d'information (bits) par unité de temps (bps).
- **Perte de paquet** (en anglais Packetloss): elle correspond au non délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau.
- **Gigue** (en anglais jitter) : C'est un paramètre important pour les applications communicantes de type voix ou vidéo où la gigue doit être la plus faible possible. La gigue est due principalement aux délais de transferts variables dans les nœuds du réseau (switches et routeurs).
- **Latence** (en anglais delay) : elle caractérise le retard entre l'émission et la réception d'un paquet[12].

III. LES NIVEAUX DE LA QOS

Le terme « niveau de service » définit le niveau d'exigence pour la capacité d'un réseau à fournir un service point à point ou de bout en bout avec un trafic donné. On définit généralement trois niveaux de QoS :

- **Meilleur effort**(en anglais ***best effort***), ne fournissant aucune différenciation entre plusieurs flux réseaux et ne permettant aucune garantie. Ce niveau de service est ainsi parfois appelé lack of QoS.
- **Service différencié**(en anglais ***Differenciated service*** ou soft QoS), permettant de définir des niveaux de priorité aux différents flux réseau sans toutefois fournir une garantie stricte.
- **Service garanti**(en anglais guaranteed service ou hard QoS), consistant à réserver des ressources réseau pour certains types de flux. Le principal mécanisme utilisé pour obtenir un tel niveau de service est RSVP (Resource Reservation Protocol, traduisez Protocole de réservation de ressources) [11].

IV. LES MODELES DE LA QUALITE DE SERVICE

Afin de garantir cette qualité de service, deux modèles se sont présentés:

- Integrated Services (IntServ).
- Differenciated Services (DiffServ).

4.1. Le modèle d'IntServ

Le modèle de l'architecture IntServ a été défini dans IETF RFC 1633.Il fournit une qualité de service garantie sur les réseaux IP. Ce modèle utilise le protocole de signalisation RSVP pour réserver des ressources sur tous les éléments du réseau pour un flux particulier.

IntServ utilise le protocole de réservation de ressources (RSVP) pour signaler explicitement les besoins de qualité de service de trafic d'une application sur les appareils dans le chemin de bout en bout à travers le réseau. Si chaque dispositif de réseau le long du chemin peut réserver la bande passante nécessaire, l'application d'origine peut commencer à transmettre.

a. Le protocole RSVP

Le protocole RSVP fonctionne de la manière suivante : la source émet un message PATH et les routeurs traversés par ce message peuvent y insérer des éléments décrivant l'état du réseau. A la réception, le destinataire décide d'accepter les conditions proposées ou demande une amélioration de la qualité de service. Le destinataire émet un message RESV qui remonte le chemin tracé par le message PATH et réserve un débit de transmission sur tous les routeurs. Chaque routeur décide s'il peut accepter la réservation ou pas.

- Message Path : On définit le chemin à emprunter. Envoi régulier.
- Message Resv : On réserve les ressources sur les équipements traversés.

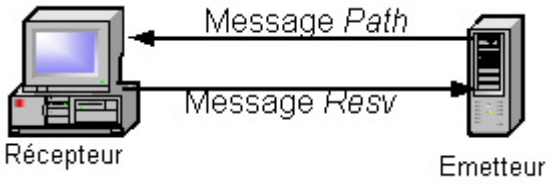


Figure 6: Fonctionnement du protocole RSVP.

Dans ce modèle, les routeurs réservent les ressources pour un flot de données spécifiques en mémorisant des informations d'états. Il est important de rafraîchir périodiquement les informations au cas où il y a eu un changement de la route empruntée par le flot [8].

b. Limites du protocole RSVP

- Le nombre de flux individuels peut être très important. Par conséquent, le nombre de messages de contrôle peut être élevé et nécessite beaucoup de ressources au niveau de chaque routeur.
- Des politiques doivent être mises en place pour déterminer quand, où et pour qui les ressources peuvent être réservées.
- Des règles de sécurité doivent être mises en place pour garantirl'interdiction d'effectuer des réservations de ressources par les utilisateurs non autorisés.
- Peu d'industriels ont implanté IntServ à grande échelle.

4.2. Le modèle DiffServ

a. L'Objectif du DiffServ

Services différenciés (DiffServ ou DS) est un protocole permettant de spécifier et de contrôler le trafic réseau en classe afin que certains types de trafic obtiennent priorité, par exemple, le trafic en temps réel, ce qui nécessite un flux relativement continu de données, pourrait obtenir la priorité sur d'autres types de trafic. Services différenciés est la méthode la plus avancée pour la gestion du trafic en termes de ce qui est appelé la classe de service.Pour un ensemble donné de règles de déplacement de paquets, un paquet est donné à l'un des 64 comportements de transmission possibles ; par des comportements dits de sauts (PHB). Un champ de six bits, connu sous le nom des services différenciés Code Point (DSCP), dans l'entête du protocole Internet IP spécifie le comportement par saut pour un débit donné de paquets [8].

b. Définition du champ DSCP

C'est un champ de remplacement de l'en-tête IP nommé champ DiffServ (DS) défini afin de constituer un ensemble étendu du champ TOS de IPv4 [Figure 7]. Il est utilisé pour désigner son comportement par saut. De plus, il détermine quel traitement d'acheminement subira un paquet. Seulement, six bits du champ DS sont utilisés comme DSCP pour sélectionner le PHB [8].

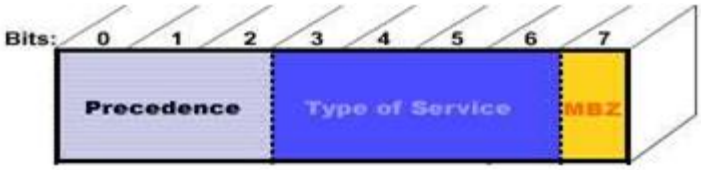


Figure 7: Composition du champ ToS.

La signification de chaque bit de l'octet DSCP est détaillée dans la figure suivante:

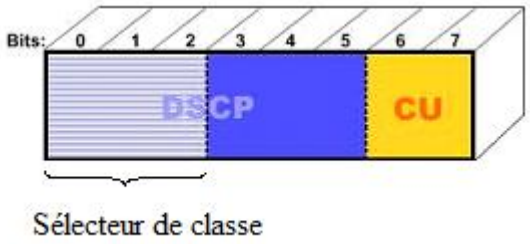


Figure 8: Composition du champ DSCP.

- **Les bits 0 à 2 : Class Selector**

Les codes DSCP de type xxx000 (ou x a la valeur 1 ou 0) correspondent aux classes de services principales. Ceux-ci seront associés aux PHB qui permettront le traitement différencié des flux dans les routeurs intermédiaires. Plus la valeur de code point est élevée, plus le flux correspondant sera prioritaire [8].

- **Les bits 0 à 5 : DSCP** (Differentiated Service Code Point)

Ce champ étend les sélecteurs de classes (bits 0 à 2) via 3 bits supplémentaires. On obtient ainsi une granularité supplémentaire (8 sous-classes par sélecteur de classe).

- **Les bits 5 à 7 : CU** (Currently Unused)

Ce champ **CU** est actuellement non utilisé.

c. Le comportement par saut : PHB (Per Hop Behaviour)

Le champ DSCP est définit par les routeurs de périphérie, il permet d'indiquer aux routeurs du cœur le comportement qu'ils doivent adopter en fonction de sa valeur. Ce comportement s'appelle le **P**er **H**op **B**ehaviour (comportement par saut). Le modèle DiffServ applique 4 classes de traitement:

- **PHB par défaut:** Le PHB par défaut a une valeur binaire de 000000. Elle est utilisée pour marquer le trafic comme meilleur effort ou essentiellement aucun QoS.
- **Expedited Forwarding (EF) PHB :** à une valeur binaire de 101110 ou une valeur décimale de 46. L'PHB de transmission accélérée est utilisée sur le trafic qui a des caractéristiques comme faible retard, faible perte et faible gigue.
- **Assured Forwarding (AF) PHB:** regroupe 4 classes de priorité selon ce tableau ci-dessous :

	Classe 1	Classe 2	Classe 3	Classe 4
Faible baisse	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Baisse moyenne	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
Haut de baisse	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

Tableau 1: Les classes de priorité.

- **Sélecteur de classe(CS) PHB:** Ces valeurs DSCP équivalentes sont appelés le sélecteur de classe des valeurs. Cela est présenté dans le tableau ci-dessous.

Binaire	Priorité IP	DSCP
000 000	0	Par défaut(0)
001 000	1	CS1(8)
010 000	2	CS2(16)
011 000	3	CS3(32)
100 000	4	CS4(40)
101 000	5	CS5(48)
110 000	6	CS6(48)
111 000	7	CS7(56)

Tableau 2: Les sélecteurs de classe.

V. LES MECANISMES DE GESTION DE LA QOS

Les règles de classification de trafic identifient le sous-ensemble de trafic qui peut recevoir un service différencié par conditionnement et/ou mis en correspondance avec un ou plusieurs BA (par remarquage de DSCP) à l'intérieur du domaine DS.

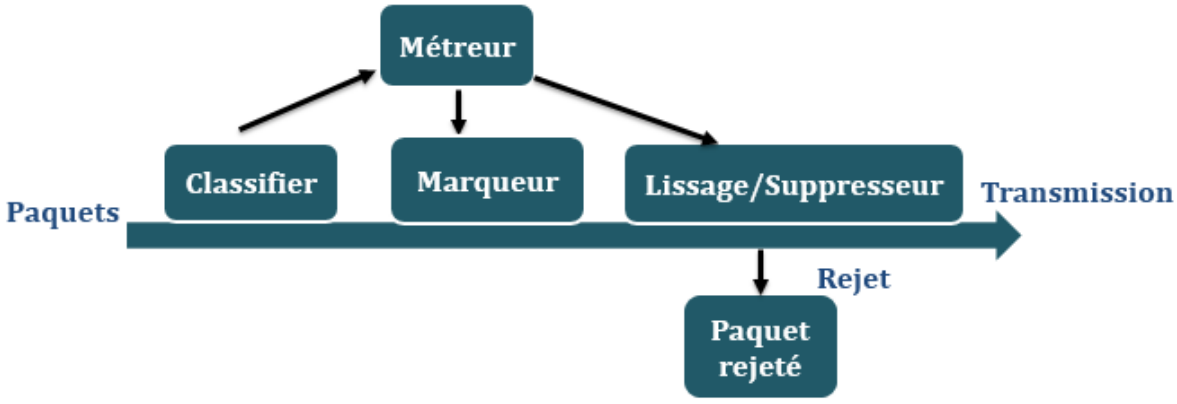


Figure 9: Mécanismes de gestion de la QoS.

- **Classifier :** Il s'agit de trier les paquets selon le contenu de certains champs de l'en-tête du paquet. Deux types de « classifier » sont définis :

- Le « Behavior Agregate (**BA**) Classifier » qui classifie les paquets uniquement en fonction du DSCP.

- Le « Multi Field (MF) Classifier » qui classifie les paquets selon des règles beaucoup plus complexes telles que : adresse source/adresse destination, DSCP, protocole, port source et port destination.

- **Le métreur (meter):** Il mesure le trafic pour vérifier qu'il est conforme au profil déterminé dans le contrat avec l'utilisateur. Il permet aux autres composants de mettre en œuvre le contrôle de trafic.

- **Le marqueur (Marker):**Le « **Marker** » positionne le champ DSCP à une valeur particulière et ajoute le paquet marqué à un agrégat particulier. Le Marker peut être configuré pour « marquer » un paquet avec un simple DSCP ou avec un ensemble de DSCP utilisé pour sélectionner un PHB dans un Groupe des PHBs, selon l'état du « Meter ». C'est le cas des « Multicolore Markers ». Le « Marker » peut également être amené à changer le DSCP d'un paquet, on dit alors qu'il a remarqué le paquet.

- **Le lisseur (Shaper) :** Le « **Shaper** » lisse le trafic en le retardant pour qu'il ne dépasse pas le débit contractuel associé au profil défini dans le contrat avec l'utilisateur.

- **Le suppresseur(Dropper) :** Il élimine le trafic dépassant le débit contractuel associé au profil du contrat de service usager.

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 deux modèles l'IntServ et le DiffServ.

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.

CHAPITRE 3:ETUDE DE L'EXISTANT ET SOLUTION ADOPTEE

Ce chapitre, est composé de deux parties, la première partie est consacrée à l'étude de l'infrastructure existante pour dégager ses points faibles et ses points forts .La deuxième traite de l'étude comparative entre la politique existante et la solution adoptée.

I. ARCHITECTURE

L'infrastructure globale du réseau de poste Maroc dispose de deux types : un réseau local Lan et un inter-site (WAN), comme présentés dans la figure 3.

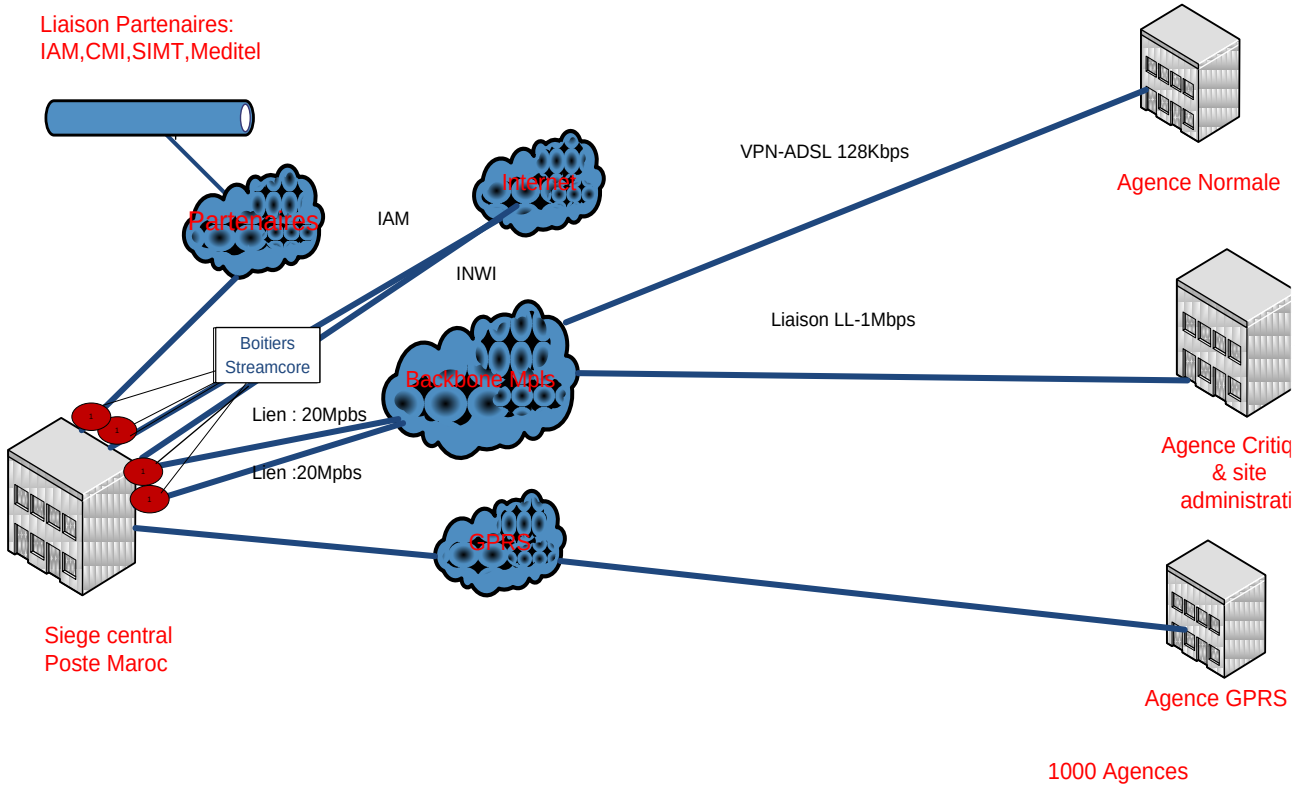


Figure 10: Réseau WAN de Poste Maroc.

Nous constatons que le siège possède quatreéquipements StreamCore répartis comme suit :

- Deuxau niveau de la liaison WAN
- Un pour les partenaires
- Un pour l'accès VPN vers l'internet

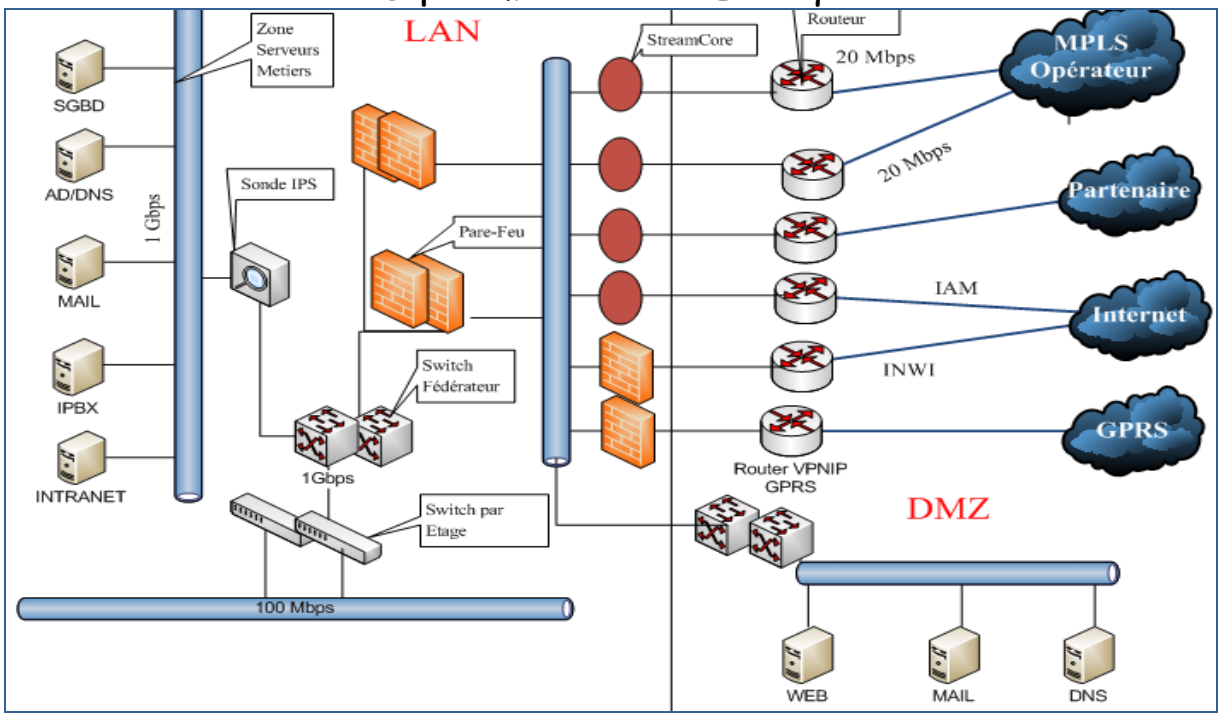


Figure 11:Réseau LAN de Poste Maroc.

II. DESCRIPTION DE L'EXISTANT

Le site central se base dans son infrastructure sur des équipements Cisco (Switch, routeur, …) et des boitiers QOS de type StreamCore.

L'infrastructure réseau et sécurité de poste Maroc est composé de quatre accès:

1. Un Accès aux différentes agences Via le réseau MPLS de l'operateur avec deux liaisons de 20Mbps chacune reliant le siège au nuage MPLS de l'operateur IAM, et il existe deux types d'agences :
    a. **Agence Critique**: accès via le réseau MPLS de l'operateur IAM avec une liaison Louée (LL) de 1Mbps au nombre de 57 agences.
    b. **Agence normale**: accès via le réseau MPLS de l'operateur IAM avec une liaison VPN-ADSL de 128kbps.
2. Un Accès des Différents partenaires (IAM, CMI, SIMT, Meditel) vers le siège.
3. Un Accès des agences non desservie par la technologie MPLS passent via GPRSavec une liaison Tunnel IP Sec vers le siège.
4. Accès Internet :

Il existe deuxaccès Internet (IAM, Inwi)

a. **Accès IAM**

b. **Accès Inwi**

III. ANALYSE DE L'EXISTANT

3.1. Accès des sites critique vers le siège via MPLS

Ce type de sites étant au nombre de centaines, ils sont caractérisés par leurpositionnement géographique et leur flux nombreux de la clientèle. Pour cela, ces sites génèrent un trafic important et critique y compris la signalisation de la Téléphonie sur IP.

3.2. Accès des sites Administratifs

Situé dans chaque grande ville, utilisant une liaison louée de 1Mbps vers le siège en passant par le réseau MPLS de l'opérateur. Les échanges de flux vers le siège sont de types Financiers, administratifs, ainsi ils utilisent de la visioconférence pour des réunions métiers entre certains sites administratifs et le siège.

3.3. Les Agences Normales

Elles constituent la majorité des agences de Poste Maroc existant dans toutes les villes avec un nombre d'utilisateurs peu nombreux par rapport aux sites critiques et administratifs, générant un trafic web (financier, Courier & Messagerie) vers le siège.

Ces agences-là passent par le réseau MPLS via liaison VPN-ADSL de 128 kbps ou GPRS dans les régions non desservies par la technologie MPLS.

3.4. Accès Internet

Il existe deux accès internet ce qui permet la séparation des flux métiers, des flux des différents utilisateurs (navigation web, mail personnel, streaming…).

a. **Accès IAM**: utilisé comme accès métier afin que le personnel puisse se connecter à la zone DMZ publique pour les consultations des différents e-mails et il permet aussi l'accès aux serveurs métiers via VPN.

b. **Accès Inwi**: utilisé pour la navigation internet du personnel du siège.

3.5. Outil StreamCore

La politique existante et qui a pour butd'optimiser le flux des applications au sein de Poste Maroc, est basée sur l'implémentation des boitiers StreamCore au niveau du siège. Une présentation générale sur l'outil s'avère donc nécessaire.

a. Présentation

StreamCore est une solution automatisée de reporting, supervision, QoS, troubleshooting et contrôle dynamique des performances pour gérer les applications métiers et les communications temps-réel (VoIP, visioconférence…)

Les solutions StreamCore permettent de :

- Superviser n'importe quelle application ou communication, et tout type de service de Cloud public/privé sur le réseau.
- Mesurer et assurer les niveaux de service fournis aux utilisateurs.
- Proposer des rapports synthétiques aux clients internes tels que les unités métier.
- Diagnostiquer les problèmes de performance en temps réel ou dans le passé.
- Garantir la meilleure qualité possible pour les applications interactives ou les communications temps réel.
- Proposer des services managés innovants et uniques.

b. Gamme et Architecture

La gamme de produits **StreamCore** se compose des **StreamGroomers** (SG), équipements de gestion du trafic, et du **StreamGroomers Manager (**SGM) qui permet une administration centralisée de toutes les fonctionnalités : configuration, monitoring temps réel, supervision, reporting et contrôle des performances. En complément, un **StreamCollector** peut être associé au SGM pour donner une visibilité long-terme et détaillée sur les sessions gérées par les StreamGroomers.

Enfin, le déploiement peut être automatisé en configurant simplement l'ensemble des paramètres initiaux par l'intermédiaire d'une clé USB [7].

- La gamme utilisée à Poste Maroc est de type StreamGroomers SG1600.

Figure 12: StreamGroomers SG1600.

c. Implémentation de la QoS sur StreamCore

Le moteur QoS de StreamCore donne par défaut la priorité aux applications de données critiques et Voix sur le réseau:

- La bande passante est optimisée selon les besoins métier,
- Les trafics secondaires ou perturbateurs (Internet récréatif, mise à jour antivirus ou système d'exploitation,…) n'entravent pas le bon déroulement de l'activité.
- Adapter dynamiquement le nombre de sessions actives par application
- Régulent naturellement les débits - sans perte de paquet
- Réaffectation dynamique de la bande passante.
- Répartition équitable de la bande passante entre les sessions actives.
- Réservation de bande passante par session permet de prendre en considération les codecs utilisés.
- QoS de bout en bout, Compression, équilibrage de charge WAN, Chiffrement.

3.6. Analyse de la QOS au sein de Poste Maroc

D'après notre utilisation de l'outil StreamCore, nous constatons que le trafic de Poste Maroc au niveau du siège est divisé en quatre catégories:

- Flux services infrastructures: Outils supervision, visioconférence, Active Directory, antivirus, Mail, ToIP, Autres.
- Flux services métiers: Données financiers, données Courier et Messagerie.
- Flux services partenaires: IMMONET Partenaires Financiers, Partenaires Courier et Messagerie.
- Flux services communs: E-learning, Citrix, HelpDesk, autres.

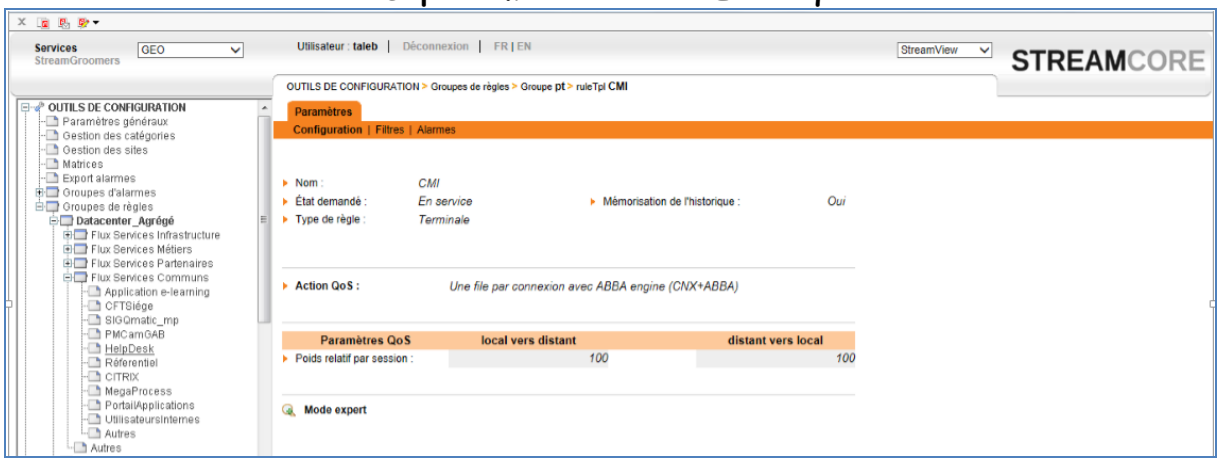


Figure 13: Le flux services communs sous StreamCore.

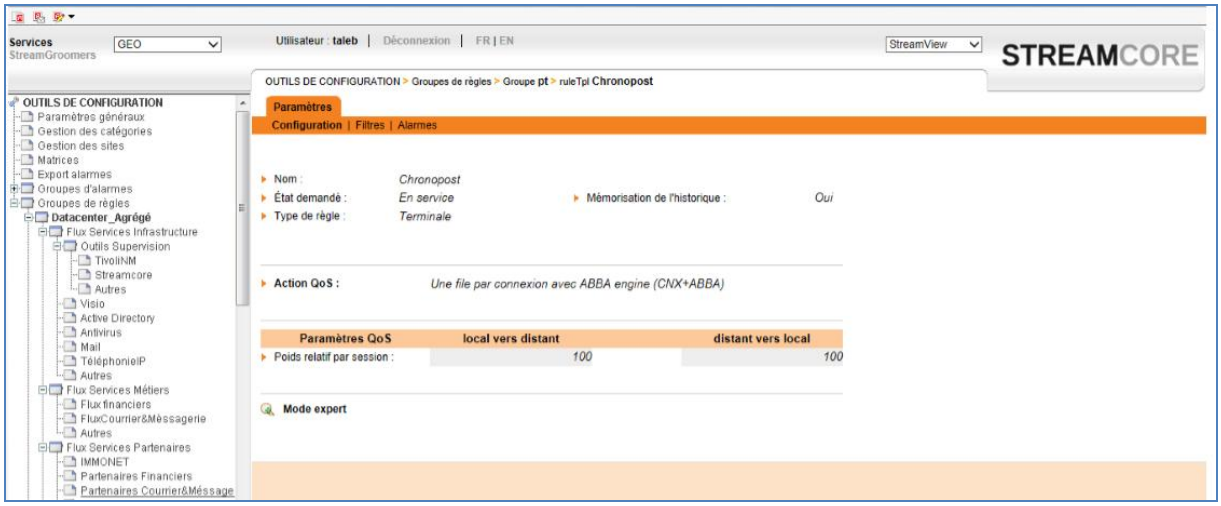


Figure 14: Les flux applicatifs sous StreamCore.

Différemment à ce qui est conçu, les responsables de l'implémentation de la QoS au sein de poste Maroc ont divisé chaque flux passant en deuxpriorités:

- Flux prioritaire présente80% de trafic dans poste Maroc, et à ce niveau, tous ces flux ont la même priorité, dont la majeure partie est de type Http.
- Flux non prioritaire présentele reste de trafic généré 20% (Mail, FTP, autres).

Taux d'utilisation du siègevers le réseau WAN:

Figure 15: Taux d'utilisation WAN vers Siège-Siège vers WAN.

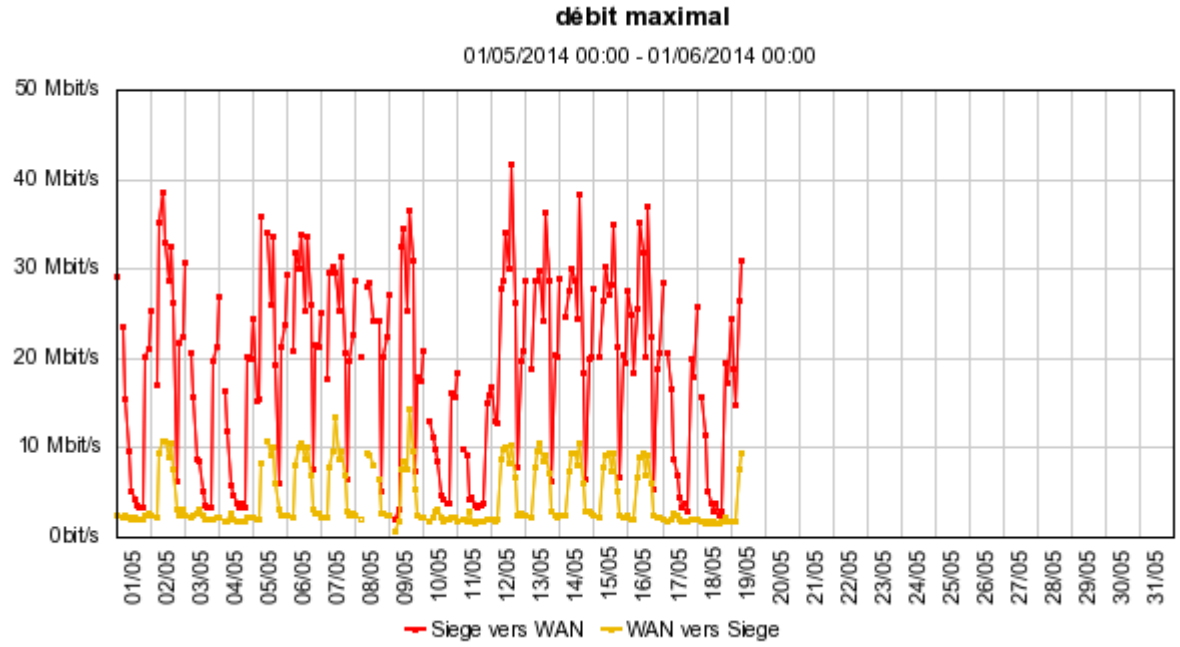


Figure 16: Débit maximal -siège vers WAN.

Nous remarquons qu'il y a une saturation de réseau par l'augmentation d'utilisation des flux applicatifs sortant du siège vers le réseau WAN. Ceci montre que laQoS n'est pas appliquéeet que l'outil StreamCore est utilisé en monitoring.

IV. CRITIQUE DE L'EXISTANT

Après l'analyse de l'infrastructure globale de Poste Maroc, nous présenterons quelques remarques et recommandations:

- **Equipement StreamCore**:

En cas de non redondance de l'outil StreamCore la panne fera arrêter tout le système jusqu'à ce qu'il soit réparé, et ainsi il retournera en mode « best effort ».

- **Qualité de Service:**

-La qualité de service est utilisée juste au niveau du siège, il est fortement recommandé de l'ajouter au niveau des agences critiques et administratives à cause de l'importance de ces flux applicatifs : Visioconférence, signalisation de la voix, donnée Métiers…

-Les flux au sein de Poste Maroc sont divisés seulement en deux(2) priorités. Or, tous les flux n'ayant pas la même contrainte de temps, de débit et le taux de perte de paquet alors pour garantir une bonne gestion de la qualité de Service, il est préférable d'avoir quatre (4) priorités pour les différents flux qui sont:

- La signalisation pour la voix, la visioconférence
- E-Learning, données Financiers.
- Courier et Messagerie.
- Best effort

NB : La voix ne passe pas par le réseau IP seulement la signalisation.

-Améliorer la QoSdans les boitiers StreamCore au niveau du siège, pour alléger le traitement avec les mêmes niveaux de priorités cité ci-dessus.

- Essayer de limiter les trafics de loisirs tels que streaming et les réseaux sociaux, en se basant sur un Filtrage Url pour les accès Internet des utilisateurs durant les heures de travail, car nous remarquons une grande partie de flux qui passent de ce genre.

-Ajouter un pare feu au niveau du lien reliant le siège aux différents partenaires car cela peut être une source d'attaque.

Le choix de l'outil StreamCore nous a poussé à faire une étude comparative avec un outil considéré comme leader du marché réseau qui est Cisco. Pour savoir si nous avons effectué le bon choix ou non, nous renvoyons à la partie suivante.

V. ETUDE COMPARATIVE

Dans cette partie nous allons présenter une étude comparative entre l'outil StreamCore et l'équipement Cisco au niveau de la mise en place de la QoS, à fin de trouver la bonne solution qui va répondre aux attentes de poste Maroc pour l'implémentation de la QoS dans les sites critiques et administratifs.

5.1. Méthodologie adoptée

Pour réussir cette étude comparative, nous nous sommes basé sur la méthode QSOS, normalement c'est une méthode d'évaluation de logiciels libres, mais nous avons juste opté leur principe et méthode de comparaison pour arriver à des meilleures résultats.

QSOS consiste en un processus itératif en quatre étapes:

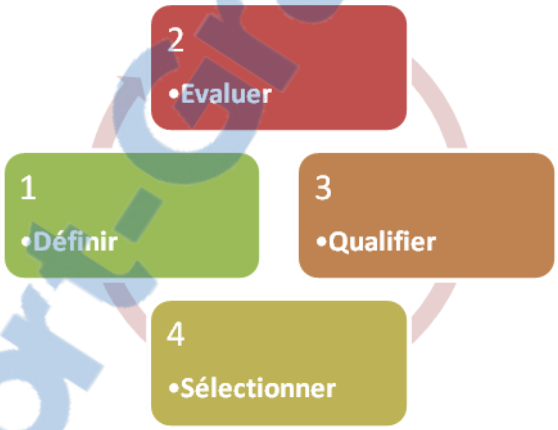


Figure 17: Schéma générale de la méthode QSOS.

Les objectifs de cette méthode sont cités ci-dessous:

- Définir les données de référentiel (types de licences, types de communautés, grilles de couverture fonctionnelle par domaine...).

- Évaluer les équipements selon trois axes principaux: couverture fonctionnelle, risques du point de vue de l'entreprise utilisatrice, risques du point de vue du fournisseur de services (expertise, formation, support). Chaque axe est constitué d'un certain nombre de critères.

Les critères seront notés selon le barème suivant :

Fonctionnalité	Note
Non couverte	0
Partiellement couverte	1
Totalement couverte	2

Figure 18: Barème de la méthode QSOS.

- Qualifier le contexte spécifique d'une entreprise (ou d'un utilisateur) en effectuant une pondération des critères précédents;
- Sélectionner et comparer les logiciels répondant aux besoins.

Le mode d'évaluation définit le score de chaque critère de la façon suivante:

[Score critère = Note * Coefficient contextuel]

Ces critères ci-dessous et leurs coefficients sont choisis à base de leur importance pour Poste Maroc et après validation de l'encadrant.

5.2. Tableaux comparatifs

Les tableaux ci-dessous représentent des grilles de critères basés sur la méthode QSOS pour les deux équipements (voir annexe A pour bien comprendre les critères choisis) :

StreamCore :

La grille de critères notée pour l'outil StreamCore se trouve ci-dessous :

Equipement		StreamCore	
Critère	**Note**	**Coef**	**Total**

AXE 1 : Point De Vue Du Fournisseur De Services			
Ancienneté sur le marché	0	2	0
Documentation	1	2	2
Popularité	0	1	0
Historique problème connu	1	2	2
Durée de vie de l'équipement	1	2	2
AXE 2 : Point De Vue De L'entreprise Utilisatrice			
Prix	1	2	1
Interface graphique	2	1	2
CPU	2	1	2
Homogénéité avec l'opérateur	0	2	0
Formation des ingénieurs	1	2	2
AXE 3 :Couverture Fonctionnelle			
Manipulation graphique	2	1	2
Mise à jour de configuration	2	1	2
Manipulation des critères QoS	2	2	4
Sécurité de trafic	2	1	2
Résultats après QoS	2	2	4
Autres fonctions: supervision, reporting	2	1	2
	Total		29

Tableau 3: Evaluation pour StreamCore.

Cisco :

La grille de critères notée pour l'outil Cisco se trouve ci-dessous :

Equipement			Cisco
Critère	**Note**	**Coef**	**Total**
AXE 1 : Point De Vue Du Fournisseur De Services			
Ancienneté sur le marché	2	2	4
Documentation	2	2	4
Popularité	2	1	2

Historique problème connu	1	2	2
Durée de vie de l'équipement	2	2	4
AXE 2 : Point De Vue De L'entreprise Utilisatrice			
Prix	2	2	4
Interface graphique	1	1	1
CPU	1	1	1
Homogénéité avec l'opérateur	2	2	4
Formation des ingénieurs	2	2	4
AXE 3 :Couverture Fonctionnelle			
Manipulation graphique	1	1	1
Mise à jour de configuration	2	1	2
Manipulation des critères QoS	2	2	4
Sécurité de trafic	2	1	2
Résultats après QoS	2	2	4
Autres fonctions : supervision, reporting	1	1	1
	Total		44

Tableau 4: Evaluation pour Cisco.

5.3. Solutions envisagée

Tenant compte de cette étude, nous avons proposé Cisco, vu qu'il est leader du marché, fiable, sécurisé, homogène avec l'opérateur IAM. Déjà plus 95% des équipements du réseau Poste Maroc sont Cisco, il suffit juste d'ajouter la configuration idéale pour la QOS.

Conclusion

La description détaillée de l'architecture existante qui couvre ce chapitre nous a permis de voir les problèmes à résoudre dans le contexte actuel. Quant à la partie critique de l'existant, elle nous a permis de dégager et de suggérer des solutions et recommandations pour les ressources réseaux au sein de Poste Maroc.

CHAPITRE 4:DEMARCHE D'IMPLEMENTER LA QOS

En se basant sur l'étude de la QoS et de l'existant, nous proposons une démarche pour la mise en place de la QoS qui parait adéquate. Pour cela nous allons présenter la matrice de flux et la politique de classification adoptée pour chaque application.

I. ETUDE DES APPLICATIONS EXISTANTES

1.1. Audit du système

L'intérêt de réaliser un audit est de pouvoir mesurerle trafic WAN et comprendre qui utilise le réseau. L'audit nous permet également la visibilité du trafic réseau, à savoir les applications existantes et son degré de priorité. Par la suite nous allons répertorier l'ensemble des applications existantes au sein de Poste Maroc qui vont être remis dans une matrice de flux.

a. Audit du Réseau

Nous avons pu recenser le flux applicatifs circulant dans le réseau WAN, suite à notreobservation de l'analyseur de StreamCore, nous avons constaté quecet analyseur produit des graphes en fonction des données stockés sur le serveur.Le Tableau 7 représente les protocoles pour les flux répertoriés:

Applications	Protocole
TivoliNM	SNMP
Visioconférence	SIP
Active Directory	LDAP, DNS
Mail	SMTP
Téléphonie	SIP, POP3
Financiers	https
Courrier & Messager	http
Partenaires Financier	https
Partenaire Courier & Messagerie	http
Autres	FTP, DNS, IMAP,POP3
Helpdesk	SIP
e-learning	http
CITRIX	ICA

Tableau 5: Les applications existantes.

b. Audit du Busines

Etant une étape métier, elle consiste à contacter les différents utilisateurs du système de Poste Maroc afin de collecter les données sur les applications utilisées, voire le niveau d'importance de chaque application afin de classifier les différentes applications tournant dans le réseau.

Cette étape se basera sur ce questionnaire:

- Quelle est l'applicationque vous utilisez le plus ?
- Quelle est l'objectif de l'application?
- Quelle est le seuil maximal en cas de disfonctionnement toléré pour l'application?

- Quel est le domaine d'utilité de l'application?
- Avez-vous d'autres applications moins importantes? si Oui reprendre le questionnaire

1.2. Matrice de flux de Poste Maroc

Cette matrice de flux présente les applications existantes et les agences qui les génèrent. Nous avons mentionné aussi dans cette matrice : l'adresse IP du serveur, le protocole de chaque application, ainsi que le port de destination et enfin le degré de criticité des applications.

Le tableau ci-dessous montre la matrice de flux utilisée au sein de Poste Maroc:

MATRICE DE FLUX POSTE MAROC					
SIEGE					
	Application	IP Serveur	Protocole	Port Dest	Criticité
Agen ritique	VoIP(Signalisation)	******	RTCP	5005	Premium
	Helpdesk	******	HTTP	80	Best Effort
	E-Learning	******	HTTP	80	Critique
	Courier & Messagerie(Poste)	******	HTTP	80	Normal
	Financiers	******	HTTPS	443	Critique
	Citrix	******	ICA	1494	Normal
	Active Directory	******	LDAP	389	Best Effort
	Mail	******	SMTP	25	Best Effort
	VoIP(Signalisation)	******	RTCP	5005	Premium
	Visioconférence	******	SIP	5061	Premium
e	Mail	******	SMTP	25	Best Effort
Adn stratif	AD	******	LDAP	389	Best Effort
R nal	Citrix	******	ICA	1494	Critique
	Helpdesk	******	HTTP	80	Normal
	Financiers (Barid Al Maghreb)	******	HTTPS	443	Critique
	Helpdesk	******	HTTP	80	Normal
	E-Learning	******	HTTP	80	Critique
	Courier & messagerie	******	HTTP	80	Normal
A nce	Financiers	******	HTTPS	443	Critique
	Citrix	******	ICA	1494	Critique
	Mail	******	SMTP	25	Best Effort
	Active Directory	******	LDAP	389	Best Effort

Tableau 6: Matrice de flux.

Cette matrice de flux se lit de la manière suivante :

Exemple :

De l'agence critique vers le siège, les flux VoIP sortant, Helpdesk, E-learning, courrier & Messagerie, les flux financiers, flux Citrix, Active Directory et Mail peuvent circuler dans cette portion de réseau.

Cette matrice nous permet d'avoir un aperçu général de ce qui circule sur le réseau entre différentes types d'agences vers le siège.

II. CLASSIFICATION DE FLUX

Après avoir récupéré le maximum d'informations sur les applications existantes dans le réseau et leur importance, nous avons adopté la politique de CISCO dans la classification des applications de site administratif et critique.

Nous avons définiquatre classes de qualité de service pour le transport des applications multimédia dans le réseau. La différence entre ces classes de QoS se base essentiellement sur des exigences sur la bande passante et la priorité de circulation.

Les quatre priorités pour les applications du site administratif sont présentées dans le tableau ci-dessous :

Classification des Flux	
Premium 4	Visioconférence, VoIP
Critique 3	E-learning, Financier
Normal 2	Courier Messagerie, Citrix
Best Effort 0	Autres

Tableau 7: Les classes de la Qualité de service.

Nous avons séparé le trafic en quatre classes de service:

1. Une classe de trafic 4 (**Premium**), destinée à véhiculer les trafics en temps réel d'un client de type Visioconférence et la signalisation de la voix (délai d'acheminement constant et très court).

2. Une classe de trafic 3 (**Critique**), destinée à véhiculer les trafics des applications critiques comme : E-learning et les données financières (délai d'acheminement court).

3. Une classe de trafic 2 (**Normal**), destinée à véhiculer les trafics des applications non critiques de type transaction (web) (délai d'acheminement minimal).

4. Une classe de trafic 0 (**Best effort**), destinée à véhiculer les trafics des applications non prioritaires ne disposant d'aucune garantie particulière (transfert de fichiers, Mail).

CONCLUSION

Au cours de ce chapitre, nous avons décrit les étapes nécessaires pour l'implémentation de la QoS dans notre prototype, à savoir l'audit des applications existantes et leur classification.

CHAPITRE5:MISE EN PLACE DE L'APPLICATION QOSET TESTS

Après avoir accompli la démarche d'implémenter la QoS, nous entamons dans ce chapitre la phase de mise en œuvre de la QoS. Nous commençons, tout d'abord, par la présentation des outils utilisés, ainsi que les tests et les résultats de notre prototype.

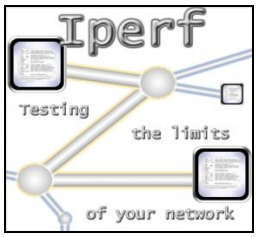
I. LES OUTILS UTILISES

Afin de ne pas perturber le trafic interne de Poste Maroc, ni d'altérer leurs serveurs http, nous avons travaillé avec les outils ci-dessous pour mettre en œuvre notre application:

1.1. Simulateur GNS3

GNS3 0.8.5est un simulateur graphique de réseaux qui vous permet de créer des topologies de réseaux complexes et d'en établir des simulations. Ce logiciel, en lien avec Dynamips (simulateur IOS), Dynagen (interface textuelle pour Dynamips) et Pemu (émulateur PIX) est un excellentoutil pour l'administration des réseaux CISCO [6].

1.2. JPerf: Générateur de trafic



JPerf 2.0.2 est un outil qui génère tout type de trafic avec un débit choisi. Cependant, il est restreint à une adresse cible unique. De plus, Jperf est fait pour fonctionner en mode client/serveur (un générateur de trafic et un serveur de récupération et interprétation des données) [2].

1.3. Wireshark

Wireshark est un analyseur de protocoles (sniffer). Celui-ci utilise directement l'interface Ethernet de votre machine pour réaliser la capture de toutes les informations circulant sur le réseau local sur lequel vous êtes connectés [5]. Il sera utilisé comme sonde réseau pour analyser les protocoles des flux générés.

1.4. VMware Workstation 10.0.1

C'est un puissant logiciel de création et d'utilisation de machines virtuelles qui permet aux développeurs et aux administrateurs des systèmes de révolutionner le développement, les tests et le déploiement des logiciels dans leurs entreprises [4].

Dans notre travail, nous avons utilisé deux machines virtuelles sur lesquelles nous avons installé le système linux Fédora pour les serveurs http, de façon à pouvoir générer le trafic nécessaire pour les différents tests.

II. LA MAQUETTE DE TEST

La figure suivante montre notre réseau WAN implémenté sous GNS3:

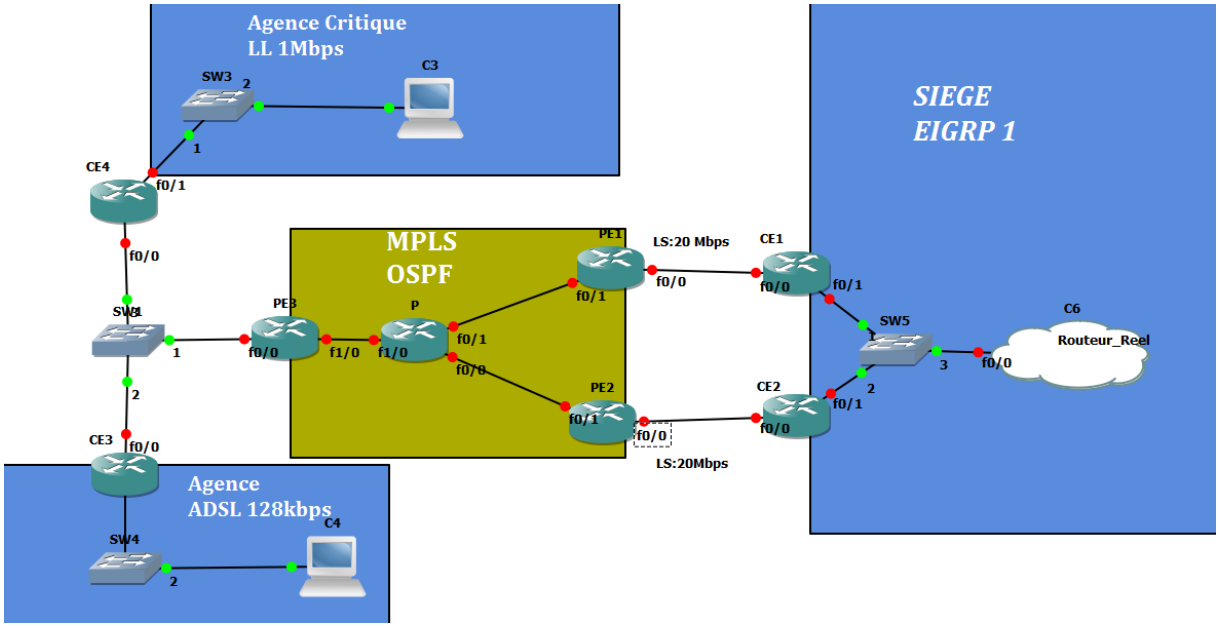


Figure 19:Réseau WAN implémentée sous GNS3.

Notre maquette de test est composée de:

- Un routeur Cisco 2660 réel et un Switch réel de type 2960 au niveau du siège.
- Un PC -Client au niveau de l'agence critique.
- Deux serveurs (web) au niveau du siège.
- Un réseau MPLS de l'opérateur IAM y compris les routeurs (PE3, P, PE1 et PE2).
- Pour connecter le WAN au LAN du siège l'encadrant a mis à notre disposition un Switch réel de type 2960 et un routeur Cisco 2660.

1.1. Adressage et configuration

Les agences étant reliées au siège via le MPLS, donc nous l'avons configuré en affectant les VRF à chaque agence pour une communication adéquate avec le siège. (Voir Annexe B, Figure B.3)

Pour le routage au niveau du siège et les agences nous avons utilisé le protocole EIGRP de Cisco étant un protocole qui permet un équilibrage de charge entre des liens à charge différente pour profiter de la redondance du lien au niveau du siège, le même protocole est utilisé entre les CE et les PE de l'opérateur (Voir Annexe B ,Figure B.2 et Figure B.3).

Nous avons eu du mal à trouver un générateur de trafic qui peut saturer le réseau, donc nous avons pensé à diminuer le débit des liens au niveau du siège jusqu'à **8kbps** par la commande **limite-Rate**. (Voir Annexe B, Figure B.2).

La répartition des adresses IP est fixée dans le tableau ci-dessous :

Routeur	Interface	IP
Routeur Réel	Fa0/0	172.16.1.1/24
	Fa0/1	192.168.2.0/24
CE1	Fa0/0	10.10.10.2/30
	Fa0/1	192.168.2.0/24
CE2	Fa0/0	10.10.11.2/30
	Fa0/1	192.168.2.0/24
CE3	Fa0/0	10.10.13.2/30
CE4	Fa0/0	10.10.12.2/30
	Fa0/1	10.10.45.0/24

Tableau 8: Adressage IP.

III. MISE EN PLACE DE LA QOS

Suite aux résultats obtenus après audit des flux applicatifs et la politique de classification, nous avons utilisé la configuration suivante au niveau du site administratif et du siège.

La QoS sera implémentée dans le routeur CE4 au niveau du site administratif.

a) La mise en place des ACLs

Nous avons utilisé des ACLs (Access Control List) étendues, permettant d'autoriser le trafic sous le réseau en fonction de l'adresse IP source, port destination adresse IP de destination et protocole.
La configuration des ACLs:

Agence Critique & Site Administratif	ip access-list extended CRITIQUE permit tcp any host 172.16.1.4 eq www permit tcp any host 172.16.1.2 eq 443 ip access-list extended NORMAL permit tcp any host 172.16.1.5 eq www ip access-list extended PREMIUM permit tcp any host 172.16.1.2 eq 5061 permit udp any host 172.16.1.2 eq 5061 permit tcp any host 172.16.1.2 eq 5005 permit udp any host 172.16.1.2 eq 5005
Siege	**ip access-list extended CRITIQUE** **permit tcp host 172.16.1.4 eq www 10.10.0.0 0.0.255.255** **permit tcp host 172.16.1.2 eq 443 10.10.0.0 0.0.255.255** **ip access-list extended NORMAL** **permit tcp host 172.16.1.5 eq www 10.10.0.0 0.0.255.255** **ip access-list extended PREMIUM** **permit tcp host 172.16.1.2 eq 5061 10.10.0.0 0.0.255.255** **permit udp host 172.16.1.2 eq 5061 10.10.0.0 0.0.255.25** **permit udp host 172.16.1.2 eq 5005 10.10.0.0 0.0.255.255** **permit tcp host 172.16.1.2 eq 5005 10.10.0.0 0.0.255.255**

Nous avons configuré quatre ACLs, PREMIUM, CRITIQUE, NORMAL et BEST_EFFORT. La liste PREMIUM permet au trafic utilisant le protocole TCP et UDP de passer à travers le routeur depuis n'importe quelle source avec un port de destination propre au protocole SIP (de visioconférence), vers toutes les destinations utilisant la même plage de port.

b) Classification des flux

La classification est le processus d'identification et de catégorisation du trafic dans différentes classes. C'est la partie la plus fondamentale de la mise en place de la QoS, sans elle tous les paquets seront traités de la même façon.

```
class-map match-all CRITIQUE_CLS
        match access-group name CRITIQUE
class-map match-all NORMAL_CLS
        match access-group name NORMAL
class-map match-all PREMIUM_CLS
        match access-group name PREMIUM
```

c) QoS Policy

A ce niveau nous avons affecté à chaque classe une priorité en se basant sur les résultats du chapitre quatre.

```
policy-map QOS_POLICY
class PREMIUM_CLS
        set precedence 4
class CRITIQUE_CLS
        set precedence 3
class NORMAL_CLS
        set precedence 2
class class-default
        set precedence 0
```

d) QoS Policy au niveau de l'interface

Au niveau des utilisateurs la politique adoptée est de type « Shaping ». Elle est appliquée en sortie du routeur.

```
service-policy output QOS_POLICY
```

IV. SIMULATION DE LA QOS

Après la mise en place de la QoS grâce à la configuration ci-dessus, nous avons essayé de simuler des flux allant du site administratif vers le siège pour valider notre démarche déployer pour la QoS.

a. Envoi de Ping de l'agence critique vers le siège

En utilisant la commande:

Ping -n 100 -f -l 1450 172.16.1.4 nous avons eu comme statistique.

Sur **100** paquets envoyés, seuls **76** sont reçus, dont**24** perdus, ce qui donne 24% de perte, et cela sans tenir en compte l'autre service allant de l'agence vers le siège.

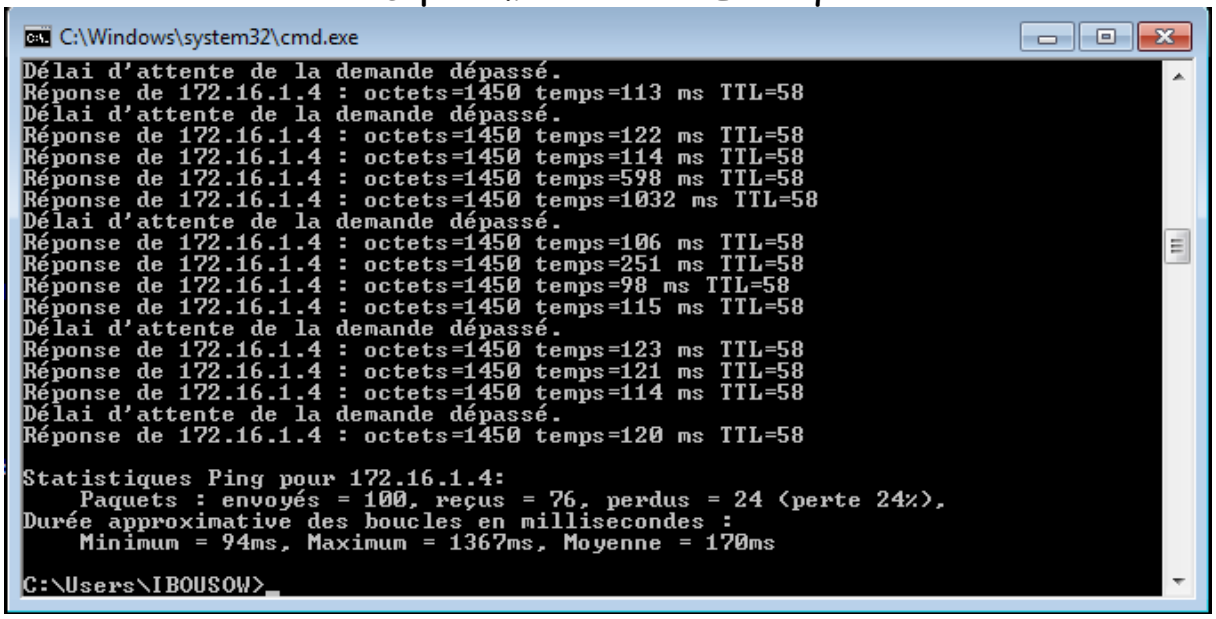


Figure 20: Ping Agence vers Siège.

Les paquets ICMP appartiennent à la class-default avec un precedence 0, donc on revient dans le mode Best effort pour l'ICMP représenté ci-dessous dans la capture avec Wireshark:

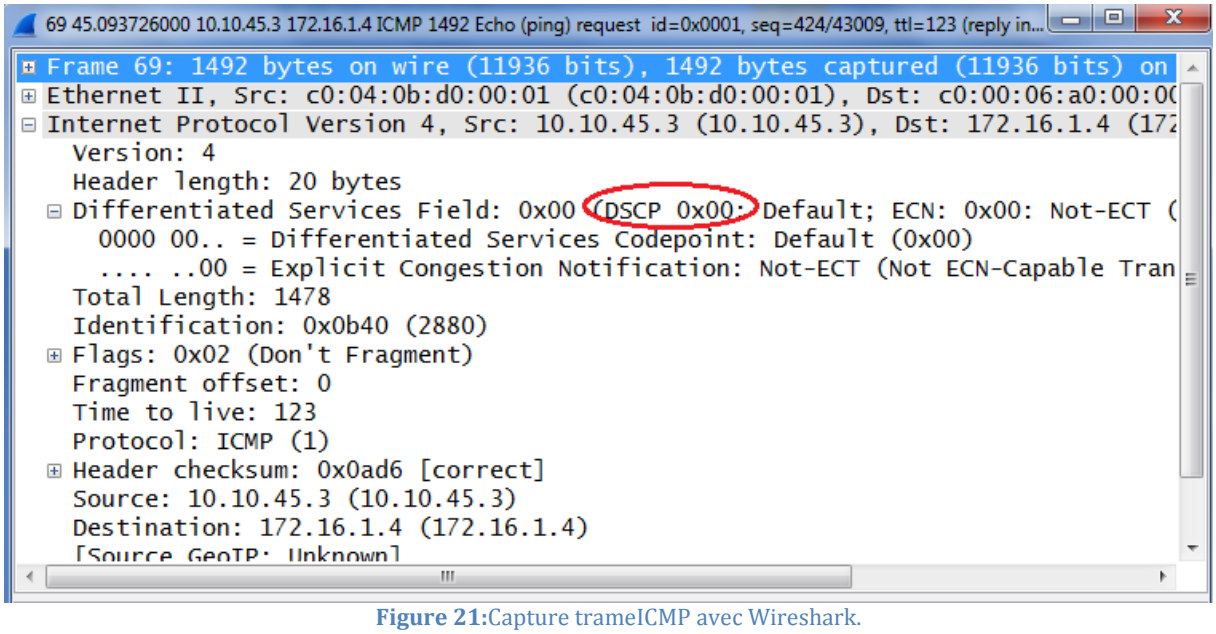


Figure 21: Capture tramelCMP avec Wireshark.

b. Après activation de tous les services

Nous allons maintenant activer tous les services allant de l'agence vers le siège qui sont :

- Signalisation de la Voix
- Flux Métiers : Messagerie & Courier
- Flux Financiers
- Visioconférence

Etapes de configuration du Jperf :

Mode Serveur :

- Configurer le premier serveur de sorte qu'un client (site administratif) peut se connecter au siège.
- Entrer le numéro du **port** attribué au protocole du trafic généré (exemple : Le http utilise le port 80).
- Assurez que Jperf ne soit pas déjà en exécution, en cliquant sur le bouton **Stop Iperf**. Choisissez l'option de serveur en mode Iperf zone et puis cliquez sur **Run Iperf**. Vous n'avez pas besoin de configurer quoi que ce soit d'autre pour le test.

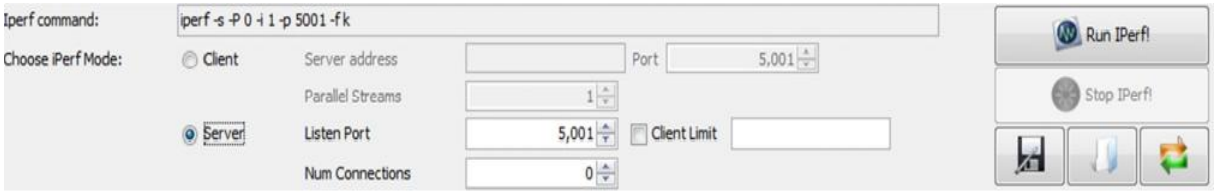


Figure 22: Configuration **Jperf** en mode serveur.

Mode client :

Nous avons configuré Jperf au premier PC au niveau du site administratif, qui est en mode client de sorte qu'il soit connecté au Jperf en mode Serveur au niveau du siège.

- Assurez Jperf n'est pas en cours d'exécution en cliquant sur le bouton **Stop Iperf.**
- Choisissez l'option de client dans la zone **Mode Iperf**. Tapez l'adresse IP du serveur dans l'adresse du serveur, le numéro de port du protocole, et puis cliquez sur **Run Iperf**.

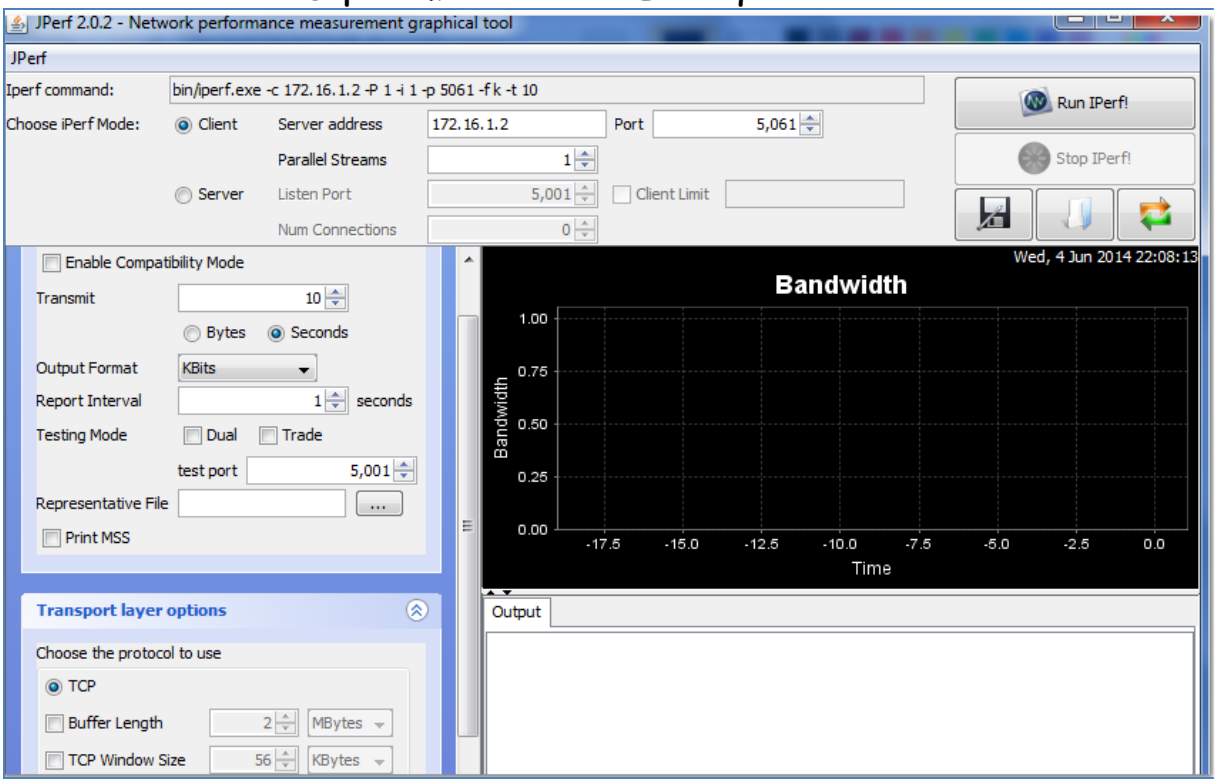


Figure 23: Configuration du **Jperf** en mode client.

En lançant la génération des flux du administratif (**Signalisation de la voix, Flux: Messagerie & Courier, Flux Financiers et la Visioconférence**) sur le PC-client, et on les écoute sur les ports (**5005, 80, 443,5061**) sur le PC en mode serveur.

Après avoir activé les flux allant de l'agence vers le siège, nous avons eu comme ci-dessous la capture sur l'outil Wireshark:

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 24: Capture pour tous type de trafic avec Wireshark.

En utilisant la même commande **Ping -n 100 -f -l 1450 172.16.1.4**

Sur **100 paquets** envoyés, seuls **59** sont reçus, dont **41 perdus** ce qui donne **41% de perte** on constate que le taux de perte de paquet vient de doubler cela en activant les services allant de l'agence vers le siège.

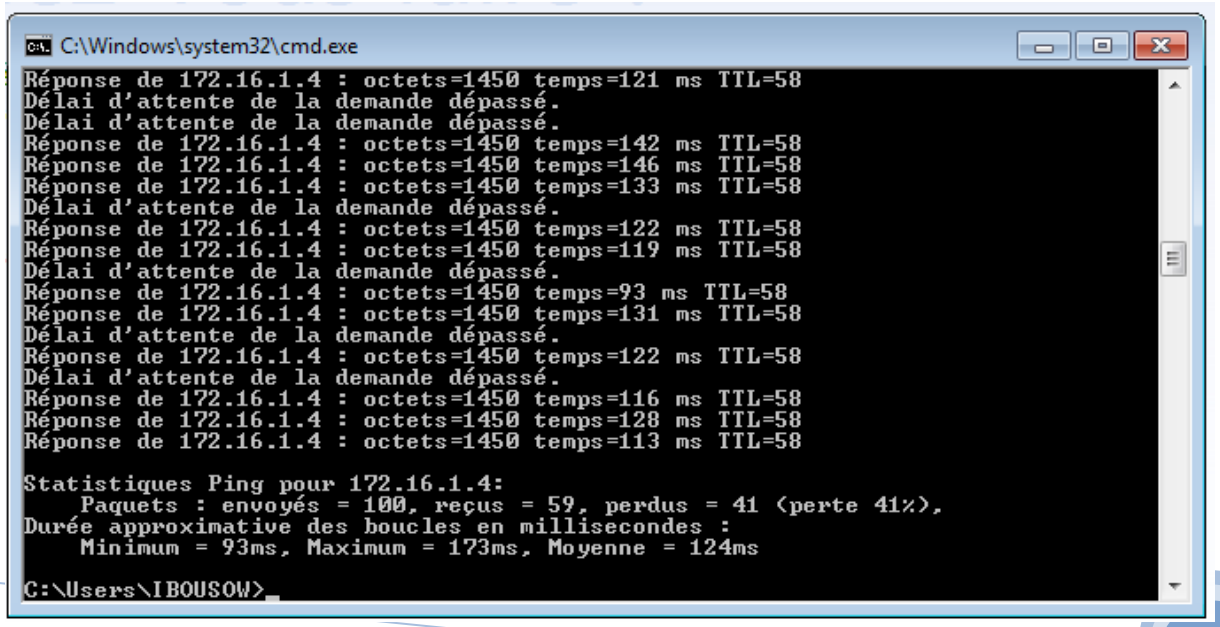


Figure 25: Ping après activation des Services.

- Détail du paquet du protocole SiP de la Visioconférence

Au niveau de la classification dans le chapitre précédent nous avons attribué la classe Premium à la visioconférence correspondant à la classe 4 au niveau de la configuration, donc nous voyons bien l'effet au niveau du champ DSCP du paquet.

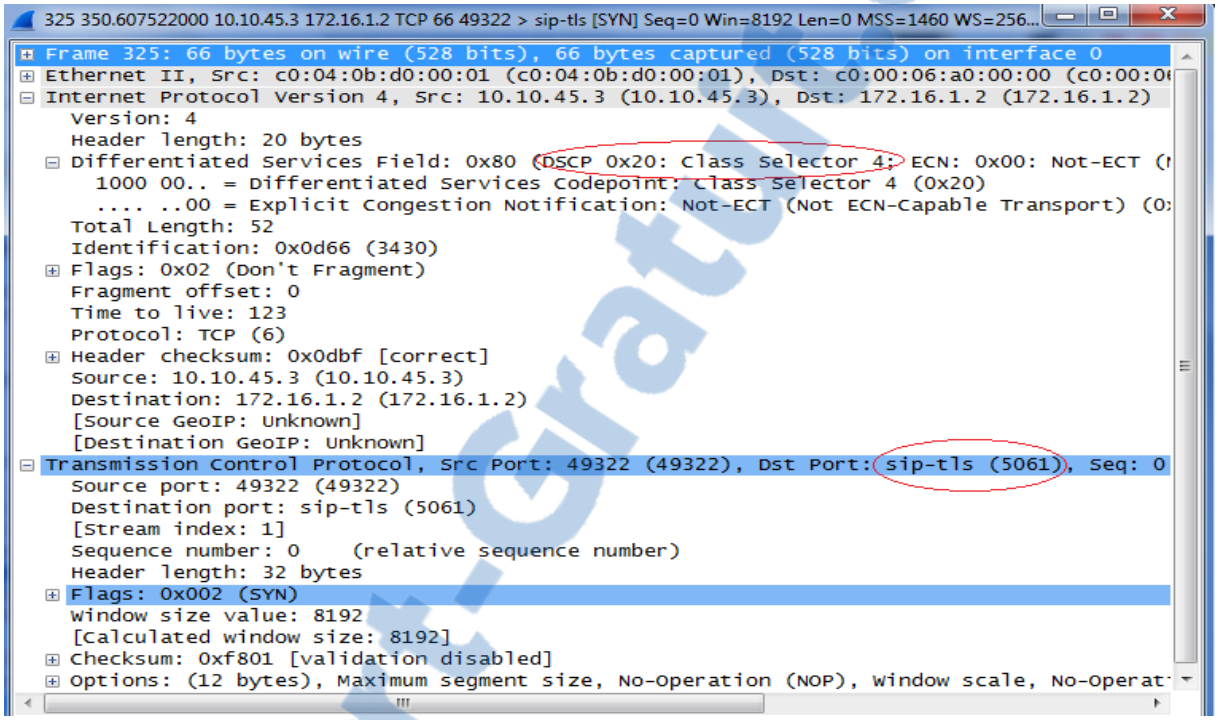


Figure 26: Capture trame SIP avec Wireshark.

Grâce à l'analyseur Wireshark, nous avons vérifié la qualité de service rendu pour la signalisation de la voix la visioconférence ainsi que pour l'utilisation de http (voir Annexe C).

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 application.Nous avons effectué des simulations sur le trafic avant et après activation de toutes les applications métiers du site administratif vers le siège.

Conclusion générale

Notre projet de fin d'études est un travail réalisé au sein de Poste Maroc 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 l'organisme d'accueil « Poste Maroc », ainsi que notre cahier des charges adopté pour ce projet.

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, dans cette partie, 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 des simulations de notre application.

Enfin, ce stage fut une expérience très enrichissante pour nous sur les deux plans personnels et professionnels. En effet, il a été l'occasionde 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.

Une extension de notre effort pourrait se baser sur cette application pour proposer une amélioration des fonctionnalités de la QoS dans les boitiers StreamCore au niveau du siège, ainsi de mettre en pratique notre application de la QoS dans les sites administratifs et critiques.

ANNEXE A

- Les critères de comparaison:

Critère	Commentaire
Ancienneté sur marché	L'Age de l'entreprise et ses expériences pendant des années
Documentation	La disponibilité de la documentation, sa qualité et sa simplicité
Popularité	Le niveau de popularité de l'entreprise et son équipement
durée de vie de l'équipement	Estimation de la durée de vie moyenne de l'outil
Prix	Le prix de l'équipement offert
Interface graphique	Est-elle automatique ou après ajout d'une application ?
homogénéité avec l'opérateur	homogénéité avec l'équipement utilisé par Maroc Telecom
CPU	La charge de la CPU performance
Formation des ingénieurs	Savoir si les ingénieurs ont besoin d'une formation pour l'outil, et sa durée ?
manipulation graphique	La simplicité de la manipulation de l'outil
manipulation des critères QOS	La simplicité de la configuration de la QOS
Sécurité de trafic	La sécurité de trafic garantit par l'outil
Mis à jour de la config	Possibilité de modifier la config à chaque instant
résultats après QOS	performances et résultats après implémentation de la QOS sur le réseau
Autres fonctions	Reporting, supervision …

Figure A.1 : Critère de Comparaison.

ANNEXE B

- **Configurations des routeurs:**

1. Routeur CE4:

```
service-policy output QOS_POLICY
!
interface FastEthernet0/1
ip address 10.10.45.1 255.255.255.0
ip flow ingress
ip flow egress
ip route-cache flow
```

```
 duplex auto
 speed auto
 !
 router eigrp 1
 network 4.4.4.4 0.0.0.0
 network 10.10.13.0 0.0.0.3
 network 10.10.45.0 0.0.0.255
 auto-summary
 !
 ip forward-protocol nd
 !
 ip flow-export source FastEthernet0/1
 ip flow-export version 5
 ip flow-export destination 10.10.45.2 9996
 !
 ip http server
 ip http authentication local
 ip http secure-server
 !
 ip access-list extended CRITIQUE
 permit tcp any host 172.16.1.4 eq www
 permit udp any host 172.16.1.2 eq 5005
 permit tcp any host 172.16.1.2 eq 443
 permit tcp any host 172.16.1.2 eq 5005
 ip access-list extended NORMAL
 permit tcp any host 172.16.1.5 eq www
 ip access-list extended PREMIUM
 permit tcp any host 172.16.1.2 eq 5061
 !
 snmp-server community public RO
 snmp-server trap-source FastEthernet0/1
 !
 control-plane
 !
 !
 !
 line con 0
 exec-timeout 0 0
 logging synchronous
 line aux 0
 line vty 0 4
 privilege level 15
 login local
 transport input ssh
 !
 !
 end
```

Figure B.1 : Configuration du routeur CE4 de l'agence critique.

2. Routeur Réel:

```
class-map match-all CRITIQUE_CLS
```

```
 match access-group name CRITIQUE
class-map match-all NORMAL_CLS
 match access-group name NORMAL
class-map match-all PREMIUM_CLS
 match access-group name PREMIUM
!
!
policy-map QOS_POLICY
 class PREMIUM_CLS
  set precedence 4
 class CRITIQUE_CLS
  set precedence 3
 class NORMAL_CLS
  set precedence 2
 class class-default
  set precedence 0
!
interface FastEthernet0/0
 bandwidth 8
 ip address 192.168.2.3 255.255.255.0
 rate-limit input 8000 1500 2000 conform-action transmit exceed-action drop
 rate-limit output 8000 1500 2000 conform-action transmit exceed-action drop
 duplex auto
 speed auto
 service-policy output QOS_POLICY
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
```

```
 speed auto
!
router eigrp 1
 network 172.16.1.0 0.0.0.255
 network 192.168.2.0
 auto-summary
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
ip access-list extended CRITIQUE
 permit tcp host 172.16.1.4 eq www 10.10.0.0 0.0.255.255
 permit tcp host 172.16.1.2 eq 443 10.10.0.0 0.0.255.255
 permit udp host 172.16.1.2 eq 5005 10.10.0.0 0.0.255.255
 permit tcp host 172.16.1.2 eq 5005 10.10.0.0 0.0.255.255
ip access-list extended NORMAL
 permit tcp host 172.16.1.5 eq www 10.10.0.0 0.0.255.255
ip access-list extended PREMIUM
 permit tcp host 172.16.1.2 eq 5061 10.10.0.0 0.0.255.255
 permit udp host 172.16.1.2 eq 5061 10.10.0.0 0.0.255.255
```

Figure B.2 : Configuration du routeur réel.

3 .Configuration du routeur PE2 de l'opérateur MPLS :

```
hostname PE2
!
boot-start-marker
boot-end-marker
```

```
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
ip vrf PM
 description Poste Maroc
rd 10:10
 route-target export 10:10
 route-target import 10:10
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
mpls label protocol ldp
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 bandwidth 20000
 ip vrf forwarding PM
 ip address 10.10.11.1 255.255.255.252
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.252
 duplex auto
 speed auto
mpls ip
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 1
 no auto-summary
 !
 address-family ipv4 vrf PM
  redistribute bgp 10 metric 20000 10 255 255 3
  network 10.10.11.0 0.0.0.3
  no auto-summary
  autonomous-system 1
 exit-address-family
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.3 area 0
```

```
!
router bgp 10
 no synchronization
bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 10
 neighbor 1.1.1.1 next-hop-self
 neighbor 3.3.3.3 remote-as 10
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 3.3.3.3 next-hop-self
 no auto-summary
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf PM
  redistribute eigrp 1 metric 3
  no synchronization
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
```

```
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Figure B.3 : Configuration du routeur PE2 de l'opérateur.

ANNEXE C

1. Détail du paquet TCP du protocole http(port 80):

Classe critique avec CS =3

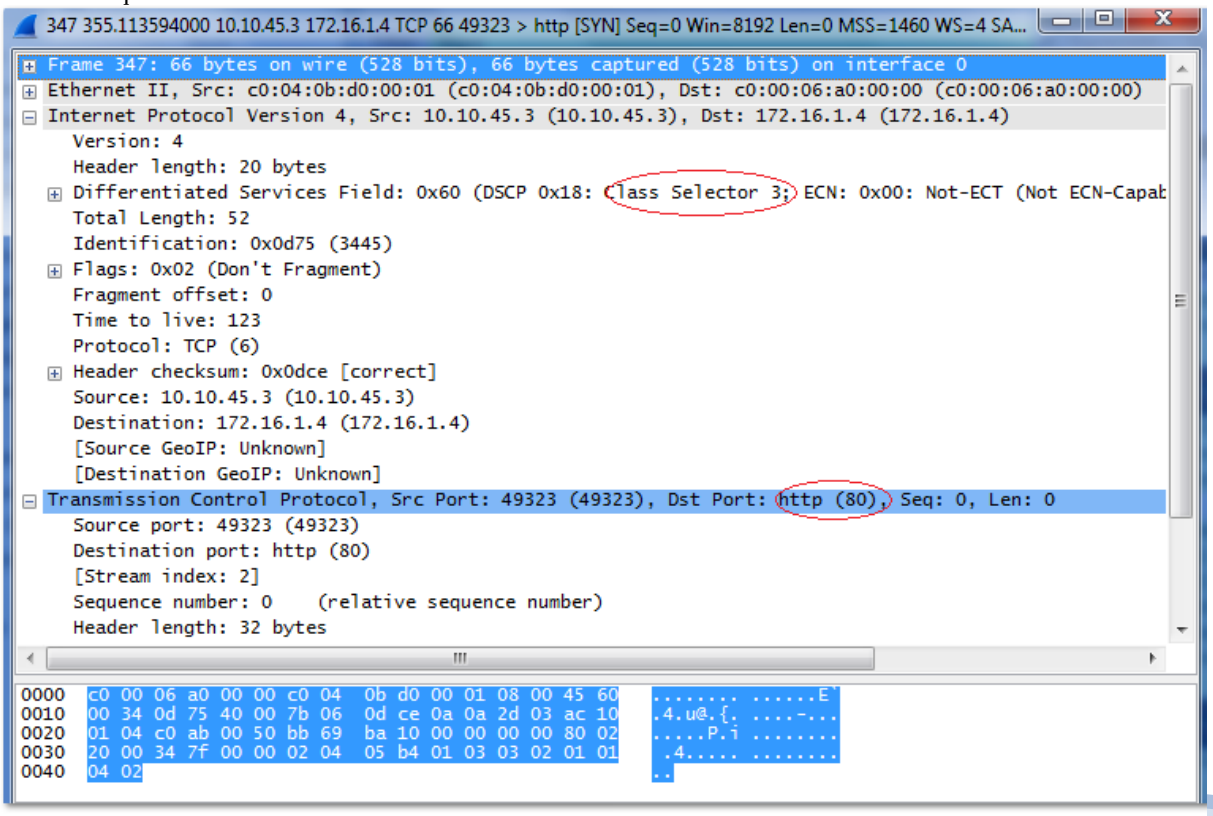


Figure C.1 : Capture trame http avec Wireshark.

2. Détaildu paquet TCP du protocole RTCP (voix, port 5005)

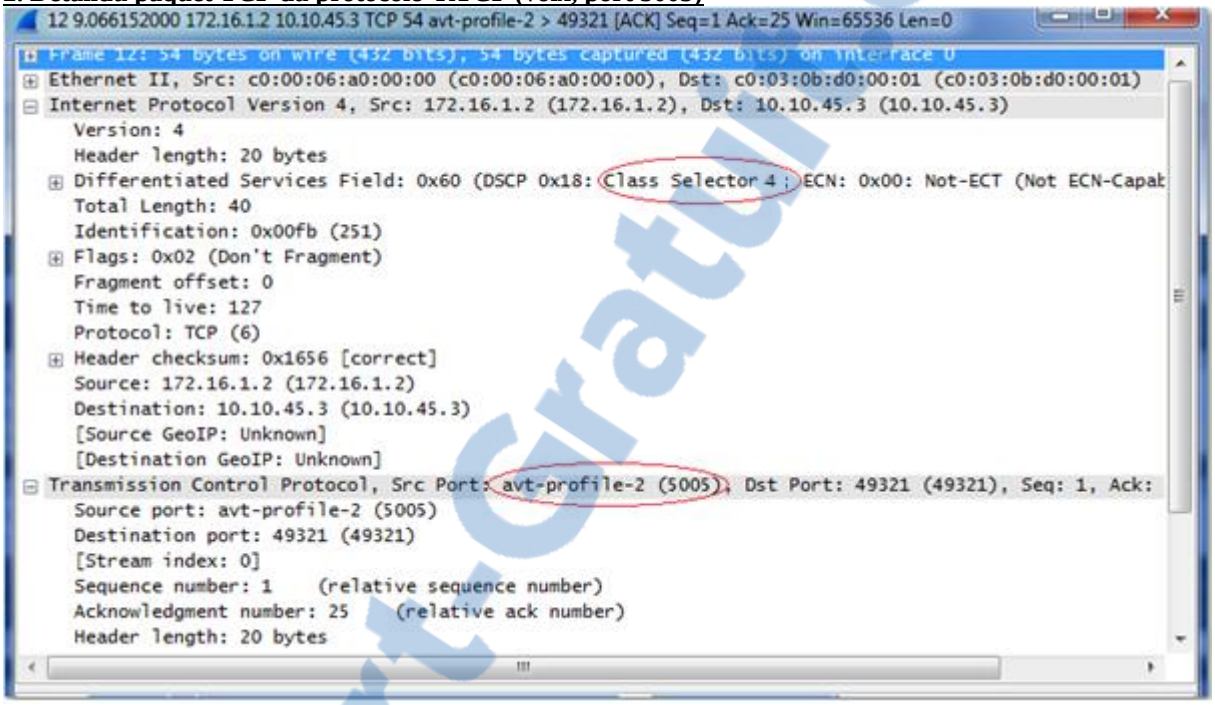


Figure C.2 : Capture trame RTCP avec Wireshark.

BIBLIOGRAPHIE ET WEBOGRAPHIE

[1]www.postemaroc.post (Date de consultation : 13/03/2014)

[2] http://iperf.fr/ (Date de consultation : 15/04/2014)

[3] Wikipedia.org (Date de consultation : 15/03/2014)

[4] www.vmware.com/ (Date de consultation : 14/04/2014)

[5] www.wireshark.org (Date de consultation : 17/04/2014)

[6] www.gns.net (Date de consultation : 14/04/2014)

[7] www.streamcore.com (Date de consultation : 22/03/2014)

[8] www.cisco.com (Date de consultation : 18/03/2014)

[9] Wendell Odom,CCIE N° 1624 ,Michael J.Cavanaugh,CCIE N° 4516 ,IP Telephony Self-Study Cisco QOS Exam Certification Guide;2005.

[10] NizarSaâda,Etude et Optimisation d'unbackbone IP/MPLS ; 2014

[11]Isabelle Guérin Lassous,Les principes fondamentaux de la qualité de service ; 2007

[12]Marie PNET, Mohammed EL MALKI, M. HAYEL ,Abdessamad TANNICHA, Mahmoud KOURDACHE, Simulateur de QoS ;2011