Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Mémoire de Projet de fin d'étude

Préparé par

Ahlam ELBIYAALI

Pour l'obtention du diplôme

Ingénieur d'Etat en

SYSTEMES ELECTRONIQUES & TELECOMMUNICATIONS

Intitulé

Optimisation de la bande passante internet mobile 3G

Encadré par :

Pr : F. MRABTI

Pr : M.LAHBABI

Mr: Y. RATBI (MAROC TELECOM-RABAT)

Soutenu le Mercredi 27 Juin 2012, devant le jury composé de :

Pr: F. MRABTI……: Encadrant

Pr: M. LAHBABI……: Encadrant

Mr: Y. RATBI……..: Encadrant

Pr: F. ABDI…….. : Examinateur

Pr: N. ES-SBAI…….: Examinateur

ANNEE UNIVERSITAIRE 2011- 2012

Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Dédicace:

A mon cher père et ma chère mère

Aucun hommage ne pourrait être à la hauteur de l'amour et de l'affection dont vous ne cessez de me combler.que vous trouvez dans ce travail un témoignage de mon profond amour et éternelle reconnaissance Que Dieu vous procure bonne santé et longue vie

A mes deux oncles Mohamed et Amine

Nul mot ne pourra exprimer ma gratitude envers vous, je l'ai dit une fois dans le temps, je le redis toujours avec la même conviction.

A mon frère Mounim et ma sœur Nouhaila

Leurs énormes supports, soutiens et encouragements ont fait d'eux les plus dévoués des personnes qu'on puisse avoir.

A ma très chère tante Meryam et oncle Mohamed

Leurs efforts, accueils et bons conseils ont été un grand secours lors de mon séjour à Rabat.

A ma prestigieuse faculté

La faculté des sciences et techniques Nous espérons que cet humble travail soit à la hauteur de vos attentes.

A toute ma famille, à mes amis et à tous ceux que j'aime et qui m'ont soutenu durant mon cursus

Je dédie ce modeste travail

Ahlam

Remerciements

Je tiens à remercier vivement les aimables personnes, qui m'ont aidé de près ou de loin à la réalisation de ce travail au sein de MAROC TELECOM.

J'adresse mes sentiments de reconnaissance et de respect à Monsieur Yassine RATBI et Madame Dounia OUARDIRHI, responsables du service « Data Mobile », pour avoir accepté de parrainer ce projet et surtout pour leurs qualités humaines et scientifiques toujours en toute modestie, leur passion du métier qu'ils savent rendre contagieuse et la confiance qu'ils ont bien voulu m'accorder tout au long de ce travail.

Je tiens à remercier vivement Mlle Fatiha MRABTI et Monsieur Mohamed LAHBABI, Professeurs à la Faculté des Sciences et Techniques de Fès, pour avoir accepté d'encadrer ce travail, pour leur enthousiasme permanent et leurs implications tant humaines que scientifiques.

Je tiens aussi à exprimer ma profonde gratitude à Jawad BOULATYAB, ainsi que l'ensemble du personnel de l'Equipe de déploiement pour leurs renseignements et orientations.

Pour conclure je remercie également les membres de jury d'avoir accepté d'évaluer ce travail, ainsi que tous les enseignants de la Faculté des Sciences et Techniques de m'avoir apporté leur savoir faire, leur expérience et leur disponibilité tout au long de ces trois ans de formation.

Liste des Acronymes

APN: Access Point Name

DB : Data Base

CPU: Central Processing Unit

CS : Circuit Switched

CSS: Caching Subsystem

DPI: Deep Packet Inspection

DSS: Dispatching Subsystem

GGSN: Gateway GPRS Support Node

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

GUI: Graphical User Interface

GZIP: GNU Zip

HTTP: Hyper Text Transfer Protocol

IMS: IP Multimedia Subsystem

IP Internet Protocol

QOS: *Quality of service*

LBS: Load Balancing System

MSISDN Mobile Station ISDN Number

MSS: Management Subsystem

P2P: Peer to Peer

PBR: Policy Based Routing

PDN: Packet Data. Network

PDP Packet Data Protocol

PLMN: Public Land Mobile Network

PS: Packet switched

RSS: Redirection Subsystem

SAS: Serial Attached SCSI

SGSN :*Serving GPRS Support Node*

SIM: Subscriber Identity Module

UMTS: *Universal Mobile Telecommunications System*

URL: Uniform Resource Locator

VOIP: Voix Sur IP

VPN: Virtual Private Network

VRRP: Virtual Router Redundancy Protocol

Liste des figures:

Liste des tableaux:

Introduction générale:

L'utilisateur du mobile porte un grand intérêt aux nouvelles technologies, et aux services qu'elles offrent. Cette demande, qui s'élargie de jour en jour, incite les operateurs télécoms à implémenter de nouvelles architectures, infrastructures et méthodologies dans leurs réseaux pour satisfaire leurs clients.
Dans ce sens, l'industrie de la communication mobile connait un essor prodigieux au delà de toutes les attentes, plus d'un milliard d'abonnés profitent des services offerts par les réseaux cellulaires. La plupart des abonnés utilisent les réseaux GSM et bénéficie du service de la parole. Le succès du GSM est alors bien établit.

Toutefois, l'évolution profonde de l'internet et la demande croissante aux services mobiles semblent être des facteurs favorables à la migration progressive du monde des télécommunications vers d'autres nouveaux réseaux se basant sur la commutation de paquets. On cite, dans cette perspective, la technologie GPRS (2.5G) destinée à la transmission des données (data) avec des débits élevés et le standard UMTS (3G) ou réseau tout IP adapté à la transmission de services multimédias et autorisant un accroissement assez important des débits.
Cependant, La demande incroyable des clients aux services 3G, le déferlement des usages internet réellement haut débit tel que le streaming, téléphonie Internet (VoIP), partage des fichiers peer-to-peer (P2P) et visioconférence exigent évidemment des garanties en termes de bande passante.
Pour éviter une congestion des réseaux et une pénurie de la bande passante, MAROC TELECOM, l'operateur historique leader au Maroc, cherche en premier lieu à optimiser le trafic sur son réseau de façon à ce que la bande passante réellement consommée ne l'oblige pas à de nouveaux investissements en termes d'augmentation de capacités de son réseau, ni à une réduction intense de l'expérience utilisateur.
Les pilotes SIG et ICACHE produits de HUAWEI Technologies déployées localement au niveau de MAROC TELECOM et bénéficiant des fonctionnalités d'inspection de paquets au niveau applicatif (DPI), présentent des solutions idéales permettant une optimisation intelligente des ressources actuelles.
En effet, le pilote ICache assure un stockage et une délivrance directe des ressources internet demandées par l'utilisateur final, il permet ainsi de réduire les coûts de la bande passante en garantissant une amélioration de la qualité du service. Alors que le pilote SIG, assure un contrôle, une gestion et un blocage dans du trafic au niveau du GGSN du réseau mobile, il permet alors une consommation de la bande passante utilisée.
Avant d'implémenter les deux solutions au niveau du réseau mobile global, une étude de leurs faisabilités en termes de leurs réponses aux exigences élaborées est indispensable. Pour ce faire, je procéderai dans un premier temps par décrire et établir les exigences qui devront être offertes par les deux solutions, dans un second temps je présenterai la stratégie à suivre pour étudier leurs faisabilités au niveau technique, logique et fonctionnel pour finir après par une phase de déploiement et un ensemble de test de fonctionnalités. Ce présent rapport, s'étalera donc sur quatre chapitres:
Le 1èr chapitre, englobera une présentation générale de l'organisme d'accueil, et explicitera ensuite le contexte du projet.
Le 2ème chapitre, donnera une vue panoramique qui trace l'évolution des réseaux UMTS.

Le 3ème chapitre, présentera la démarche suivis pour étudier la faisabilité des solutions SIG et ICACHE au niveau physique, logique et fonctionnel.
Le 4ème chapitre, abordera la phase de déploiement, il explicitera donc les tests de fonctionnalités préparés et exigés ensuite au groupe Huawei, les étapes poursuivies pour mener à bien l'installation des équipements, et leur mise en service. Et décrira enfin l'ensemble de test de fonctionnalités effectuées et leurs résultats.

Table des matières :

Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Chapitre 1: Contexte Général du Projet

ANNEE UNIVERSITAIRE 2011- 2012

Introduction:

Ce chapitre, sera consacré à la présentation du contexte général du projet dans lequel cette mémoire de fin d'étude a été réalisée mais avant d'y mettre l'accent une présentation succincte de la société MAROC TELECOM s'avère indispensable.

1. La présentation de MAROC TELECOM:

1.1 L'Identification:

Itissalat Al-Maghreb (IAM) ou également Maroc Telecom est une entreprise de proximité, par tradition, issue de la lignée d'opérateurs télécoms ayant profondément façonnés le paysage des télécommunications marocaines, c'est le premier operateur au MAROC et le deuxième en Afrique.

1.2 La fiche signalétique:

Raison sociale	Itissalat Al-Maghreb
Forme juridique	S.A. à Directoire et à Conseil de Surveillance
Siège social	Avenue. Annakhil, Hay Riad – RABAT
Président du Directoire	M. Abdeslam AHIZOUNE
Date de création	25/02/1998
Objet	Télécommunications
Registre de commerce	48 947 Rabat
Identification fiscale	333 2162
Patente	27603573
Nombre de directions régionales	17307131
Effectif total	13 414 (dont 2884 cadres et 7818 maîtrises)

Téléphone	(212) 37.71.21.21
Télécopie	(212) 37.71.48.60
Site web	www.iam.ma

Tableau 1: Fiche signalétique du groupe Maroc Telecom

1.3 Les activités:

Maroc Telecom, le pionnier des services de hautes technologies, offre une large gamme de produits et de services afin de satisfaire ses clients, il est organisé ainsi autour de trois activités principales: Mobile, Fixe et Internet où il a démontré une présence incontestable comme le prouvent les chiffres suivants:
Dans le contexte d'un marché de télécommunications bénéficiant des conditions économiques et démographiques favorables à la poursuite de sa croissance, Maroc Telecom a pour objectifs de rester leader sur chaque segment de son marché (mobile, fixe et Internet) et de maintenir sa rentabilité, en stimulant la croissance du marché Mobile, en renforçant la compétitivité et l'offre du Fixe pour faire face à la concurrence et en restant le principal moteur du développement de l'Internet au Maroc.

1.4 L'organisation:

L'organisation de l'operateur Maroc Telecom s'articule autour de quatre pôles (Pôle services Pôle réseaux, Pôle Administratif & Financier, Pôle Règlementation Communication et Développement à l'International et 8 Directions Régionales (figure 1).

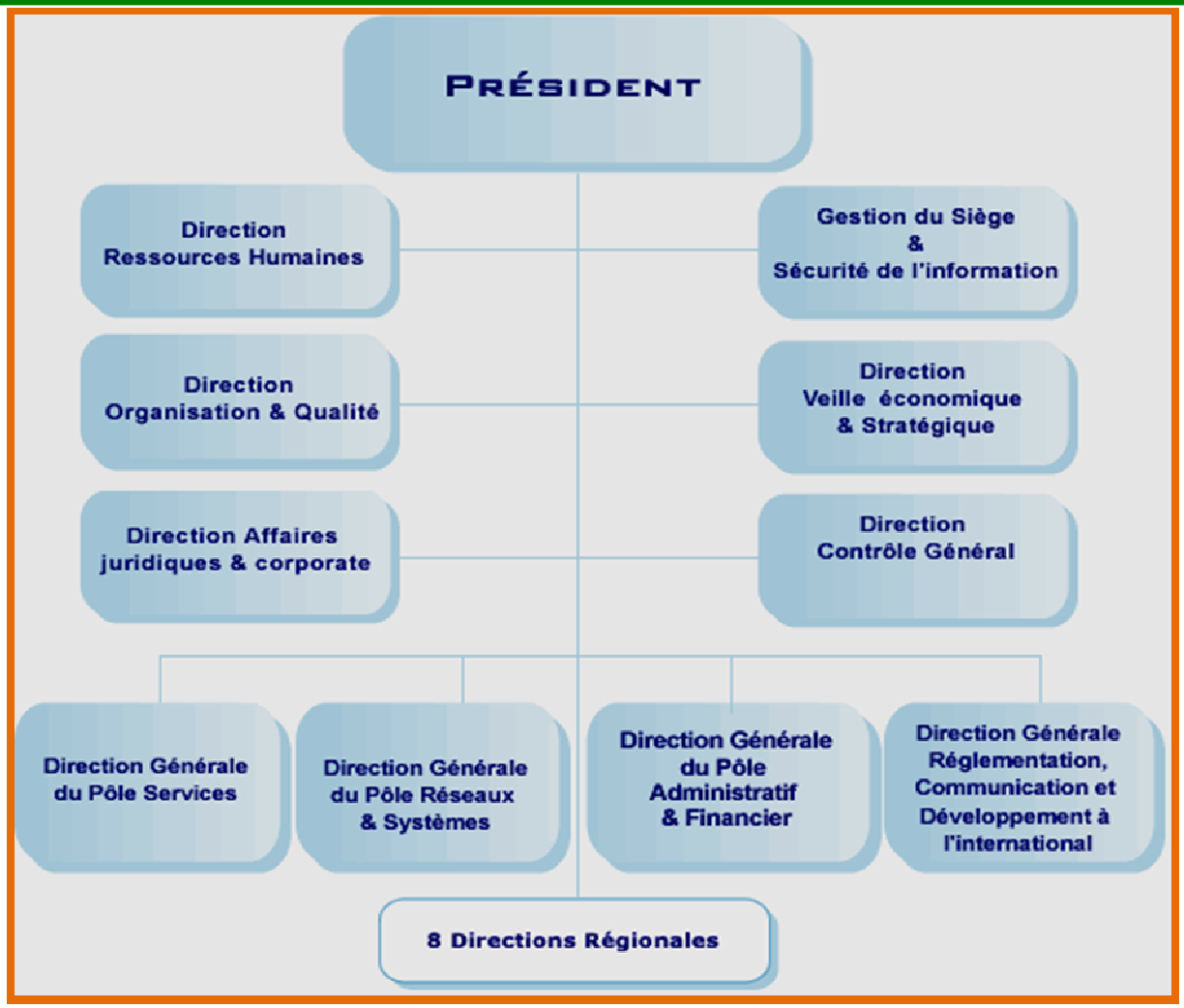


Figure 1. Organigramme général du groupe MAROC TELECOM

2. La présentation du contexte du projet:

Les technologies mobiles de troisième génération (3G) mises en place par l'opérateur MAROC TELECOM ouvrent de nouveaux horizons aux usagers en termes d'applications internet innovantes et débit de plus en plus élevé.

Cependant, les statistiques actuelles, se basant sur les tendances du trafic internet, montrent que le nombre des abonnés augmente et que plus de 80% de leur trafic s'est orienté vers les applications internet VOIP, Vidéo en Ligne, P2P et HTTP.

Ces applications internet sont utiles, apportent de nouvelles opportunités commerciales, enrichissent les cultures des utilisateurs, certaines sont en temps réel ou représentent un mode de téléphonie sur IP de haute qualité et de haut débit. Mais, elles apportent leurs lots de pression sur la bande passante internet. Pour résoudre ce problème qui exige de nouvelles ressources en termes de bandes passantes les solutions suivantes s'avèrent adéquates.

- L'élargissement de la bande passante: La solution de l'expansion de la bande passante est simple à mettre en œuvre, Pourtant, elle est coûteuse, peu rentable et n'est pas une solution à long terme. Ainsi l'expansion de la bande passante apporte peu de bénéfices et ne peut jamais avoir de fin.

- La facturation des services internet: cette solution permet de réduire la pression sur la bande passante de l'opérateur MAROC TELECOM, Cependant elle dégrade intensivement l'expérience de l'utilisateur, cela conduira ensuite à une perte de clientèles dans un marché mature et concurrentiel.

Dans ce sens, l'élargissement de la bande passante et la facturation supplémentaire ne présentent pas des solutions flexibles et capables d'améliorer à la fois l'expérience utilisateur et les revenus des investissements. Par comparaison les solutions SIG et ICache bénéficiant de nouvelles fonctionnalités d'inspection du trafic au niveau applicatif (DPI) apparaissent un choix optimum et idéale pour l'opérateur MAROC TELECOM et l'expérience utilisateur.

2.1 La présentation de la solution SIG:

La solution SIG est un pilote gratuit proposé et implémenté localement par le fournisseur HUAWEI TECHNOLOGIES au niveau du réseau mobile d'IAM. Il a pour objectif l'analyse, le contrôle, la gestion du trafic internet 3G au niveau du GGSN IP pool du réseau télécom. Il permet une gestion intelligente des **ressources actuelles** en termes de bandes passantes.

Le système SIG est constitué des éléments suivants (figure 2):

- La SIG FE (Front-end),
- La SIG BE (Back-end).

A coté de ces deux éléments de la SIG, il y a le STORAGE DEVICE, BYPASS DEVICE et SWITCH qui assurent les exigences de fiabilité.

Parmi les fonctionnalités dédiées par cette solution et qui assurent son rôle il ya:

- La gestion du trafic VOIP.
- Le contrôle parental.
- Le filtrage des URLs.
- La fonction FUP (Fair Usage Policy).
- La fonction Taxation/Charging.
- La fonction rapports et statistiques.
- La fonction IPush (Information pushing service).

Le fonctionnement des équipements et les fonctionnalités présentés ci-dessus seront détaillés par la suite **(dans le chapitre étude de faisabilité des solutions SIG et ICache**).

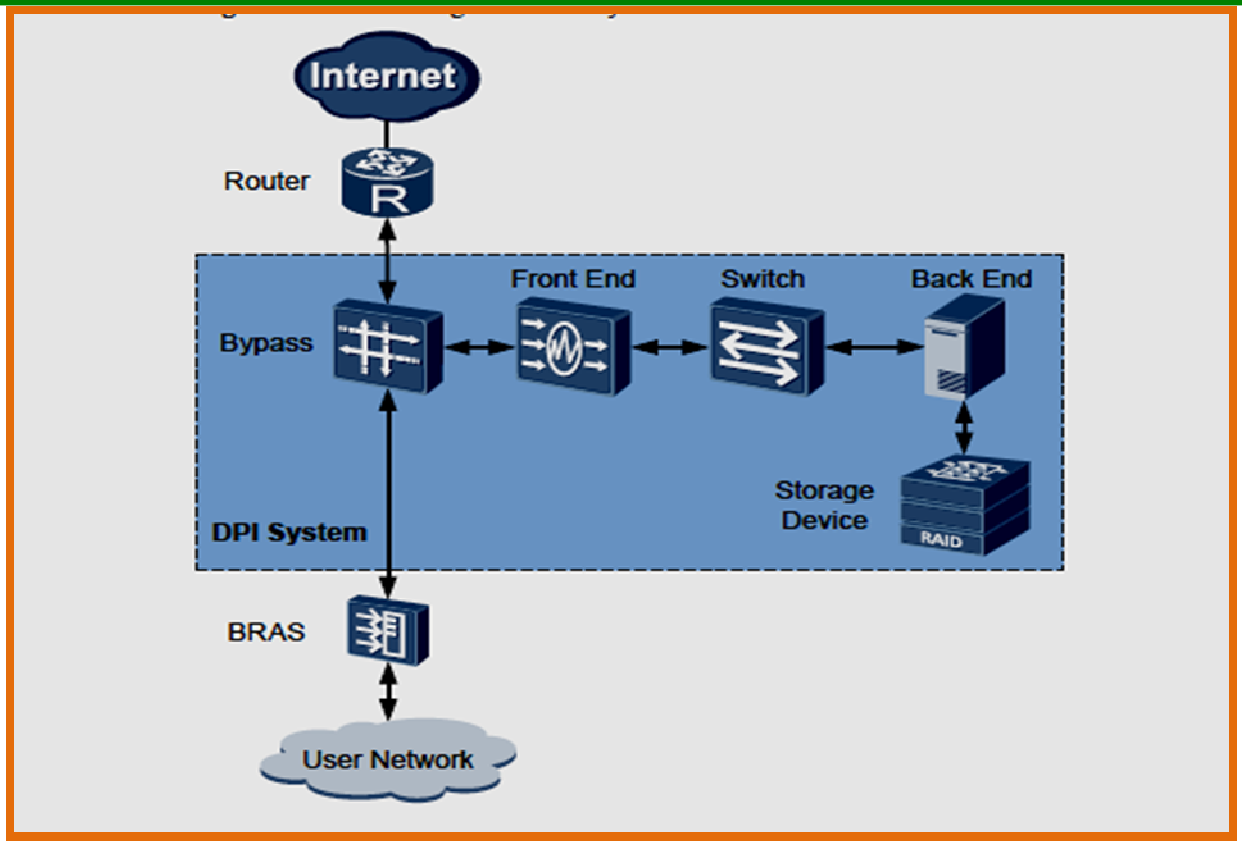


Figure 2: Equipements constituants le système DPI SIG

2.2 La présentation de la solution ICache:

La solution ICache est aussi un pilote gratuit proposé et implémenté dans le réseau mobile d'IAM. Il a pour objectif le cache du trafic HTTP et vidéos en ligne pour le délivrer directement aux utilisateurs finaux sans passer par le backbone internet. Il permet ainsi de **réduire les couts de la bande passante et d'améliorer la qualité des services**.

La solution ICache contient les éléments suivants (figure 3)**:**

- Le sous système de cache CSS (Cache Subsystem).
- Le sous système de gestion (Management Subsystem).
- Le Switch.
- Le système d'équilibrage de charge LBS (Load Balancing System).

Les différentes fonctions dédiées et assurant la réduction des couts de la bande passante internet utilisées sont:

- La fonction cache HTTP et vidéo en ligne.
- La fonction compression GZIP.
- La fonction gestion intelligente de l'espace disque.

Le fonctionnement et les fonctions ci-dessus seront aussi détaillées par la suite **(dans le chapitre étude de faisabilité des solutions SIG et ICache).**

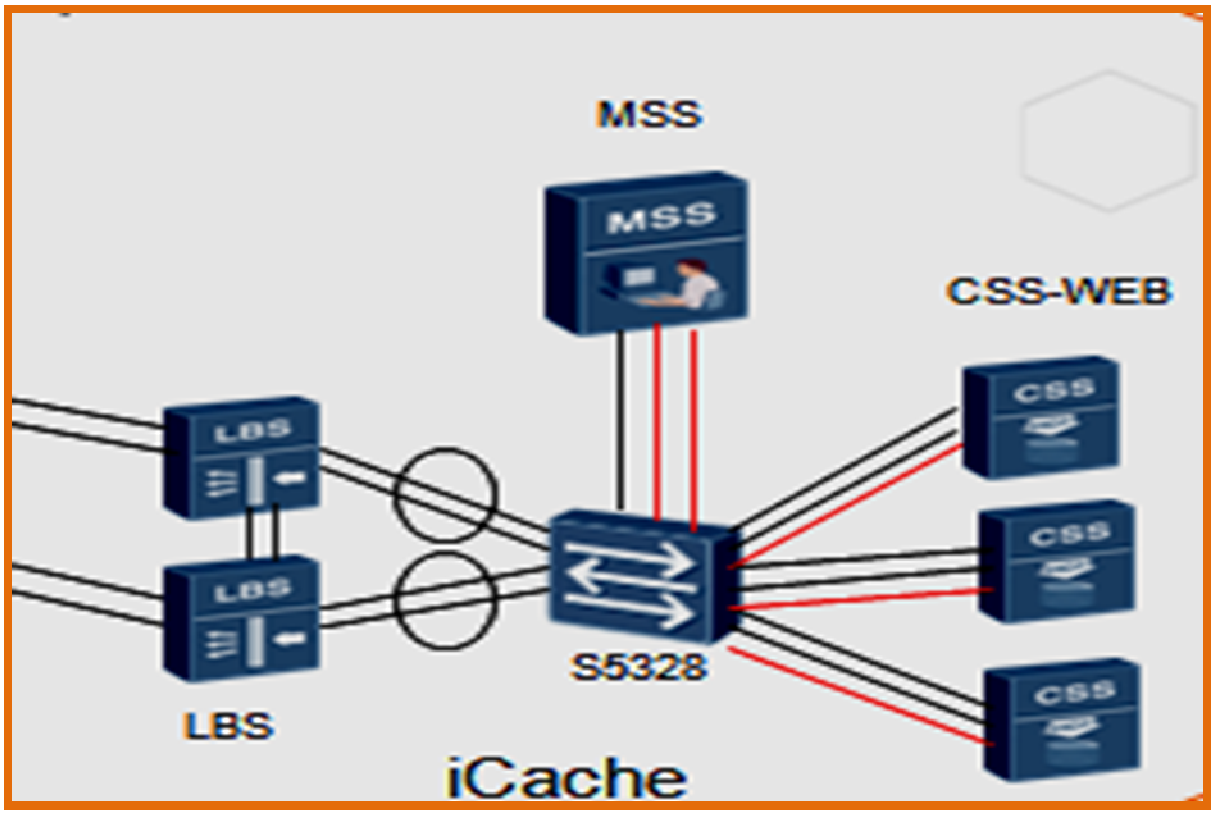


Figure 3: Equipements physiques de la plate forme ICache

3.1 La planification du projet:

Pour mener à bien ce projet, une planification dans l'ordre chronologique des différentes tâches à réaliser a été précisée. (Figure 4 et tableau 2).

Phases	Taches à réaliser
Etude préalable	➢ Documentations sur les évolutions des réseaux télécoms mobiles GSM GPRS UMTS

Cahier de charge Spécifique aux solutions SIG et ICache	➢ Etude de l'architecture du réseau Maroc Telecom. ➢ Analyse des exigences du service Technique de l'opérateur Maroc Telecom. ➢ Analyse des exigences du service Marketing. ➢ Elaboration des exigences qui devront offertes par les solutions SIG et ICache.
Etude de faisabilité des solutions	➢ Etude de faisabilité physique logique et fonctionnelle de la solution SIG ➢ Etude de faisabilité physique logique et fonctionnelle de la solution ICache
- Déploiement et tests de fonctionnalités	➢ Préparation des tests de fonctionnalités pour les deux solutions ➢ Déploiement des solutions. ➢ Tests de fonctionnalités. ➢ Evaluation des différents tests établis.
Clôture	➢ Phase de synthèse

Tableau 2: Taches à réaliser

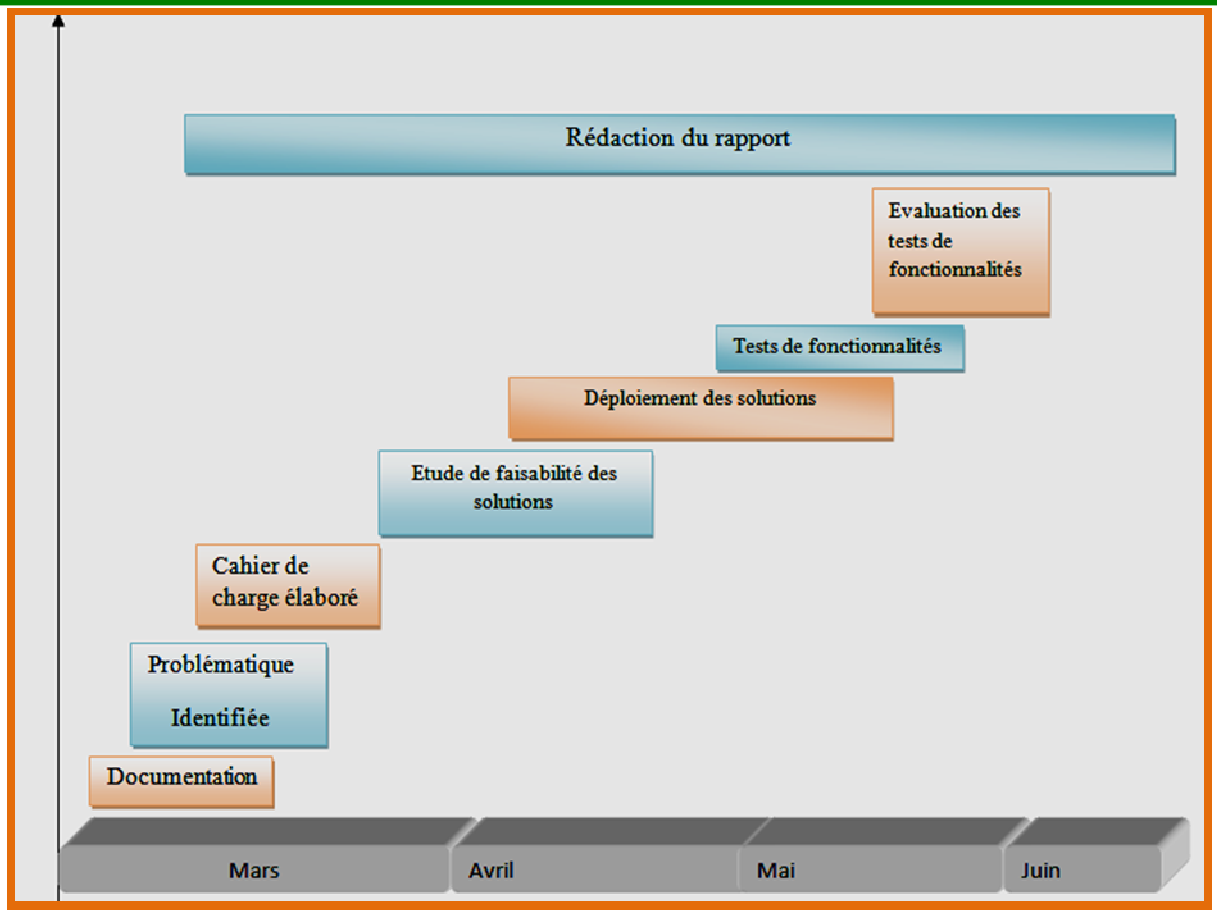


Figure 4: Phase de réalisation du PFE

Conclusion:

Une fois présenté l'organisme d''accueil et compris le contexte du projet, je tenterai d'établir dans le deuxième chapitre une synthèse de recherches théoriques liées aux réseaux de la troisièmes génération (UMTS) au niveau desquels le problème s'est posé.

Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Chapitre 2: Réseaux de troisième génération (UMTS)

ANNEE UNIVERSITAIRE 2011- 2012

Introduction:

Le réseau UMTS (Universal Mobile Telecommunications System) ou système de télécommunication mobile de troisième génération vient compléter les deux réseaux existants, il a combiné ainsi des services de type Voix en mode circuit du réseau GSM et des services de type Data en mode paquets du réseau GPRS.

Avec la standardisation de l'UMTS par le groupe de normalisation 3GPP, une remarquable tendance a émergé, influant fortement les réseaux UMTS. Il s'agit d'une évolution vers une architecture UMTS tout IP basée sur la spécification Release 5 qui a remplacé les technologies en mode circuit par une commutation en mode paquet. Cette spécification représente ainsi le support des applications multimédias novatrices avec un débit élevé de 2 Mbps, une qualité et une couverture meilleure.

Ce chapitre traite donc l'evolution des réseaux de télécommunications mobiles UMTS. Pour ce faire je présenterai dans un premier temps les différentes technologies utilisées au niveau cœurs, les differents services fournis, les architectures, les entités fonctionnelles et les différentes interfaces réseaux mises en jeu.

1 L'architecture du réseau télécom mobile UMTS:

Le réseau UMTS se divise en deux domaines: le domaine équipement utilisateur UE (User Equipment) et le domaine infrastructure. Le domaine infrastructure comporte aussi deux parties: le réseau d'accès radio RAN (Radio Access Network) et le réseau cœur CN (Core Network) (figure 5).

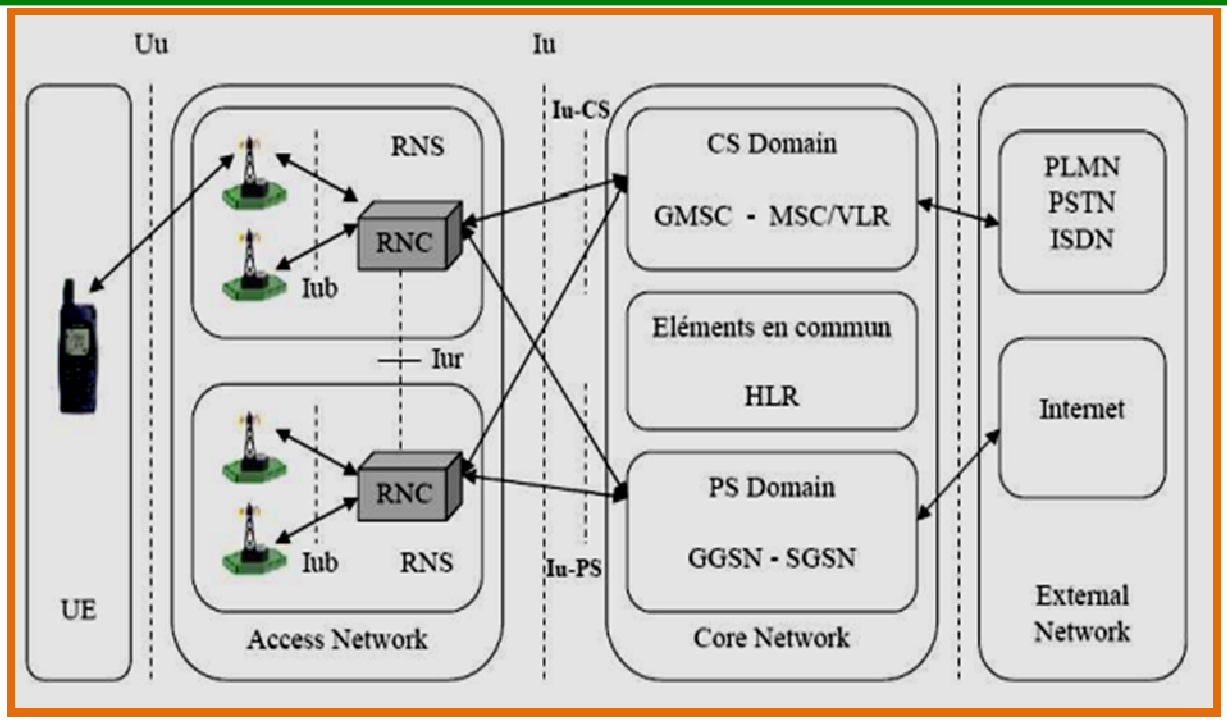


Figure 5: Architecture du réseau UMTS

1.1 L'équipement utilisateur:

Un équipement mobile est composé des deux éléments suivants:

✓ terminal mobile (ME):

C'est un terminal radio utilisé pour les communications à travers l'interface Um.

✓ la carte USIM:

C'est une carte à puce aux fonctionnalités très voisines de celles de la carte SIM du réseau GSM, elle contient l'identité de l'abonné et certaines informations relatives à cet abonnement comme les algorithmes d'abonnements, authentifications et cryptage.

1.2 Le réseau d'accès:

Le réseau d'accès radio de l'UMTS UTRAN (UMTS Terrestrial Radio Access Network) est constitué d'un ou de plusieurs sous système radio RNS (radio Networks sub-system) qui comprennent chacun un contrôleur de réseau radio RNC (radio networks Controller) et des stations de bases qu'on appelle nodes B.

✓ le node B:

C'est un nœud logique qui gère la couche physique de l'interface radio. Il assure principalement le codage du canal.

✓ le RNC:

il gère:

- Le contrôle de la charge des différents Nœuds B.
- Le contrôle d'admission et d'allocation des codes pour les nouveaux liens radio qui s'établissent dans les cellules gérées.

Le RNC est en liaison avec le réseau cœur pour les transmissions en mode paquet à travers l'interface Iu – PS et en mode circuit à travers l'interface Iu – CS (figure 6).

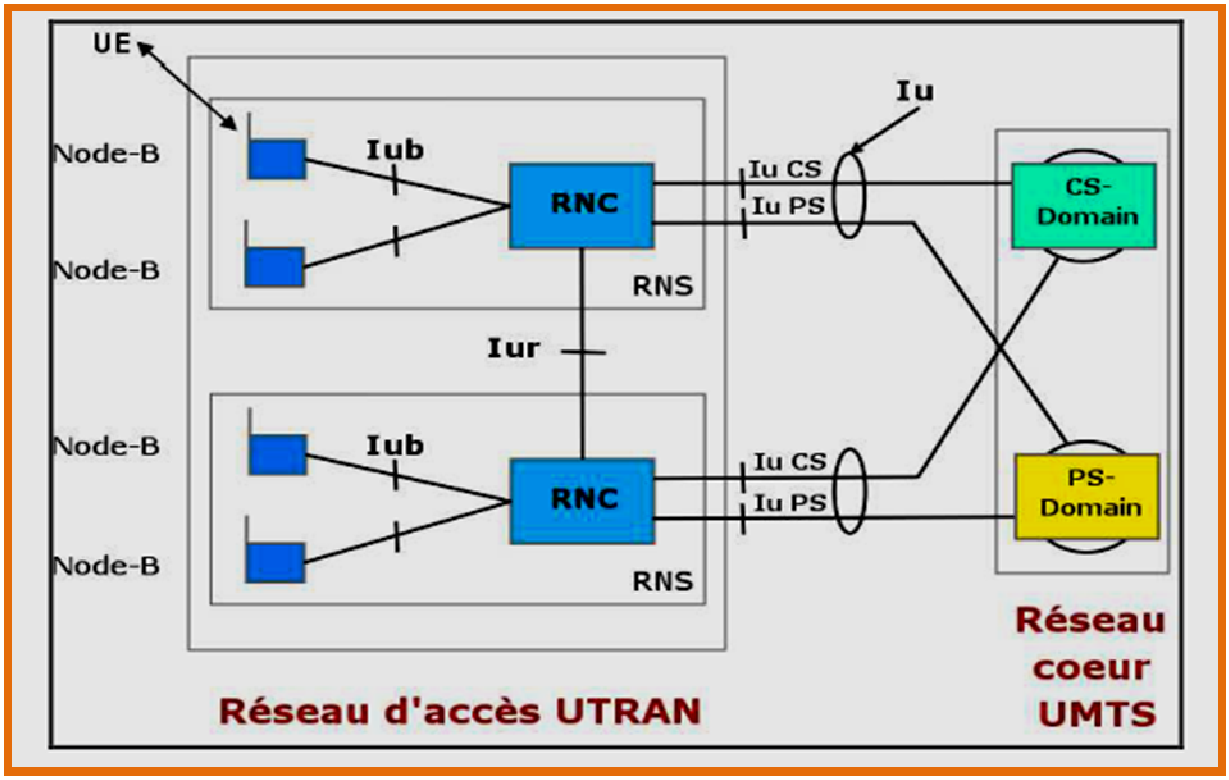


Figure 6: Liaisons du RNC avec le réseau cœur de l'UMTS

1.3 Le réseau cœur:

Le réseau cœur est responsable de la commutation et du routage des communications (voix/données) dans le même réseau ou vers les réseaux externes. Il se décompose en deux parties: le domaine paquet PS (Packet Switching) et le domaine circuit CS (Circuit Switching).

✓ Le domaine circuit (CS):

Ce domaine permet de gérer les services temps réels tels que les appels téléphoniques, la visioconférence et les applications multimédia. Le débit supporté par ce mode peut atteindre 384 Kbits/s. Le domaine CS est composé de plusieurs modules :

- **Le MSC (Mobile-services Switching Center**) est en charge d'établir la communication avec l'équipement usager. Il a pour rôle de commuter les données.

- **Le GMSC (Gateway MSC)** est une passerelle entre le réseau UMTS et le réseau téléphonique commuté PSTN (Public Switched Telephone Network). Si un équipement usager contacte un autre équipement depuis un réseau extérieur au réseau UMTS, la communication passe par le GMSC qui interroge le HLR pour récupérer les informations de l'usager. Ensuite, il route la communication vers le MSC dont dépend l'usager destinataire.

- **Le VLR (Visitor Location Register)** est une base de données, assez similaire à celle du HLR, attachée à un ou plusieurs MSC. Le VLR garde en mémoire l'identité temporaire de l'équipement usager.

✓ Le domaine Paquet (PS):

Le domaine paquet est constitué d'un backbone IP. Le routage des informations se fait soit dans le même réseau, soit vers les réseaux paquets externes. Ce domaine traite les services non temps réel tels que le téléchargement des fichiers ou des E-mails, les jeux en réseau, la navigation sur le web etc. Le temps de transfert pour ce type d'applications n'est pas important. Le débit pourra atteindre 2 Mbits/s. Le réseau IP est basé sur un SGSN (Serving GPRS Support Node) jouant le même rôle que le MSC/VLR en mode paquet et un GGSN (Gateway GPRS Support Node) pour faire transiter les données vers les réseaux externes de transmission de données. Le domaine PS repose en principe sur deux éléments clés à savoir, le SGSN et le GGSN.

- **SGSN (Serving GPRS Support Node)**

Le SGSN est l'interface logique entre l'abonné et un réseau de données externe, sert de passerelle permettant l'acheminement des données dans les réseaux mobiles GPRS, Il est dans le même niveau architectural que le MSC.
Ses fonctions principales sont:

- La gestion des abonnés mobiles actifs (mise à jour permanente des références d'un abonné et des services utilisés) d'une façon similaire à la VLR.
- La gestion des liens logiques comme l'établissement de session, le maintien et la libération de la ressource.
- Le relais des paquets de données, Il assure les fonctions de sécurité et de control d'accès (authentification, paramètres, les procédures, cryptage, …).
- La collecte des tickets CDR (Charging Data Record) relatif à chaque UE.
- Le Support des tunnels GTP à travers Iu-Ps et l interface Gn/Gb.

- **GGSN (Gateway GPRS support node):**

Le GGSN est le nœud d'interfonctionnement entre le réseau de données extérieur et le réseau mobile de transfert de paquets. Il a le même niveau hiérarchique que le GMSC, il offre des fonctions d'établissement de Contact entre les éléments du GPRS et les PDN (Packet Data Network), le GGSN permet les fonctions suivantes:

- Le transfert de données et signalisation au SGSN via l'interface Gn.
- Le routage de paquets vers le(s) SGSN.

Chaque PDN (Packet Data Network), est accessible à partir du GGSN par son APN (Access Point Name), chaque APN doit être associé à un ensemble d'adresses statiques ou correspondantes à un VPN. Le GGSN supporte des adresses statiques et dynamiques, l'assignation d'adresse IP à la MS se fait durant l'établissement du contexte PDP relatif à

chaque APN. Le GGSN supporte RADUIS qui est un protocole AAA (Authentification, Authorization and Accounting) via un serveur RADUIS rattaché au GGSN, il permet de faire l'authentification des utilisateurs lors d'une demande d'un service précis. L'authentification est faite soit à base du MSISDN ou d'un login et mot de passe.

✓ Les éléments en Commun:

- **HLR (Home Location Register):**

C'est l'unité fonctionnelle utilisée pour la gestion des abonnés mobiles. Deux types d'informations sont stockés dans le HLR: les informations de l'abonné et une partie des informations du mobile pour permettre aux appels entrants d'être routés vers le MSC.

- **EIR (Equipement Identity Register):**

C'est la base de données qui contient la liste des identités des équipements. Elle permet d'identifier les équipements non autorisés et leur refuser l'accès au réseau.

- **AUC (Authentication Center):**

C'est le centre qui fournit les clés et les algorithmes pour maintenir la sécurité des identités des abonnés, et pour chiffrer les informations.

2 les interfaces réseaux et le contexte PDP:

Les échanges des informations entre les éléments du réseau UMTS et entre ce dernier et les réseaux externes respectent une série de protocoles permettant de mettre en place un nombre de procédures assurant l'établissement et le maintien d'une communication.

2.1Les interfaces réseaux pour le domaine CS:

Les interfaces de communications au niveau réseau d'accès sont décrites dans la figure suivante:

Interface	Localisation	Descriptif en bref	Equivalent GSM /GPRS
Uu	UE – UTRAN	Interface radio qui permet au mobile de communiquer avec l'UTRAN.	Um
Iu	UTRAN – réseau fédérateur	Iu – CS permet au RNC de communiquer avec le MSC/VLR	A
		Iu – PS permet au RNC de communiquer avec le SGSN	Gb
Iur	RNC – RNC	Communication entre deux RNC, notamment dans le cadre de la procédure de macro diversité.	-
Iub	Node B - RNC	Communication entre le Node B et le RNC	Abis

Figure 7: Interfaces au niveau UTRAN du réseau UMTS

2.2Les interfaces réseaux pour le domaine PS:

Les interfaces réseau permettant une communication entre les équipements du réseau cœur du l'UMTS d'une part et entre ce réseau cœur et les réseaux externes sont:

- L'interface Gc: elle est utilisée par le GGSN pour interroger le HLR et identifier ainsi l'adresse IP du SGSN auquel la station mobile est rattachée et cela dans le cadre de l'activation d'un contexte PDP initié par le GGSN.
- L'interface Gf: elle est définie entre le SGSN et l'EIR, elle permet ainsi de vérifier l'authenticité de l'équipement mobile auprès de l'EIR.
- l'interface Gi: elle permet d'assurer le transfert de données en connectant le PLMN avec des réseaux de données externes.
- l'interface Gn: elle est utilisée entre les entités GSN, elle assure la gestion des déplacements entre SGSNs, l'établissement, le maintien et la libération de tunnels et le transfert des données d'usager entre SGSN et GGSN.
- l'interface Gr: elle est utilisée par le SGSN pour contacter le HLR afin d'obtenir des données de souscription d'usagers GPRS.
- l'interface Ga: elle a pour rôle de connecter un GSN à une entité CG servant dans le transfert de tickets de taxation.

2.3L'activation du contexte PDP:

Pour échanger des paquets IP via le réseau GPRS, l'UE doit activer un contexte PDP. La procédure d'activation de contexte PDP (PDP Context Activation) (figure 8) déclenchée par l'UE, après l'attachement au réseau UMTS, lui permet d'être connue de l'entité GGSN concernée.

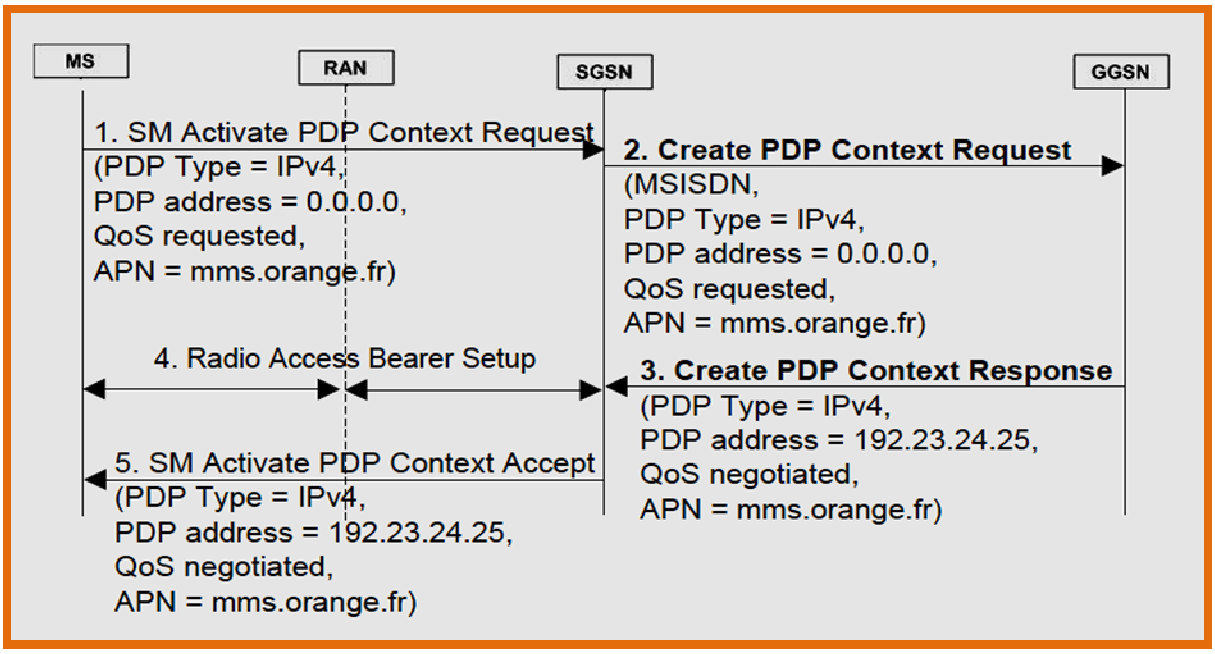


Figure 8: Etablissement du contexte PDP dans le réseau UMTS

- Au cours de cette procédure, l'UE communique au SGSN via la commande SM Activate PDP Contexte Request, le point d'accès au réseau externe auquel il souhaite se connecter (i.e. APN), le type d'adresse IP quel souhaite obtenir, appelé PDP Type, et la QoS requise.
- Le SGSN traduit à l'aide du DNS l'APN en l'adresse IP du GGSN qui supporte l'APN, puis émet une demande d'établissement d'un tunnel réseau à ce GGSN, appelé Create PDP Contexte Request. Les paramètres fournis par l'UE sont inclus ainsi que son MSISDN.
- Une négociation de qualité de service est engagée. Le GGSN alloue une adresse IP du type demandé et la retourne dans la réponse Create PDP Context Response ainsi que la QoS négociée.

- Le SGSN doit maintenant demander au RNC d'établir un RAB entre l'UE et le SGSN. Le RAB est constitué d'un tunnel radio entre l'UE et le RAN et d'un tunnel d'accès entre le RAN et le SGSN.
- Une fois le RAB établi par le RNC, le SGSN peut retourner à l'UE la confirmation d'établissement du contexte PDP via le message SM Activiate PDP Context Accept. L'UE peut donc commencer à émettre et recevoir des paquets IP.

3l'évolution de l'UMTS vers un réseau tout IP:

3.1 l'évolution vers le sous système multimédia (IMS):

Dans le domaine des réseaux mobiles, le système UMTS évolue dans sa globalité vers une architecture réseau flexible s'appuyant entièrement sur le protocole IP. Dans cette architecture, on n'a pas besoin de réaliser la distinction des domaines de commutation de circuit et de commutation de paquet, parce que les services temps réel et non temps réel seront traités simultanément en tant que services multimédias IP.
Le groupe de normalisation 3GPP a défini ainsi dans ses spécifications, les différentes releases permettant le passage à cette architecture tout IP (annexe 1). La principale innovation de la release 5 (figure 9) apportée à l'architecture du réseau cœur UMTS est l'introduction d'un nouveau sous-système permettant de connecter le domaine PS à des réseaux IP proposant des services multimédias. Ce sous-système est appelé sous-système multimédia IP (IMS).
L'IMS représente ainsi un pas décisif vers un réseau cœur tout IP car même le service de téléphonie desservi par le domaine de commutation de circuit CS peut être servi par ce sous-système suivant l'approche VoIP (voix sur IP).

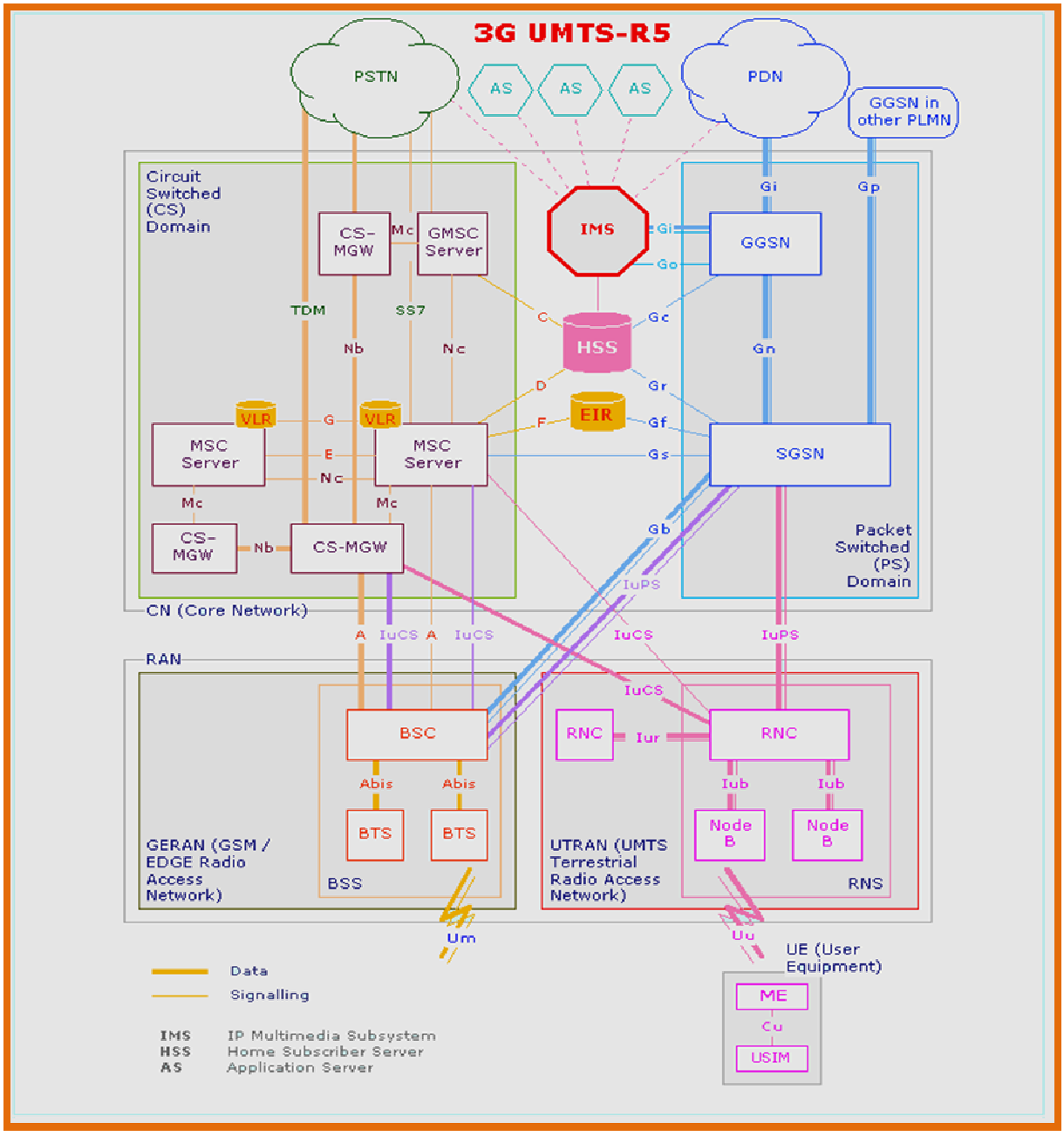


Figure 9: Architecture du réseau UMTS release 5

3.2 L'évolution vers l'architecture « one tunnel »:

Les éléments impliqués sur le plan contrôle et le plan usager pour un contexte PDP, Jusqu'à la Release 6, sont l'UE, le Node B, le RNC, le SGSN et le GGSN. Afin d'améliorer les performances du réseau UMTS, une architecture plate a été considérée à partir de la Release 7.

Cette nouvelle architecture a l'option d'une architecture « one-tunnel » dans laquelle le réseau établit un chemin direct **« Direct Tunnel »** pour le trafic usager entre le RNC et le GGSN sans passer par le SGSN. Les éléments impliqués sur le plan usager sont donc l'UE,

le Node B, le RNC et le GGSN. Par contre le SGSN est toujours présent sur le plan de contrôle pour l'établissement du contexte PDP. Cela permet de minimiser le nombre d'éléments ayant à traiter le trafic usager et donc réduire les délais ainsi que simplifier l'ingénierie du réseau (figure 10).

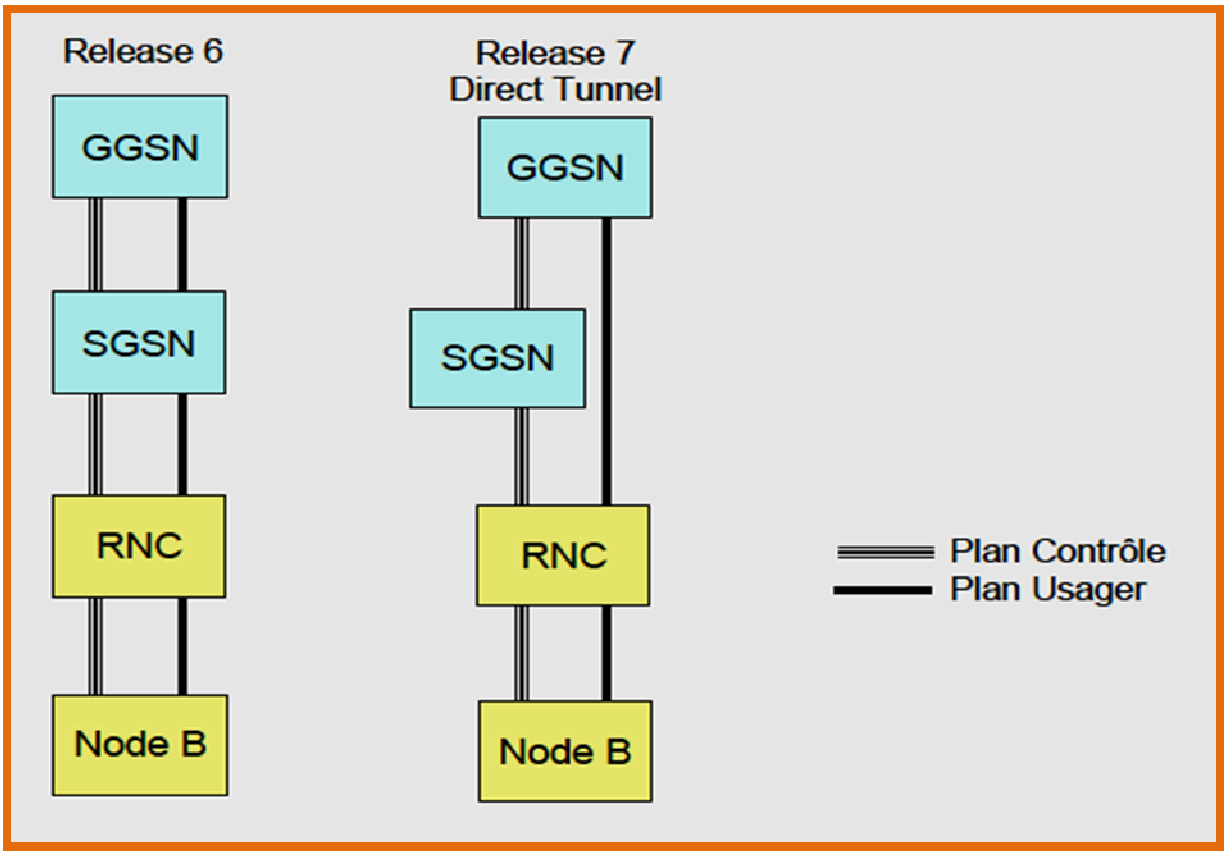


Figure 10: Evolution de l'architecture UMTS vers une architecture « one-tunnel »

Conclusion:

Dans ce chapitre, j'ai exposé une synthèse de recherches liées à l'évolution du réseau UMTS qui présentera ensuite un acquis sur lequel je me suis basée pour assurer l'aboutissement du projet. L'objectif du prochain chapitre sera une étude de faisabilités des solutions SIG et ICache avant de les déployer au niveau du réseau mobile.

Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Chapitre 3: Etude de faisabilité des solutions SIG et ICache

ANNEE UNIVERSITAIRE 2011- 2012

Introduction:

Les solutions SIG et ICache s'avèrent répondre au besoin actuel de l'opérateur Maroc Telecom. Elles assurent une optimisation intelligente de la bande passante allouée en bénéficiant des fonctionnalités d'inspection de paquets au niveau applicatif. Ces solutions se basent sur une architecture disant novatrice qui s'appuie sur un ensemble de protocoles et un ensemble d'équipements assurant de multiples fonctions.

Avant d'implémenter ces solutions au niveau du réseau mobile global, une étude de faisabilité analytique est primordiale pour s'assurer de leurs performances et de leurs réponses aux exigences.

Comme première étape de cette étude de faisabilité au niveau physique logique et fonctionnel, je procéderai par comprendre les fonctionnalités et savoir leurs réponses aux exigences ou non, sur les équipements, leurs capacités et leurs qualités techniques pouvant éviter tout type de redondance ou de panne dans un tel réseau télécom, sur l'architecture logique et sa facilité d'intégration dans le réseau sans aucun impact sur le fonctionnement actuel.

1. Le cahier de charge:

1.1 La technologie de l'inspection de paquet DPI:

Les technologies d'inspection de paquets au niveau applicatif (DPI) consistent à analyser les contenus des paquets IP en forçant leur passage par un serveur DPI. En fonction des critères de contrôle, le DPI autorise ou interdit le transit des paquets vers leur adresse destination.

1.1.1 Le Principe de fonctionnement:

Le principe général repose sur le contrôle des paquets IP selon une liste de critères définis par l'opérateur télécom. Ces critères peuvent être de plusieurs natures: URL, numéro de port.., Les paquets qui répondent aux critères de contrôle ou de blocage subissent un traitement particulier, par exemple un routage différent du reste du trafic.

Les critères sont compilés et triés par catégories avant d'être chargés dans le système DPI. Ces critères de contrôle ou de blocages doivent être configurés selon les exigences de l'opérateur télécom. Quand les utilisateurs tentent d'accéder à l'internet, le système DPI vérifie les politiques de contrôles de ces utilisateurs avant d'interdire ou d'autoriser l'accès par exemple à la page web demandée (figure 11).

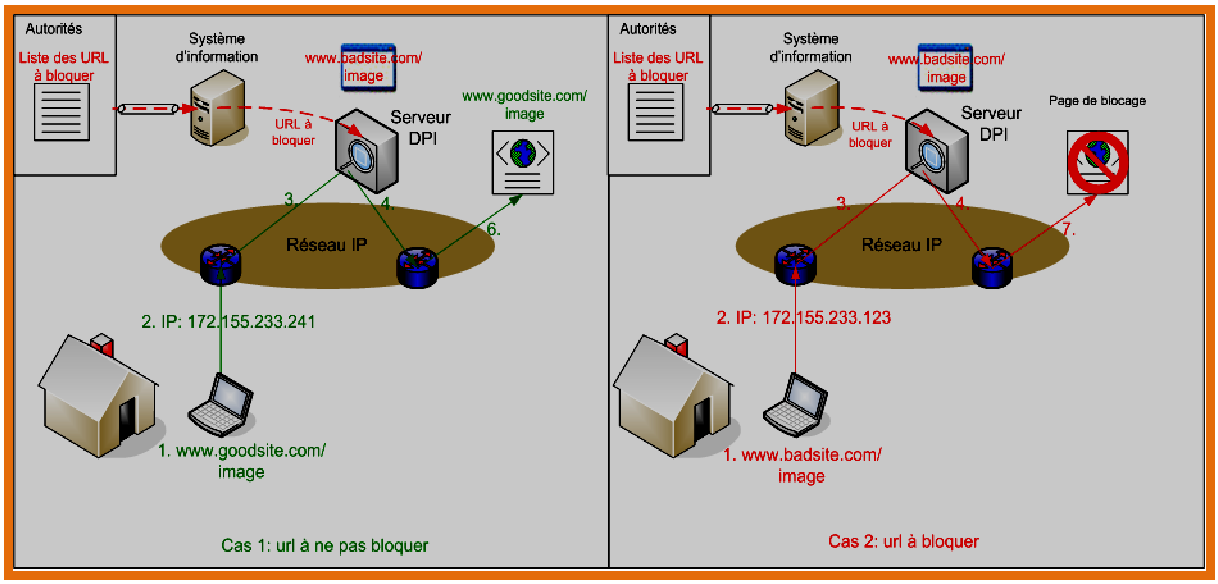


Figure 11: Principe de fonctionnement de la technique d'inspection de paquets

1.2 Le cahier de charge élaboré:

Le cahier de charge élaboré prend en charge le critère d'inspection de trafic au niveau applicatif, le blocage sera appliqué sur certains services qui apportent leur lot de pression sur la bande passante internet. Il contient les exigences suivantes:

1.2.1 Les exigences fonctionnelles:

Les solutions envisagées devront vérifier les critères fonctionnels suivants:

- Les solutions doivent permettre l'inspection, le contrôle, la détection et l'analyse du trafic sur les interfaces Gi des GGSN 3G.
- Les solutions doivent supporter les abonnés post payés et prépayés d'IAM.
- Les solutions devront offrir au minimum les fonctionnalités suivantes.
    - Deep packet inspection
    - Allocation de la bande passante par service / flux / abonné,
    - Application de la politique de contrôle par trafic/APN/flux/abonné,
    - Possibilité d'appliquer le DPI sur les flux d'un APN donné,
    - Identification de trafic selon les méthodes suivantes:
        - Analyse de l'adresse IP,
        - Analyse du/ des numéros de ports,

- Identification et éventuellement blocage du trafic en fonction de l'application, à titre indicatif il doit être possible d'identifier séparément les applications suivantes:
  - P2P,
  - VoIP.
- Visualisation/monitoring temps réel de l'occupation de la Bande passante par flux de service.
- Application des politiques de contrôle suivantes.
- Allocation de la bande passante : définition des seuils en bande passante.
- Gestion de la QoS : dégradation de la QoS, attribution d'une QoS spécifique etc.
- Limitation du nombre de sessions par utilisateur.
- Blocage de trafic: blacklisting.
- Possibilité de redirection de l'utilisateur vers un portail ou une page web (adaptés à la charte graphique d'IAM): dans le cas où l'utilisateur a atteint le seuil d'utilisation d'un service particulier.

- Les solutions devront être fournies avec une interface graphique permettant une gestion, une administration à distance des équipements ainsi que la configuration des politiques de contrôle du trafic.

1.2.2 Les exigences dimensionnement et capacité:

Les solutions envisagées devront vérifier les exigences de dimensionnement et capacité suivantes:

- Les solutions proposées devront être suffisamment dimensionnées pour supporter l'actuel trafic du réseau Maroc Telecom.
- Les solutions devront suivre le trafic si la capacité demandée augmente.

1.2.3 Les exigences intégration dans le réseau Maroc Telecom:

Les solutions envisagées devront vérifier les critères d'intégration dans le réseau de l'opérateur Maroc Telecom suivants:

- Les solutions devront être intégrées dans le réseau d'IAM sans aucun impact sur le fonctionnement actuel des nœuds interconnectés.
- En cas de problèmes sur la solution, le trafic ne doit connaitre aucune perte, et les différents services de navigation doivent continuer à fonctionner.

1.2.4 Les exigences rapports et statistiques:

Les solutions envisagées devant vérifier les exigences rapports et statistiques suivantes:

- Les solutions devront générer les statistiques relatives au fonctionnement de la solution sous format directement exploitable, et exportables sur des serveurs externes. Ces

statistiques seront générées périodiquement (par heure, jour, semaine et mois). L'administrateur doit pouvoir visualiser et imprimer ces statistiques sous forme de tableaux, de graphiques, et d'histogrammes de répartition.

- Les solutions devront produire au minimum les statistiques et les rapports suivants:

  - Rapports du trafic global, Downstream et Upstream.
  - Rapports du trafic global par type de protocole.
  - Rapports spécifique relatif à un protocole ou application bien défini.
  - Rapports de classement des tops Hosts et top Servers (adresse IP) par package d'applications pour le suivi des volumes de trafic ou statistiques des serveurs les plus consultés (Web servers, Mail servers,…etc.).

Les exigences élaborées tiennent un rôle primordial et déterminant. Elles vont faciliter l'étude de faisabilités des solutions ICache et SIG choisies.

2. La solution SIG et son étude de faisabilité:

2.1 L'étude de faisabilité technique des équipements de la solution SIG:

Dans ce paragraphe je me suis chargée d'identifier, auprès du fournisseur Huawei, quatre points pertinents assurant les performances techniques de la solution SIG. Ils se résument dans la capacité du système, la qualité des équipements, la redondance, et la maintenance.

2.1.1 Les équipements physiques:

- **La SIG FE (Front-end):**

Elle est basée sur l'interconnexion de plusieurs cartes de traitements insérées dans des **slots** chacune à son propre rôle permettant en ensemble de recueillir des données, de donner ensuite des statistiques sur le trafic et de les signaler enfin au système back-end (SIG-BE).

✓ **Répartition des slots au niveau SIG FE:**

Les slots sont des tiroirs où une carte de traitement est insérée, les différentes cartes de traitement (figure 12) assurant les fonctions de la SIG FE sont:

- Les LPUs (Line Processing Units), ce sont des unités responsables, dans un premier temps, de la réception du trafic pour l'envoyer ensuite à d'autres unités assurant d'autres fonctions, dans un second temps, elles effectuent une politique de blocages ou de contrôles selon les commandes reçues du système BE.
- Les SPUs (Service Processing Units), ce sont des unités responsables de l'analyse des paquets reçus et l'identification des protocoles utilisés sur le réseau.

- Les MPUs (Main Processing Unit), ce sont des unités responsables de la surveillance de l'état des dispositifs du système SIG FE, elles sont en communication avec toutes les unités du système (front end).
- Les SFUs (Switch Fabric Unit), ce sont des unités responsables de l'interconnexion (le switching) des différentes unités cités ci-dessus.

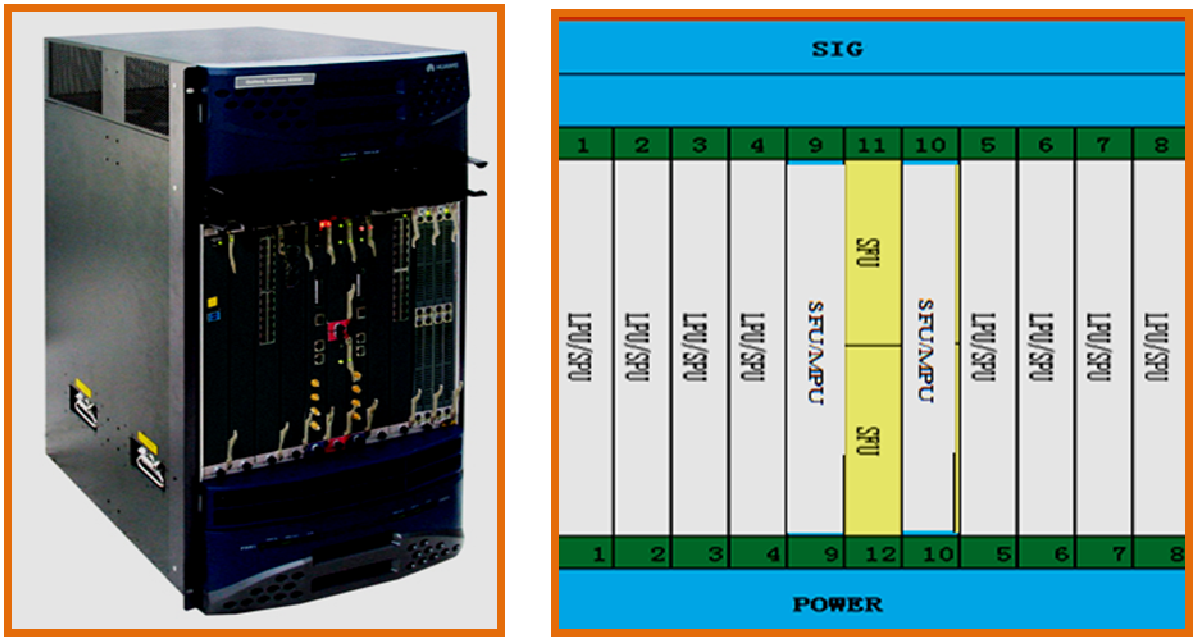


Figure 12: Apparence de la SIG FE et répartition des différentes slots

- Les Slots de 1 à 8: elles sont réservées pour les unités LPUs et les SPUs.
- Les Slots 9 à 10: elles sont réservées pour les unités SFUs et MPUs.
- Les Slots 11 et 12: elles sont réservées pour les unités SFUs.

La SIG-BE

Cette plate forme a un role primordial, elle est capable d'appliquer, selon les informations et les statistiques du trafic actuel recueillies et envoyées par la SIG FE, une politique de contrôle selon les profiles des abonnés déjà configurés dans le Storage Device.

✓ Répartition des slots au niveau SIG BE

Les slots sont des tiroirs où il est inséré une carte de traitement, les différentes cartes de traitement (figure 13) assurant les fonctions de la SIG BE sont:

- Les SMMs (Shelf Management Module), ce sont des unités responsables de la gestion de l'ensemble du système concluant la gestion du matériel, alarme et les enregistrements
- Les BHs/BRs (Service Processing Units), ce sont des unités responsables de traitement et des fonctions principales de la plate forme SIG back end.

- Les SWUs (Switch Units), ce sont des unités responsables de l'interconnexion (le switching) des différentes unités cités ci-dessus.

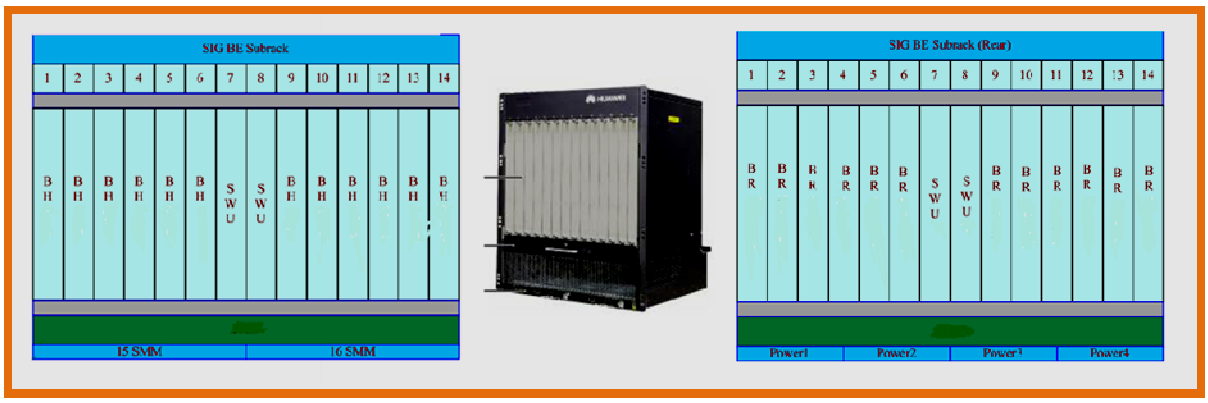


Figure 13: Apparence de la SIG BE et répartition des différentes slots

- Les Slots 1 à 6 et 9 à14: elles sont réservées pour les unités BH/BR.
- Les Slots 7 à 8: elles sont réservées pour les unités SWUs.
- Les Slots 15 à 16: elles sont réservées pour les unités SMMs.

- **Le Storage Device:**

Il s'agit d'un ensemble de disques destiné à stocker tous les fichiers de données tels que les politiques de contrôles configurées, les informations sur les abonnés et les informations du système (figure 14).

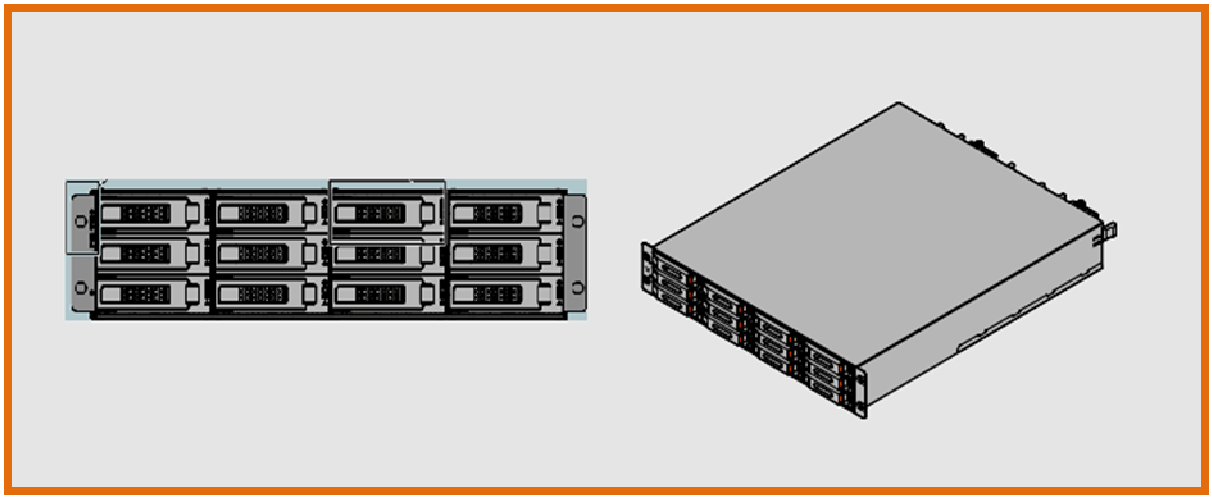


Figure 14: Apparence du Storage Device

- **Le Bypass:**

Ce module, offre une gamme complète de mécanismes de protections du réseau de l'operateur télécom (figure 15).

Figure 15: Apparence du Bypass

- **Le Switch:**

Ce commutateur est utilisé pour connecter les différents équipements. (figure 16).

Figure 16: Apparence du Switch

2.1.2 La qualité des équipements physiques:

La qualité des équipements internes ou externes est un point primordial qui doit être vérifié par tous les composants du système SIG. Dans ce sens, la plate forme matérielle SIG hérite d'excellentes caractéristiques de conception, elle adopte une architecture physique interne performante se basant sur les architectures FPGA+NP et les architectures ASIC+FPGA+ multicoeurs pour le traitement des paquets de données. Cette architecture en termes de dispositifs ne répond pas seulement aux exigences de DPI, haute performance et bas temps pour le traitement des données mais aussi la conception unitaire du matériel et l'architecture à haute densité permet, en outre, d'économiser efficacement l'espace et réduit la consommation d'énergie, réduisant ainsi le cout de déploiement.

Pour les autres équipements, ils sont issus de gammes ou de familles ayant fait leur preuve en garantissant une meilleure capacité de traitement des données. On trouve ainsi la famille S2600i pour le Storage Device, la famille OP9000 pour le Bypass et la famille S5328 pour les Switch. Le choix de ces familles assure une haute stabilité, sécurité et fiabilité.

2.1.3 Les spécifications en termes de capacités:

Dans ce sens la capacité de la plate forme SIG au niveau de réception et de traitement du trafic du réseau 3G d'IAM est énorme et selon le dimensionnement et le besoin, elle peut supporter tout le trafic et à long terme **(tableau 3).**

	Les spécifications	La performance de la SIG
La capacité totale du système	Le nombre maximum des usagers	10,000,000
	La capacité globale de traitement	2,000 Gbit/s
	Le nombre d'unité font end à gérer	80
La capacité de traitement d'une SIG front end unique	La capacité maximum de traitement	2.5 Gbit/s par SPS
	Le retard d'acheminement	Moins de 200 ms
	le nombre de nouveaux connections par seconde	100,000 par SPS
	Le nombre maximum de connections simultanées	32, 000,000
	Le nombre maximum des adresses IP simultanées	3, 200,000

Tableau 3: Spécifications en termes de capacités de la plate forme SIG

2.1.4 La redondance:

Le fonctionnement en mode redondant est un facteur primordial qui doit être présent et offert par le matériel télécom. Il permet, lorsqu' un équipement interne ou externe est défaillant, de basculer automatiquement sans intervention de l'opérateur vers un autre équipement de secours assurant la même fonction. Cela améliorera ensuite la tolérance aux pannes, la sécurité, et la performance de l'ensemble.

Les composants externes de la plate forme assurent aussi ce point, les cartes MPU/SRU adoptent une redondance de type 1+1, les cartes SFU/SRU adoptent une redondance de type 3+1, les cartes SPU adoptent une redondance de type N+M. Le choix de type de redondance se base sur la nature du composant, sa position dans la plate forme, la sensibilité de sa fonctions et sa capacité de traitement.

En cas de défaillance de la liaison entre GGSN/ et SIG FE, l'équipement Baypass offre une protection complète assurant le retour au fonctionnement sans l'intervention de la plate forme SIG, cela sera via une permutation au niveau de ses deux canaux de protection et celle de fonctionnement usuel **(voire figures 17, 18).**

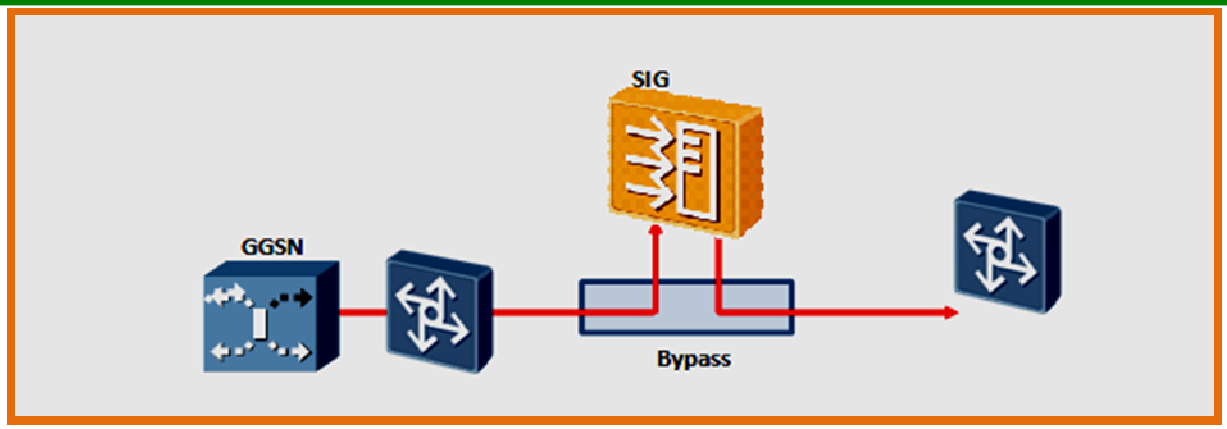


Figure 17:Flux en fonctionnement normal de l'équipement Baypass

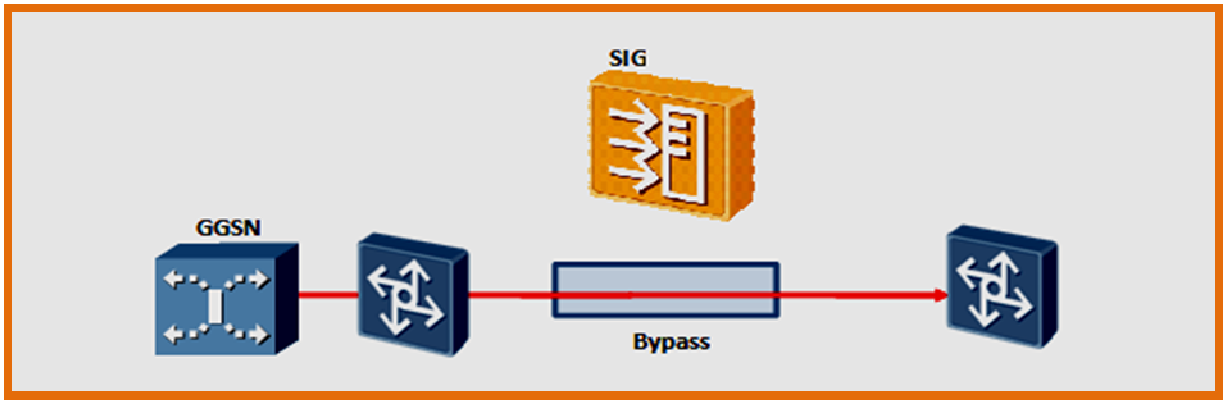


Figure 18:Flux en fonctionnement protection de l'équipement Baypass

Le retour au fonctionnement normal sans l'intervention de la plate forme SIG en cas de panne est important, cela évitera tout type de réclamation prévenant du client en cas de l'interruption de la connexion. Un autre point primordial auquel je me suis intéressée se résume dans le fait de savoir des spécifications temporelles répondant aux exigences d'un temps de réparation court, d'un passage rapide au fonctionnement en mode protection ou en mode normal, d'un temps de redémarrage raisonnable (tableau 4) toute panne ne respecte pas les exigences citées ci-dessus sera immédiatement financé par le fournisseur.

Les paramètres		**Les spécifications**
Le temps moyen entre deux défaillances		25 années
Le temps moyen de réparation		≤ 30 Minute
Le temps de démarrage		≤ 15 Minute
Le temps de basculement du canal de fonctionnement au canal de protection Au niveau de l'équipement Baypass	Le temps actif de basculement	≤ 2 Ms
	Le temps passif De basculement	≤ 8 Ms

Tableau 4: Spécifications en termes de temps de la plate forme SIG

2.1.5 L'utilisation et la maintenance:

Pour que le système soit attractif, sa maintenance et son utilisation doivent être faciles, dans ce stade la plate forme SIG assure une utilisation assez simple réalisée à distance via des interfaces graphiques conçue pour que la communication avec l'utilisateur soit claire, la prise en main, la gestion et l'installation de logiciel se fait aussi à distance à travers le serveur web Pour faire tous ces taches il faut avoir un bon PC-utilisateur muni de la configuration suivante **(tableau 5).**

Les paramètres	Les Caractéristiques
Le microprocesseur	Intel Pentium 1.6 GHz ou supérieur
La mémoire	512 MB ou supérieur
Le disque dur	20 GB ou supérieur
La carte réseau	10/100/1000 Mbit/s
Le système d'exploitation	Windows XP
Le navigateur	Internet Explorer 7.0 ou version ultérieure Mozilla Firefox 3.5 ou version ultérieure

Tableau 5: Paramètres matériels et logiciels du PC-utilisateur

La solution SIG au niveau physique et technique est faisable, elle répond aux exigences de l'opérateur MAROC TELECOM. Le passage à une autre phase assurant l'aboutissement du projet est indispensable.

2.2 L'étude de faisabilité logique de la solution SIG:

2.2.1 La position de la plate forme SIG dans le réseau télécom:

Le système SIG sera placé entre le GGSN du réseau Maroc Telecom et le backbone internet. **(figure 19)**. Cette implémentation demandera des composants d'interconnections, des interfaces de communications entre les équipements d'interfonctionnement.

Le dialogue (signalisation et transmissions des données) entre la plate forme SIG, le serveur RADUIS et la Gateway GGSN sera réalisé par les interfaces de communications, Dans ce sens l'interface Gi assure la communication entre la SIG et le GGSN, l'interface Radius permet l'échange des données d'authentification entre le serveur RADUIS et la SIG, les interfaces privées assurent la communication entre le système back end and front end.

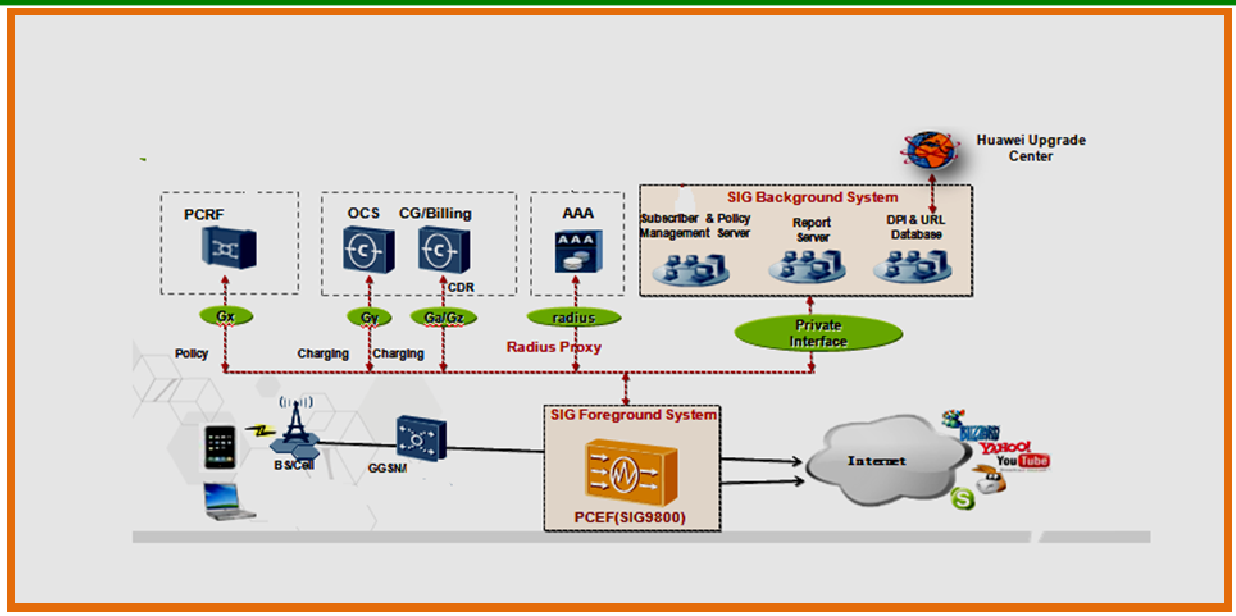


Figure 19: Interconnexion de la plate forme SIG avec le serveur RADUIS et le GGSN

2.2.2 L'orientation du trafic du réseau télécom:

L'élément puisant Baypass, selon le groupe HUAWEI, prend en charge l'orientation du trafic du réseau d'IAM vers la plate forme SIG. La seule interface réseau de communication mise en jeu dans ce cas est l'interface Gi. L'élément Baypass joue un rôle double, l'orientation du trafic vers la plate forme SIG pour le traitement d'une part et le retour au fonctionnement normal en cas de défaillance de la plate forme SIG d'autre part.

Selon cette étude logique, l'intégration de la solution dans le réseau d'IAM sera sans aucun impact sur le fonctionnement actuel des nœuds interconnectés.

2.3 L'étude de faisabilité fonctionnelle de la solution SIG:

2.3.1 La fonction FUP et sa réponse aux exigences:

La fonction FUP ou l'utilisation équitable des ressources de l'opérateur télécom se base sur l'affectation des ressources en termes de bandes passantes aux clients post payé et prépayé en fonction du volume consommé. Dans ce sens lorsque l'utilisation du service internet atteint un niveau de volume, le système SIG réduit la qualité du service (QOS) jusqu'à l'interruption de la connexion lorsque le volume autorisé est insuffisant, la dégradation du débit alloué est proportionnelle au volume consommé par l'utilisateur et à son débit initial au niveau HLR.

Pour l'opérateur MAROC télécom, La dégradation de la qualité en fonction du volume consommé est une solution optimale, elle va assurer une consommation des ressources disponibles. Mais au lieu du scenario de la dégradation proposé, il est exigé un autre type qui réduit la qualité en fonction de volume jusqu'à un seuil ou la QOS est tellement faible

sans l'interruption de la connexion. Ce point est garantit par le groupe HUAWEI par la suite.

Pour assurer la fonction FUP, la SIG doit être en communication avec la plate forme PCRF (Policy and Charging Rule Function), Plate forme qui comprend une BD au niveau de laquelle sont stockées les informations MSISDN, Services Data, Débit et quotas des abonnés. La communication entre ces deux entités est assurée via l'interface Gx (figure 20).

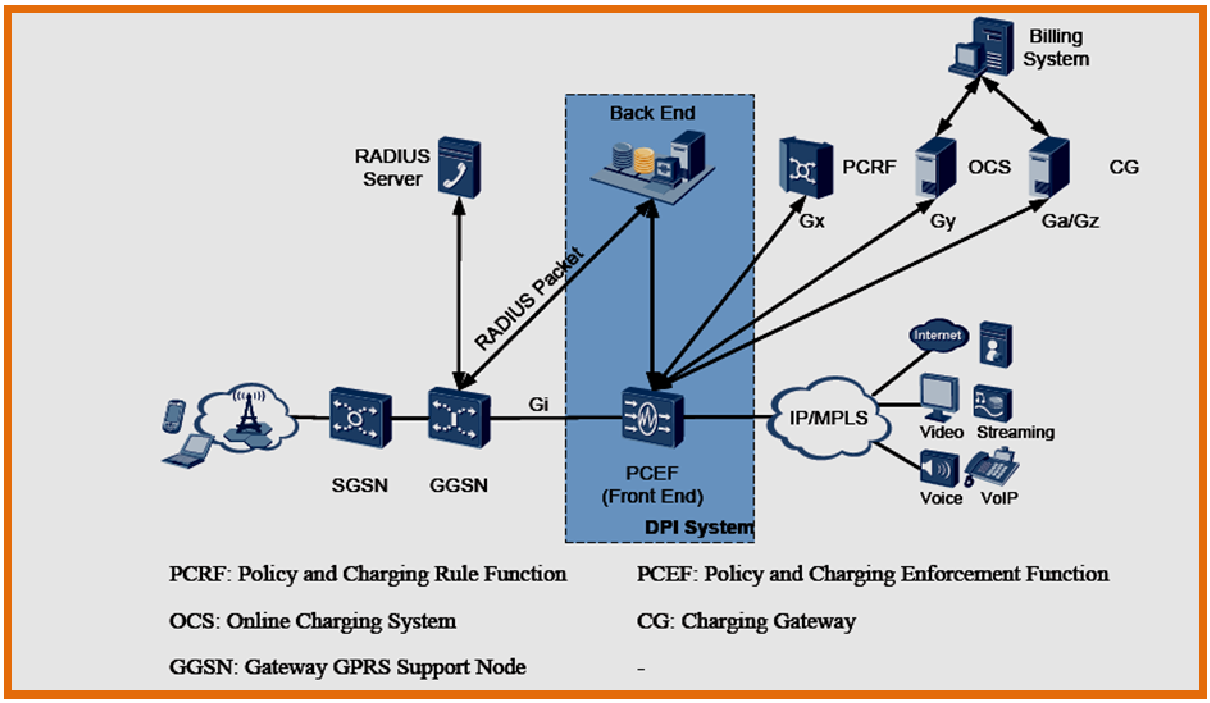


Figure 20: Interconnexion de la plate forme PCRF avec la plate forme SIG

L'établissement de la fonction FUP sur le trafic d'un client, nécessite une définition du package assurant la fonction FUP via l'outil graphique au niveau de la plate forme SIG plus exactement au niveau du serveur POLICY et demande ensuite une définition d'un type de quota au niveau de la PCRF pour contrôler le trafic de ce client (les quotas sont définit suivant une demande de l'abonné ou un choix de l'operateur télécom).

Les scenarios de quotas définis sont multiples, il y a un quota qui permet la gestion de tout le trafic traversant la plate forme SIG, un quota permet la gestion d'un type de trafic (P2P, VOIP…) et un quota permet la gestion de tout le trafic ou un type de trafic dans des périodes précises (par jour, par semaine ou par mois) un quota pour la gestion du trafic montant ou descendant …etc. Un exemple de quota défini au niveau d'un utilisateur particulier (figure 21). Dans la figure ci-dessous le quota défini assure la gestion du trafic de l'utilisateur Bill pendant un mois, cela est réalisé en diminuant la QOS lorsque le volume consommé atteint 50G, 100G et 200G.

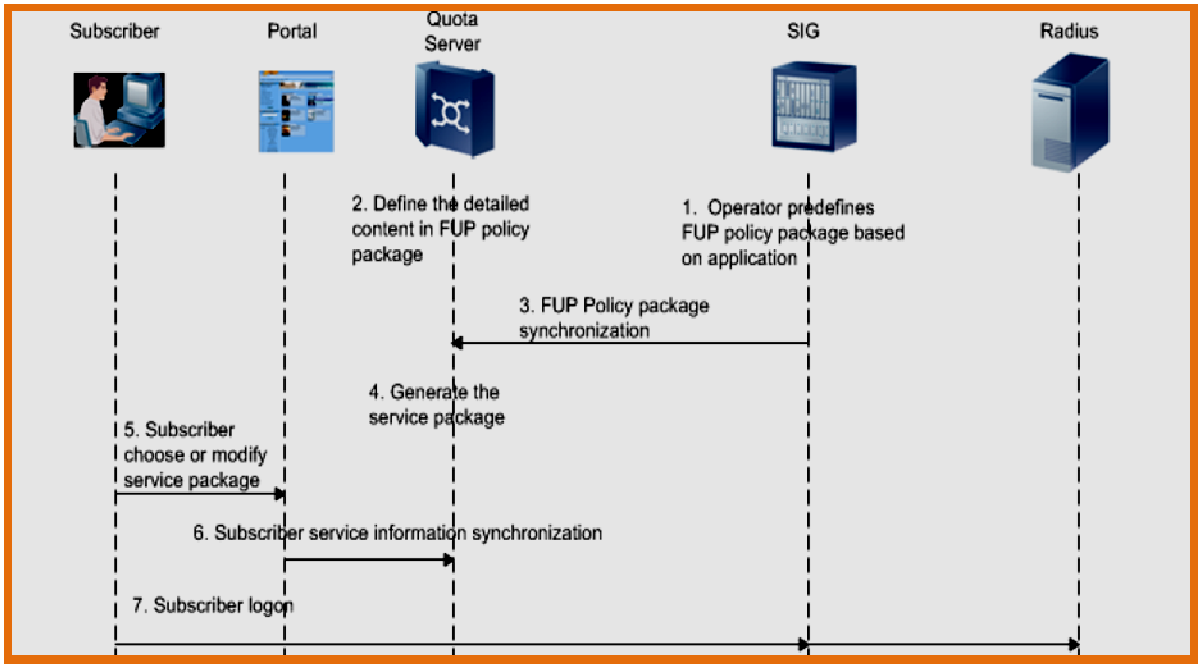
Figure 21: Exemple d'application de la fonction FUP

Apres avoir définir un package désignant la fonction FUP au niveau du serveur Policy, et après avoir signaler un type de quota au niveau de la PCRF.

L'utilisateur peut accéder à un service internet particulier en envoyant un contexte PDP, après son authentification auprès du serveur RADUIS, et avant d'activer le contexte PDP la SIG envoie une notification à la plate forme PCRF où elle demande le quota de cet utilisateur.

Les règles de gestion des abonnés sont configurées au niveau PCRF qui échange les informations de consommation avec la SIG.

Le PCRF envoie les quotas de cet utilisateur à la SIG. L'utilisateur bénéficie du service internet demandé. En même temps, la SIG analyse l'état de son trafic tout en envoyant des mises à jour de son usage en fonction du volume consommé à la PCRF. Celle là effectue aussi des mises à jour sur le quota et envoie le nouveau quota à la SIG et ainsi de suite jusqu'à arriver à un premier seuil qui exige la diminution de la QOS, Après avoir diminuer la QOS, la communication entre le PCRF et la SIG est toujours assurée, la mise à jour des quotas est toujours établit jusqu'à arriver à un seuil ou la QOS affecté sera faible (figures 22, 23).



Figue 22: Définition du quota et authentification de l'utilisateur

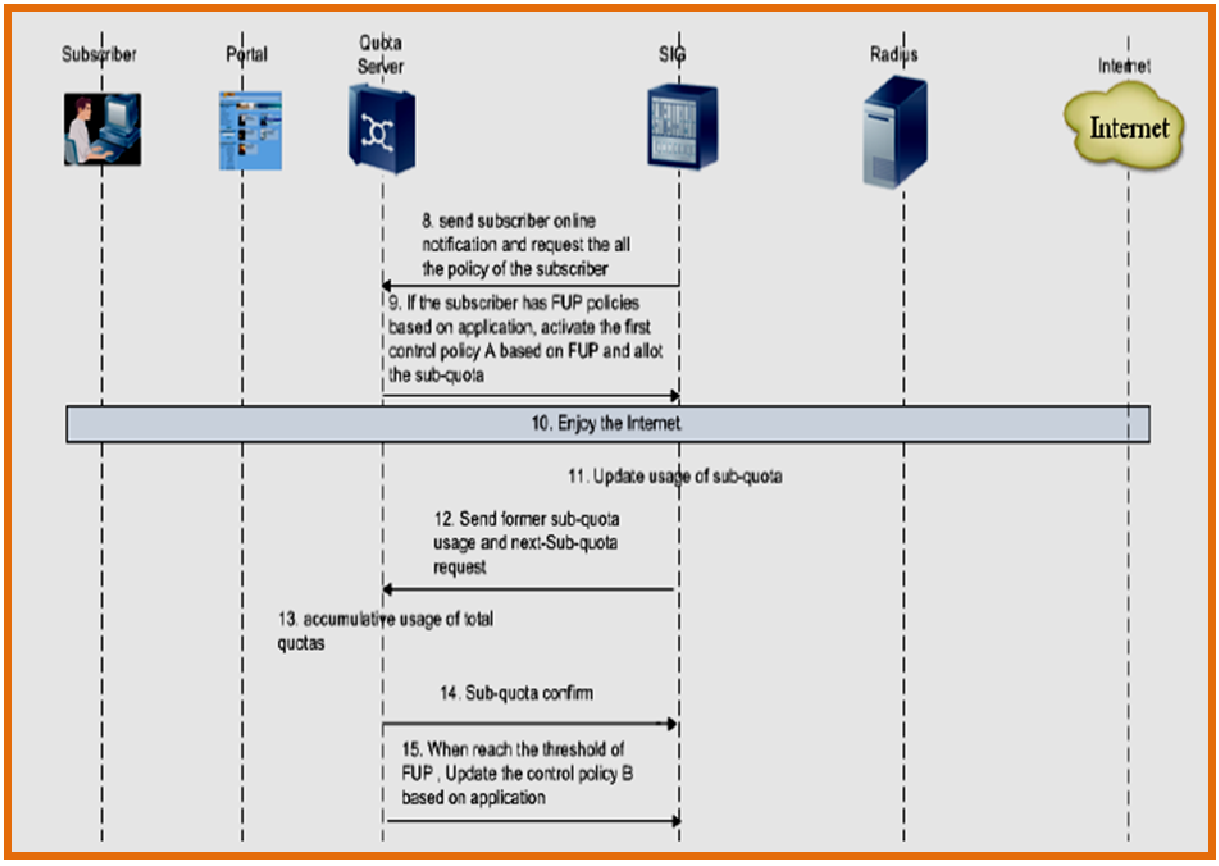


Figure 23: Mise à jour du quota utilisateur

2.3.2 La fonction du filtrage des URLs et sa réponse aux exigences.

Le système SIG assure la fonction du filtrage des URLs visant à limiter l'accès à certains services normalement accessibles sur le réseau internet. La procédure consiste à définir un URL, plusieurs URLs ou une catégorie d'URLs qui identifient certains types de services tels que des sites Malveillants, des sites qui affichent des contenu peu approprié ou pornographiques, des sites de vidéos, illégales, violence….etc.

Lorsque les utilisateurs de l'internet mobile demandent l'accès à un service auquel l'accès est bloqué, la plate forme SIG n'autorise pas l'accès. Ces utilisateurs reçoivent une notification de refus qui comporte la catégorie de demande refusée (figure 24).

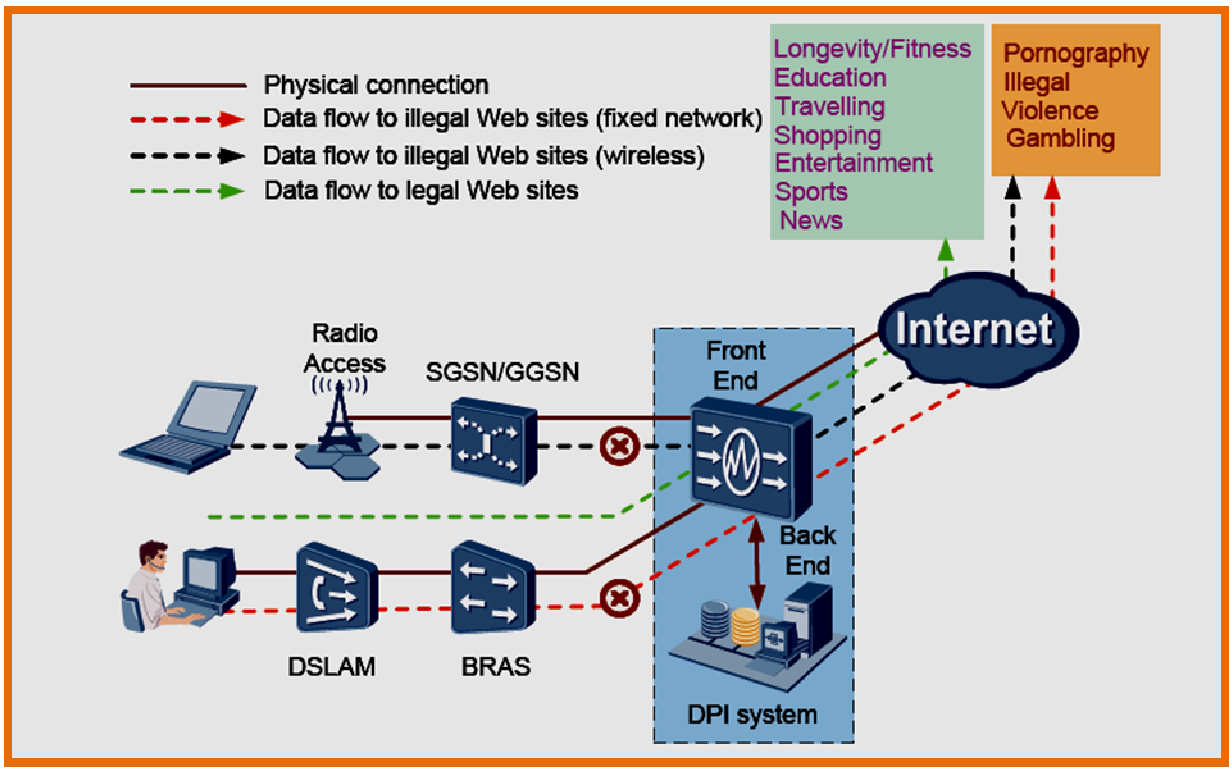


Figure 24: Procédure d'autorisation d'accès ou non à une URL

pour assurer la fonction de filtrage des URLs, il faut définir cette fonction au niveau du serveur « Policy », il faut ensuite entrer les categories des URLs à bloquer au niveau du serveur « URL Classify » tout cela sera via l'outil graphique.

lorsque l'utilisateur veut acceder à un URL, en envoyant un contexte PDP, après son authentification auprés du serveur RADUIS et avant d'activer le contexte PDP.

Le serveur « Policy» signale à la SIG front end qu'il y a une politique de contrôle pour cet utilisateur de nature filtrage URL, la SIG front end interroge le serveur « URL Classify » de la SIG back end de la nature des catégories d'URLs interdits pour cet utilisateur **(**figure 25).

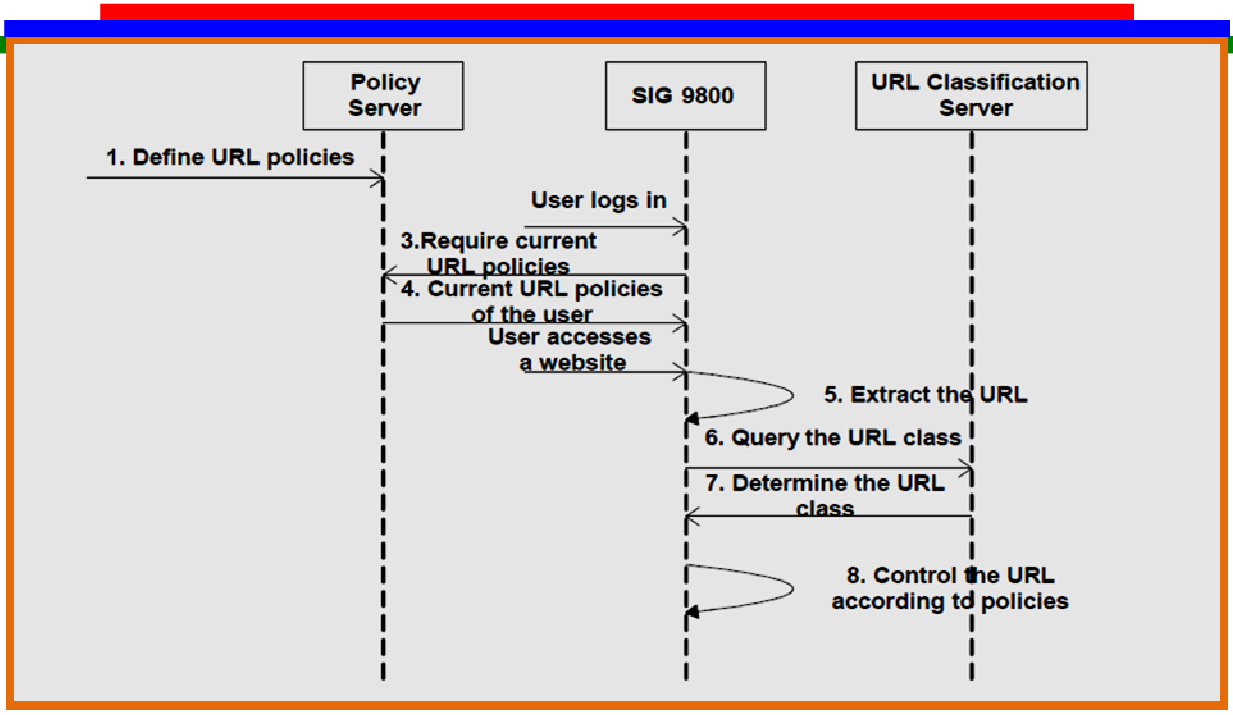


Figure 25: Etapes du flux du service filtrages des URLs

Si l'URL demandé appartient à une catégorie d'URLs interdits, l'utilisateur va recevoir une notification de refus, si l'URL demandé n'appartient pas à une catégorie d'URLs interdits, l'utilisateur va bénificier du service (figure 26).

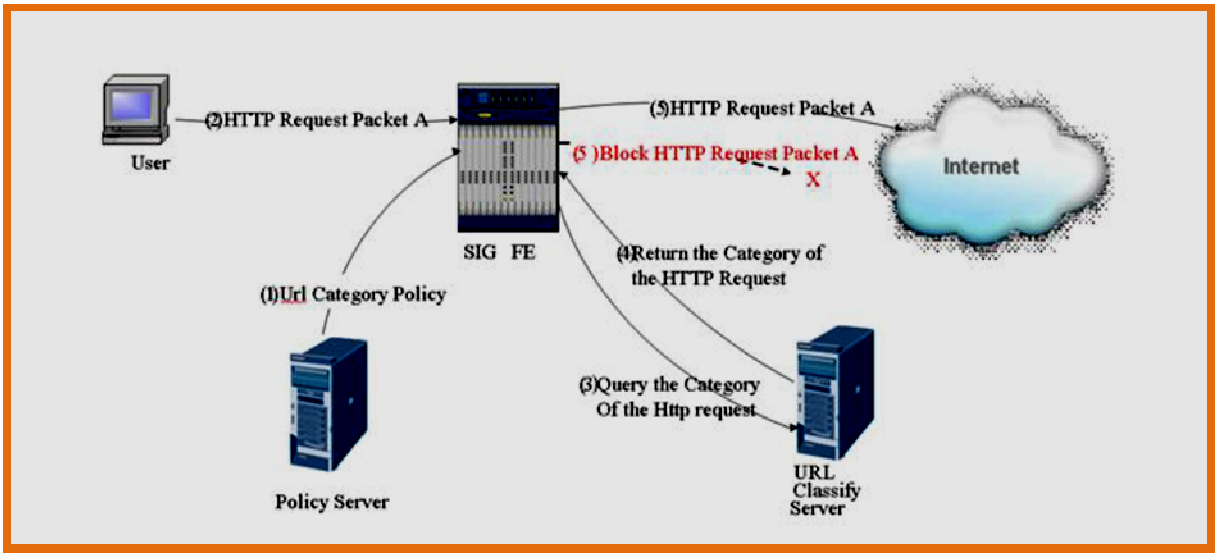


Figure 26: Service filtrages des URLs

2.3.3 La fonction contrôle parental et sa réponse aux exigences.

Le contrôle ou filtrage parental est une fonction importante exigé par le service Marketing. Pour satisfaire les parents utilisateurs, il est exigé au groupe Huawei de n'assurer pas

seulement le filtrage des URLs mais plutôt de restreindre dans un premier temps l'accès de leurs enfants aux certains services, sites, contenus indésirable ou dangereux, dans un deuxième temps de limiter la durée de la connexion et dans un troisième temps d'appliquer le scénario à partir du portail de MAROC TELECOM via une application web ou l'utilisateur parent peut configurer les paramètres des comptes de ses enfants (figure 27**).C**ette fonction est assurée par le groupe HUAWEI par la suite .

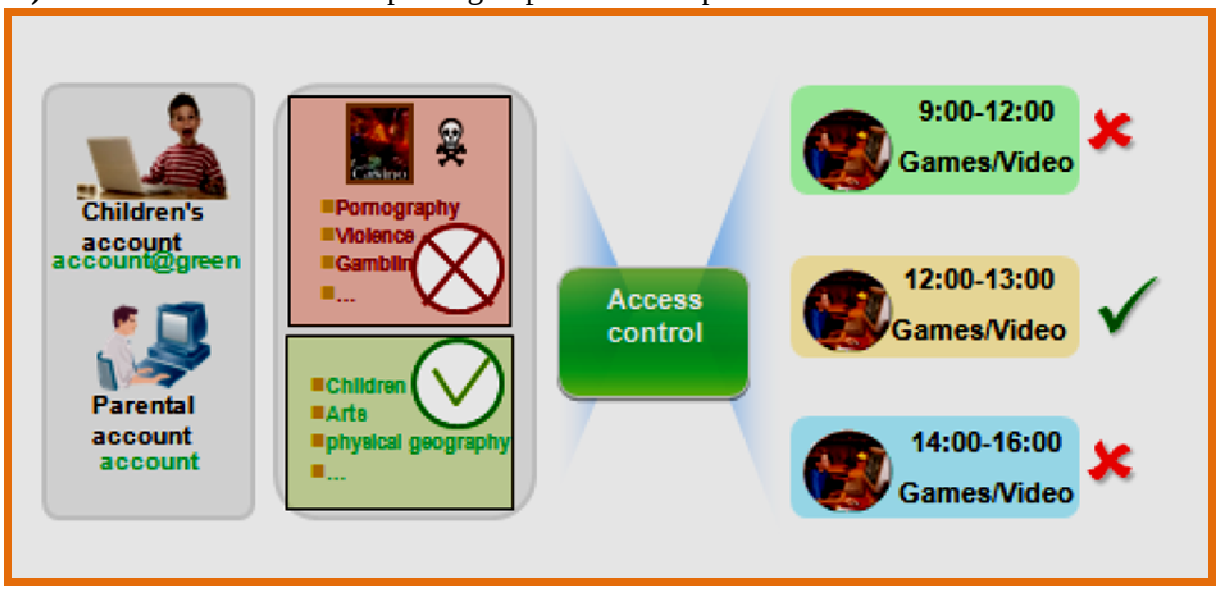


Figure 27: Service contrôle parentale

2.3.4 La fonction de Charging/ Taxation et sa réponse aux exigences:

Cette fonction est importante pour le groupe MAROC TELECOM, elle lui permet d'appliquer les politiques de facturations qui répondent aux exigences actuelles. Cette fonction sera assurée à travers une communication de la plate forme SIG avec le CG (charge Gateway) via l'interface Ga/Gz et par suite avec le BS (Billing System) (figure 28).

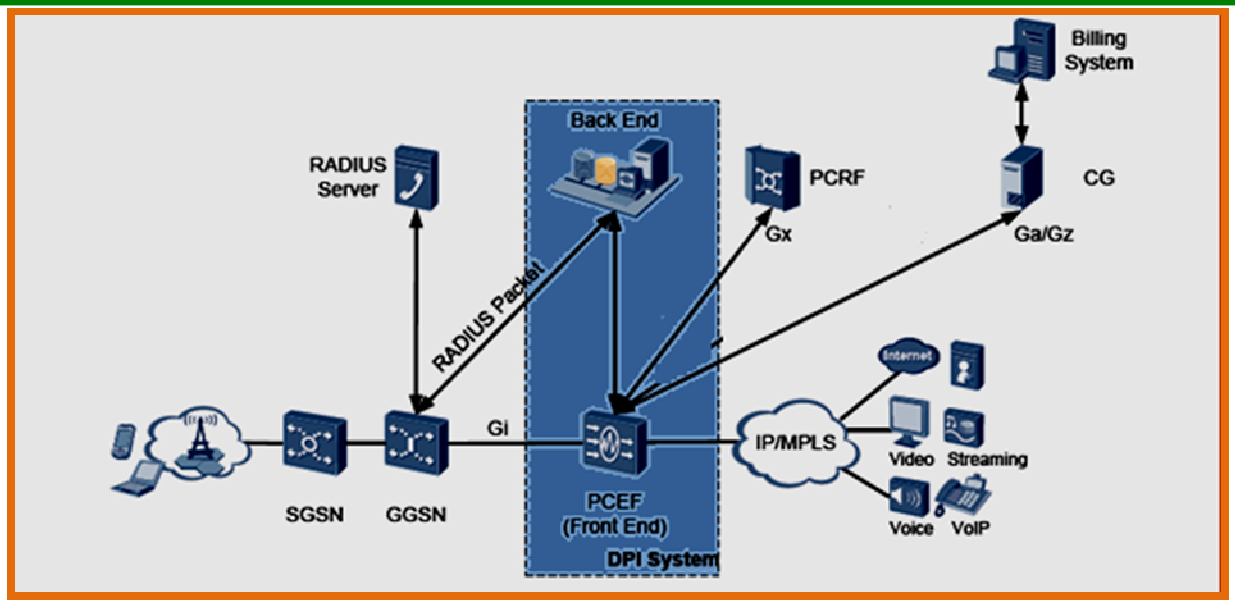


Figure 28 : Interconnexion de la SIG avec le BS et la CG

La procédure se réalise via les informations contenues dans les fichiers CDRS (Charging Data Record) envoyés au CG puis au système Billing. Ces fichiers contiennent des statistiques élucidant les natures de services utilisés ou la durée du temps ou le volume consommé. Le système Billing se chargera ensuite d'établir le crédit de l'utilisateur à payer selon les informations reçues et les politiques de tarifications enregistrées (figure 29). Les fichiers CDRs sont générés par le serveur CFS (Charging Data Record File Server) au niveau de la SIG back end envoyés au CG via l'interface Ga/Gz puis au système Billing.

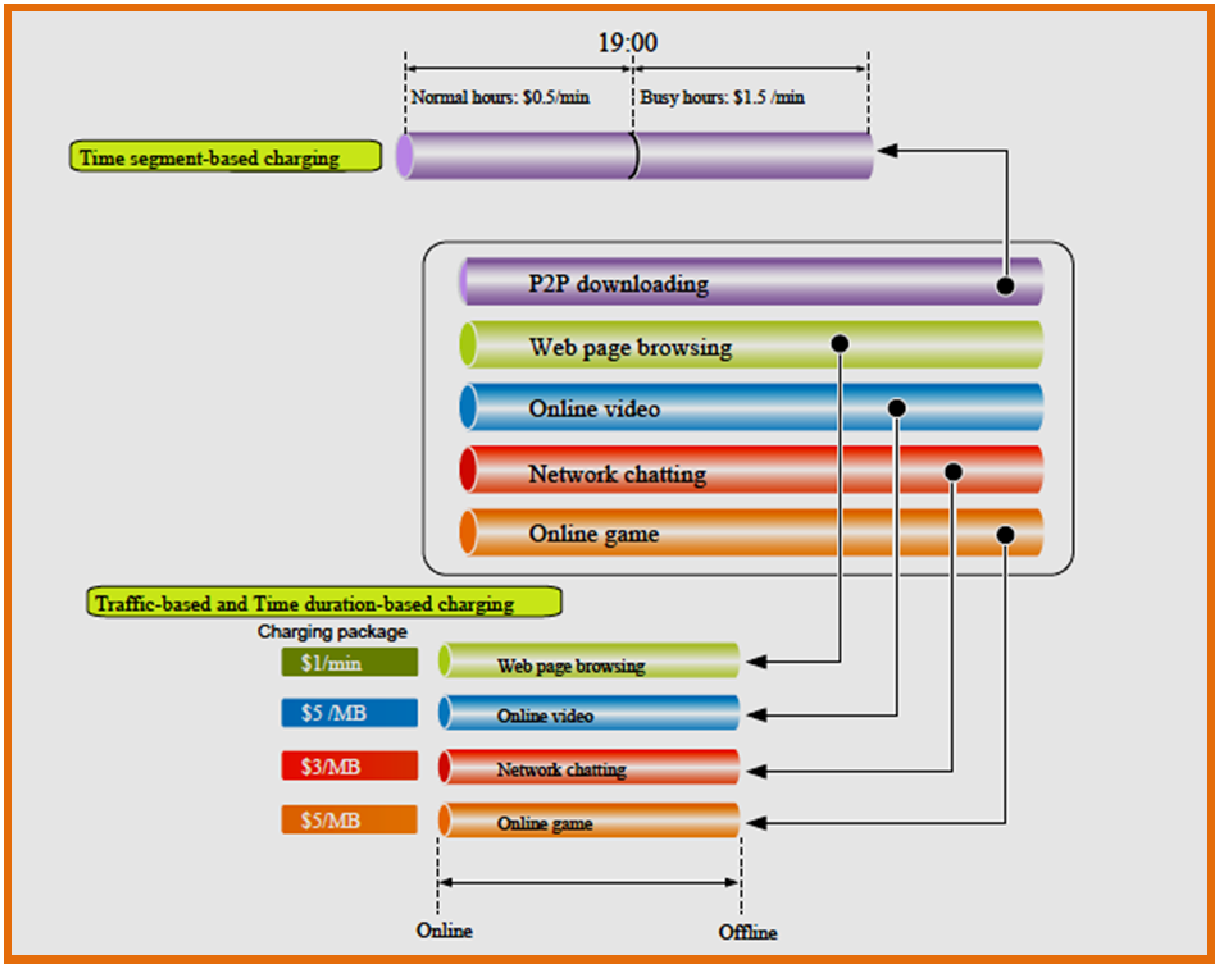


Figure 29: Modes de chargement possibles

Le scenario proposé par le groupe Huawei est puissant surtout pour les abonnés qui veulent bénéficier d'une connexion durable et d'un accès aux applications internet sans contrôle.ils peuvent facturer en fonction de leurs consommations mais pour les autres utilisateurs il est exigé de faire une procédure où l'utilisateur bénéficie des applications internet en fonction de son solde.

Ce point est assuré par le groupe Huawei par l'introduction du système de facturation en ligne OCS (Online Charging System) dans le réseau. La communication avec la plate forme SIG est assurée via l'interface Gz (figure 30).

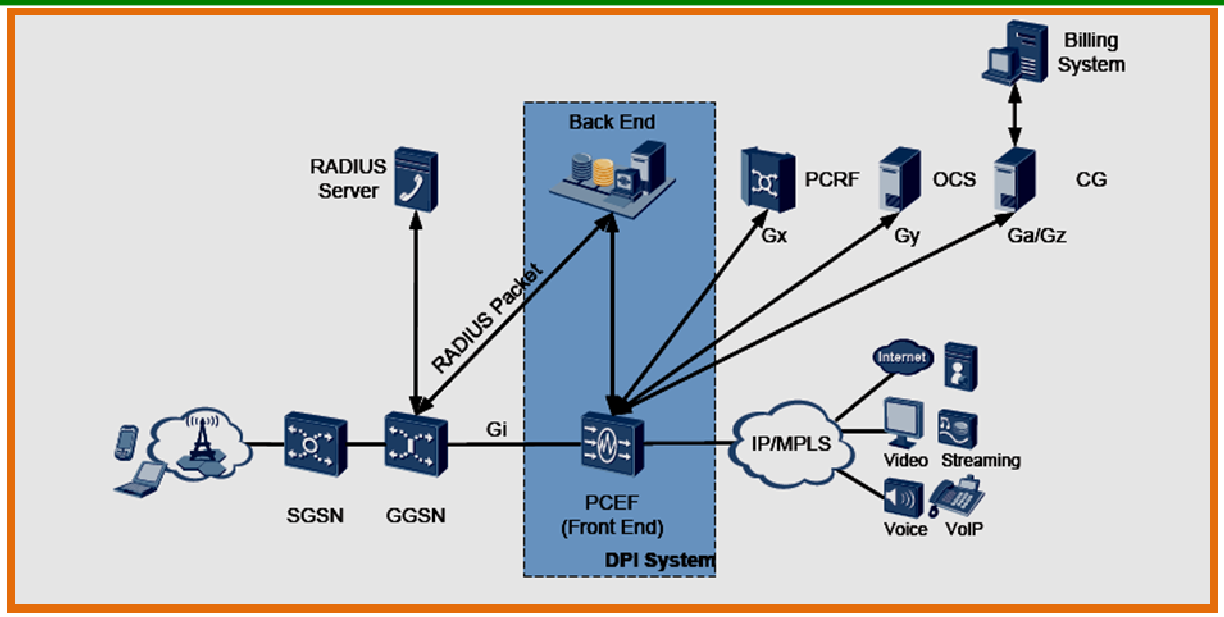


Figure 30: l'interconnexion de la SIG avec l'OCS

Dans ce sens lorsque l'utilisateur commence bénéficier du service temps réel, le système de facturation en ligne (OCS) qui contrôle les soldes des abonnées vérifie s'il ya lieu d'effectuer ce service à l'aide des informations des utilisateurs et les soldes des comptes. Il retrace ensuite l'utilisation actuelle du solde du compte selon les critères du temps du trafic des applications et des protocoles en temps réel. Cela est réalisé via une communication avec la SIG front end qui joue le rôle du PCEF (Policy and Charging Enforcement Function) en chargeant les fonctions et les politiques de facturations Lorsque le solde est insuffisant ou épuisé le service est immédiatement désactivé.

Un autre point est exigé se résume dans le fait de rassembler les deux types de chargements où l'OSC sera responsable de l'attribution des services en fonction des soldes des abonnés alors que le CG sera responsable d'envoyer les fichiers CDRs reçus au système Billing pour calculer le crédit restant en cas d'épuisement du solde de l'abonné. Les politiques de facturation seront en fonction du service ou protocole, du volume ou de la durée du temps

2.3.5 La fonction rapports et statistiques et sa réponse aux exigences.

La plate forme SIG fournit des rapports et des statistiques identifiant le trafic du réseau et le comportement des abonnés (figure 31**).** Les rapports fournis sont en fonction du temps (minute, heure, jour, mois) caractérisant l'état du trafic ou donnant des statistiques sur les services les plus demandés par le client la bande passante allouée, le nombre de clients par trafic, les protocoles en fonction des clients. Ceci permettra à IAM de déterminer les top N des sites, abonnés, protocoles… pour appliquer une taxation préférentielle dépendamment de ces paramètres

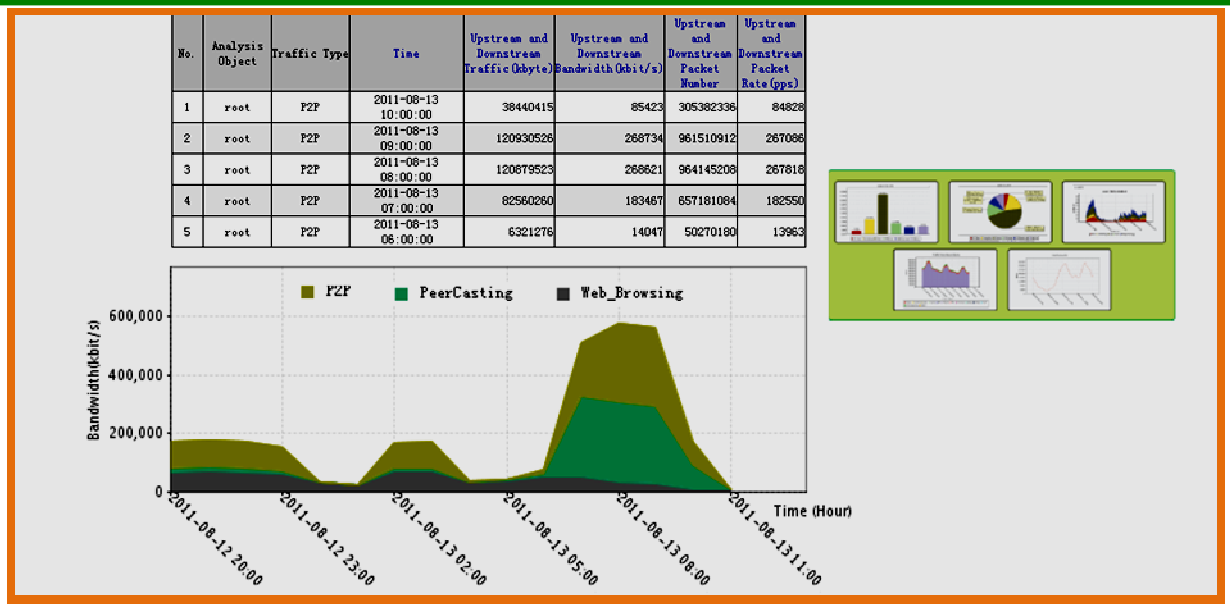


Figure 31: Différents rapports fournis par la plate forme SIG

2.3.6 La fonction IPush (Information pushing service).

La fonction IPush est une fonction importante selon le groupe Huawei dédiée par la plate forme SIG, c'est un service permettant implicitement une gestion efficace de la bande passante, son principe se base sur le fait de pousser les informations d'une société comme par exemple insérer ses annonces ou ses logos permettant de diriger les utilisateurs immédiatement vers son portail.

Donc, il s'agit d'un service dédié aux différentes entreprises, son avantage consiste à tirer pleinement de profit en termes de ressources financières pour mener à bien d'autres services à valeur ajoutée.
Cette fonction semble avoir des avantages pour le groupe MAROC Telecom. Mais avant de décider l'accord de cette fonction je me suis chargée ensuite de faire aussi une étude de sa faisabilité en termes de sa performance et sa réponse aux exigences.
La solution SIG en termes fonctionnelles répond aux exigences de cahier de charge élaboré et assure les nouveaux points et scénarios exigés dans l'étude de faisabilité traitée ci-dessus.

3 La solution ICache et son étude de faisabilité:

3.1 L'étude de faisabilité technique des équipements physique:

3.1.1 Les équipements physiques:

- **Le LBS:**

Il a pour rôle de contrôler ou d'équilibrer la charge du trafic utilisateurs entre les différents CSS-WEB afin d'améliorer la capacité du traitement de la plate forme ICache

- **Le CSS WEB:**

Ou http cache: il permet de cacher automatiquement le trafic http internet des utilisateurs finaux comme.

- **Le MSS**:

En définissant les paramètres et en fournissant des politiques de gestion, le MSS assure le fonctionnement normal du système ICache. il a pour objectif les fonctions suivantes:

- Surveillance de l'état: le MSS met une surveillance globale de l'état et en temps réel en s'assurant que tous les équipements du système ICache fonctionnent normalement.
- Rapports et statistique: le MSS analyse et enregistre les données délivrées par chaque sous système, il fournit des rapports quotidiens, hebdomadaire et trimestriels, les données reflètent l'état générale du système ICache cela facilitera ensuite une gestion et un contrôle de ce système.
- gestion des alarmes: le MSS reçoit les alarmes produites pas les autres sous systèmes ICache. Il délivre ensuite la politique convenable pour gérer les alarmes.

- **Le Switch**:

Il assure la communication entre les équipements cités ci-dessus.

3.1.2 La qualité des équipements physiques

Les équipements de la plate forme ICache sont issus de gammes ou de familles ayant fait leur preuve en garantissant une meilleure capacité de traitement des données. On trouve ainsi la famille P9200 pour le MSS, la famille LBS3600 pour le LBS, la famille S5328 pour les Switch et la famille T3000 pour les CSS-WEB. Le choix de ces familles assure une haute scalability, stabilité, sécurité et fiabilité.

3.1.3 Les spécifications en termes de capacité et redondance:

Après avoir s'assurer de la qualité des équipements, il est le temps de savoir les spécifications en termes de capacités répondant aux exigences du cahier de charge.

A ce stade, et selon le groupe HUAWEI la capacité de la plate forme ICache au niveau de réception et de traitement du trafic du réseau 3G de l'opérateur MAROC TELECOM se mesure à partir des caractéristiques de traitements des équipements LBS, CSS-WEB et

MSS,**(tableaux 6,7)** et les caractéristiques de ces équipements puissent répondre aux exigences de l'opérateur, il faut juste établir un dimensionnement correcte de la solution.

L'équipement LBS3600	
Paramètre	**Valeur**
Capacité de traitement	2 Gbit/s

Tableau 6: Spécifications en termes de capacités de l'élément LBS

L'équipement CSS-WEB	
Paramètre	**Valeur**
Type de disque	**SAS**
Nombre de disque	**12**
Capacité de disque	300 GB *2 (software) 300 GB* 10 (Data)
Débit	>900 Mbit/s
Taux de succès de la demande	40 % to 70 %
Réduction de l'occupation de la bande passante	30% to 80%

Tableau7: spécifications en termes de capacités de l'élément CSS-WEB

Contrairement à la solution SIG qui sera implémentée localement, la solution ICache sera implémentée pour tester un GGSN du réseau mobile d'IAM. Pour ce faire et afin de s'assurer de sa performance en termes de capacité, un dimensionnement est nécessaire.

Pour calculer le nombre nécessaire de chaque sous système de la solution pouvant répondre au besoin actuel, la connaissance de certains paramètres et formules est indispensable.

- **Les paramètres et la formule de dimensionnements de LBS**

Pour calculer la capacité de traitement du LBS, la formule suivante s'est utilisée

W= N*L (1-1) avec W: Required processing capability of the LBS.
N: Number of the CSS-WEBs..
L: Traffic that needs to be processed by the LBS for each CSS-WEB

- **Les paramètres et la formule de dimensionnements de CSS-WEB**

Pour calculer la capacité de traitement du CSS-WEB, la formule suivante s'est utilisée

N = (W*P*M)/L (1-2) N: Number of the required CSSs, which must be rounded up.
W: Actual egress bandwidth (single-way and downstream).
P: Distribution percentage of the protocol.
M: Hotspot rate of traffic.
L: Maximum output traffic of a protocol cache device.

- **Les paramètres et la formule de dimensionnements de MSS**

Pour calculer la capacité de traitement du MSS, la formule suivante s'est utilisée

N=T/L (1-3) avec N: Number of the required MSSs.
T: Number of subscribers.
L: Number of the users allowed by a single MSS.

Les paramètres de dimensionnements nécessaires de l'operateur MAROC TELECOM dans ce Cas sont:

- Le nombre d'abonnés sans fil est de **100.000**.
- Le pourcentage de la bande passante en Upstream et Downstream utilisé est **50%.**
- La capacité du GGSN IP Pool est **5G**.
- Le pourcentage du trafic HTTP downstream est **80%.**

Selon les formules et les paramètres du réseau MAROC TELECOM, le nombre des équipements nécessaires pour supporter le trafic du **GGSN IP POOL** à tester est:

Le MSS:

La formule de calcul de la quantité MSS représentée dans **(1-1)** donne:

- T = 100,000.
- L = 1, 000,000.
- N = 100,000/1000000 = 0.1 **fonctionnement en mode redondant** donne **N=1**.

Le CSS:

La formule de calcul de la quantité CSS représentée dans **(1-2)** donne:

- W= 5Gbit/s x 50% = 2.5Gbit/s.
- P = 80%.
- M = 50%.
- L = 900 Mbit/s.

- N = (2.5Gbit/s *80%*50%*1024)/900 Mbit/s= 1.33 **fonctionnement en mode redondant** donne **N= 1.33*200%=3**.

Le LBS:

La formule de calcul de la quantité CSS représentée dans **(1-3)** donne:

- N = 3.
- L = 650 Mbit/s.
- W = 3 *650 Mbit/s = 1950 Mbit/s = 1.90 Gbit/s **fonctionnement en mode redondant** donne **N=2.**

Après avoir faire le dimensionnement de la solution ICache et s'assurer de son fonctionnement en mode redondant. Un autre point auquel aussi je me suis intéressée se résume dans la résolution du problème dans le cas de défaillance de la liaison entre le GGSN et la plate forme ICache.

Dans ce sens et selon le groupe HUAWEI, l'élément LBS présente un mécanisme de protection puissant. Les deux éléments LBS, justifiés par le dimensionnement traité ci-dessus, Fonctionnent en alternatif en mode actif et en mode standby.

A ce cas le protocole VRRP (Virtual Router Redundancy Protocol), tolérant aux pannes, assure une fiabilité et une continuité de la communication entre tous les équipements du réseau en attribuant une adresse IP virtuelle au LBS virtuel, le protocole élit ainsi un LBS maitre qui traite les paquets envoyés normalement. En cas de défaillance du LBS maitre, le protocole élit le deuxième LBS esclave qui effectue le même rôle que celui défaillant. Les autres éléments de la plate forme ICache sont configurés pour utiliser l'adresse IP virtuelle comme passerelle par défaut.

Si les deux LBS tombent en panne en même temps, ce qui est impossible selon le groupe Huawei, La plate forme ICache joue le rôle d'un nœud vers le backbone internet. Le retour au fonctionnement cache se récupère rapidement.

3.1.4 L'utilisation et la maintenance:

La configuration L'accès et la maintenance de la plate forme ICache se fait à distance via des interfaces graphiques qui facilitent ces taches à l'operateur **(figures 32,33, 34).**

Figure 32: interface graphique pour l'accès à l'élément LBS

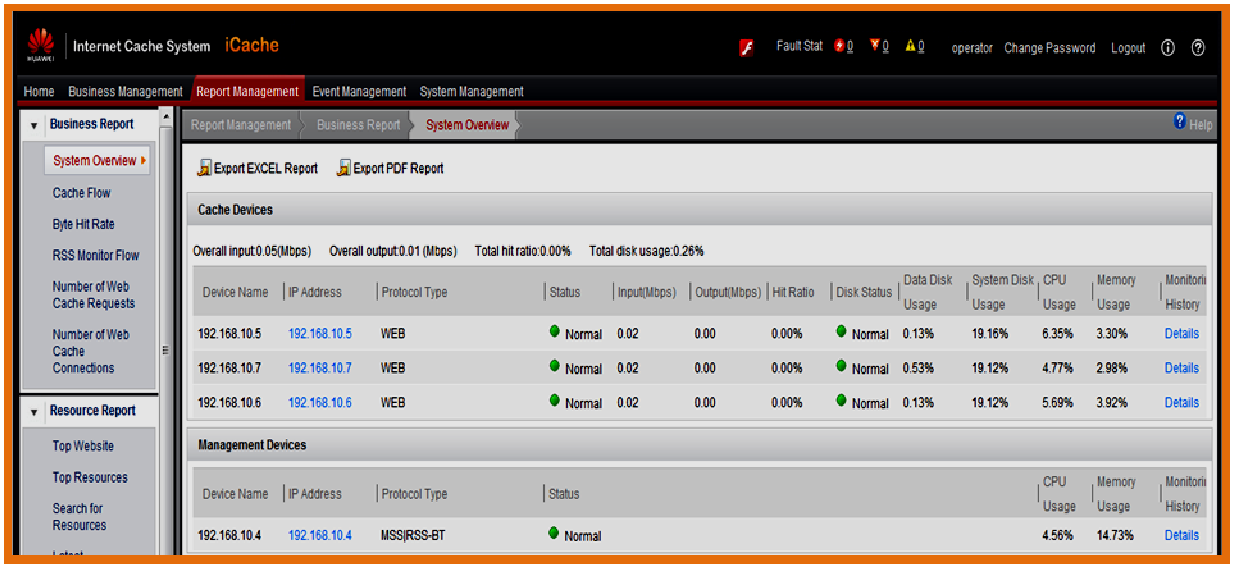


Figure 33: Interface graphique pour l'accès à l'élément CSS-WEB

Figure 34: interface graphique login pour l'accès à l'élément MSS

3.2 L'étude de faisabilité logique de la solution ICache:

3.2.1 la position de la plate forme ICache dans le réseau télécom:

La plate forme ICache se positionne aussi entre la Gateway GGSN du réseau mobile IAM et le backbone internet **(figure 35).**

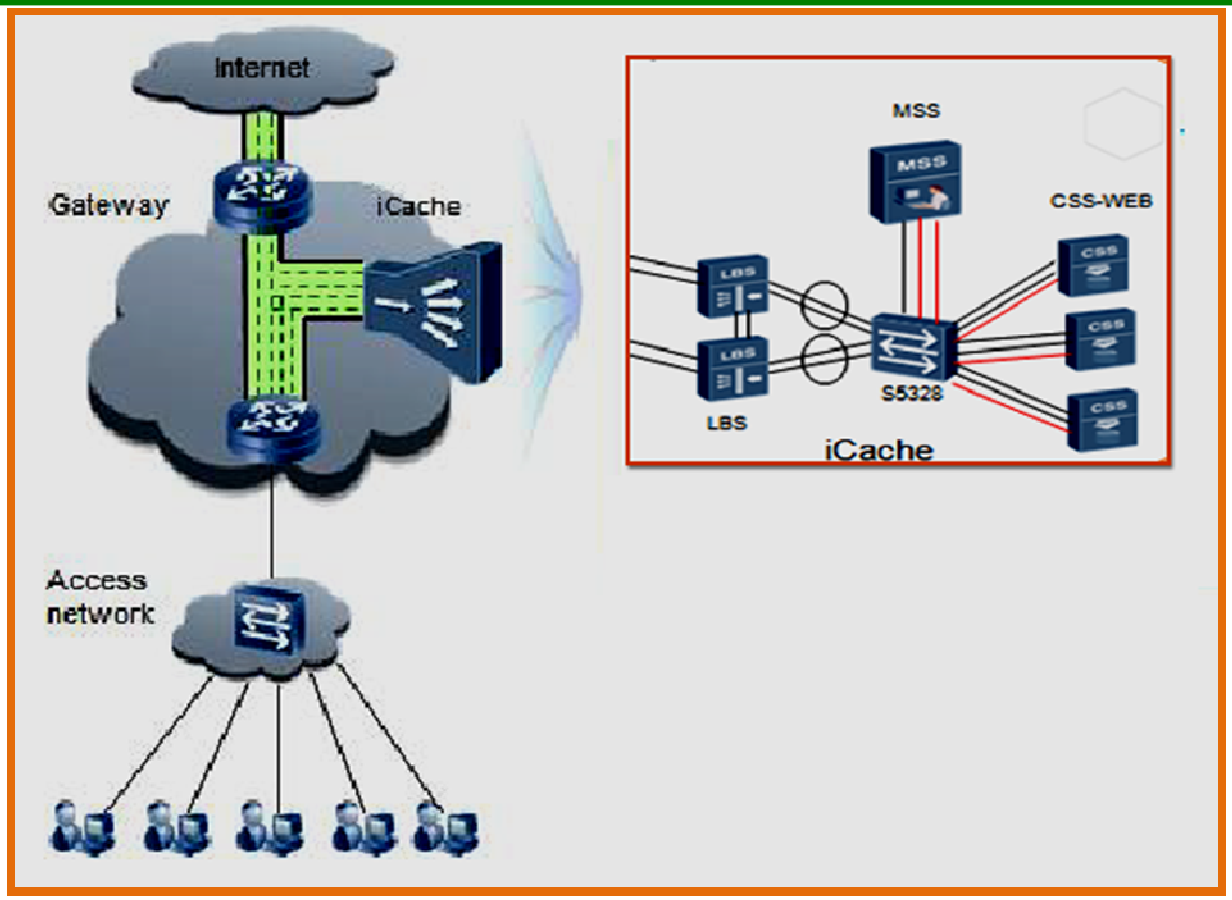


Figure 35: Position de la plate forme ICache au niveau réseau télécom

3.2.2 l'orientation du trafic du réseau télécom

Le protocole PBR (**Policy-Based Routing)** est responsable sur l'orientation du **trafic HTTP et vidéos en ligne** du réseau Maroc Telecom vers la plate forme ICache. Selon le groupe, le GGSN IP Pool doit supporter ce protocole, cela n'a aucune influence sur le fonctionnement du réseau de l'opérateur télécom ni sur les nœuds interconnectés.

3.3 L'étude de faisabilité fonctionnelle de la solution ICache:

3.3.1 La fonction « cache HTTP et vidéo en ligne » et sa réponse aux exigences.

Il s'agit d'une fonction principale de la plate forme ICache, elle adopte la technologie de détection hotspot, lorsque le montant d'accès des utilisateurs internet à une même source HTTP ou vidéos en ligne internet atteint un seuil de hotspot, la plate forme ICache télécharge cette ressource, la met en cache et la fournit ensuite aux utilisateurs qui demandent cette même ressource. La fonction « Cache HTTP et vidéo en ligne » se realise suivant des étapes:

- Etape 1: Lorsque l'utilisateur envoie une demande HTTP au serveur Web, le trafic se dirige vers la plate forme ICache (PBR),

- Etape 2: Si la ressource demandée n'est pas en cache (au niveau CSS-WEB). La CSS-WEB envoie la demande au serveur Web.
- Etape 3: Dans ce cas le serveur web envoie la ressource demandée à la CSS-WEB (PBR).
- Etape 4: Si le montant d'accès à cette ressource n'atteint pas un seuil de hotspot, la ressource sera envoyée directement à l'utilisateur sans la mettre en cache.
- Etape 5: Si le montant d'accès à cette ressource atteint un seuil de hotspot, la plate forme ICache télécharge cette ressource, la met en cache et la envoie ensuite à l'utilisateur.

3.3.2 La fonction « Compression GZIP »:

La plate forme ICache assure la compression GZIP. Dans ce stade, le CSS-Web applique cette compression Gzip sur les ressources avant de les envoyer aux utilisateurs Finaux. Cette fonction se réalise suivant des étapes **(figure 36)**

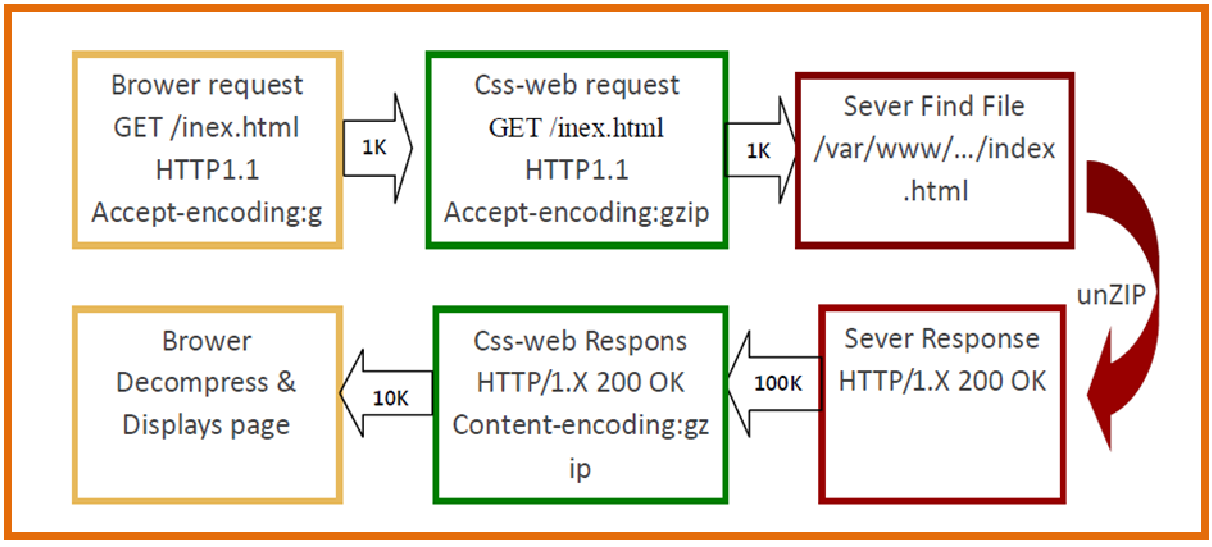


Figure 36: Le flux de http GZIP par CSS-Web:

Les étapes de la réalisation de la fonction « Cache HTTP et vidéo en ligne » sont:

- Etape 1:Le client envoie une demande HTTP pour obtenir le fichier « www / ... / index.html », qui est de 100K.
- Etape 2:La CSS-WEB personnifie en premier temps le client et sa demande pour obtenir le fichier « www / ... / index.html », elle envoie la demande au serveur web.
- Etape 3:Le serveur web envoie le fichier demandé. S'il ne prend pas en charge une compression GZIP, Le fichier sera donc de 100K dans sa transmission vers la CSS-WEB.

- Etape 4:La CSS-WEB reçoit le fichier de 100K, elle le compresse ensuite avant de l'envoyer au client.

3.3.3 La fonction « gestion intelligente de l'espace disque »

Grâce à cette fonction, le système ICache utilise et gère intelligemment l'espace du disque massif. En effet lorsque l'utilisation de l'espace disque atteint le seuil prédéfini, le système ICache nettoie le disque automatiquement et supprime les fichiers qui n'ont pas été accédés fréquemment.

En règle générale, si l'utilisation de l'espace disque est plus de 90%, le système supprime certains fichiers pour recycler l'espace de telle sorte que l'utilisation du disque soit inférieure à 80% **(figure 37).**

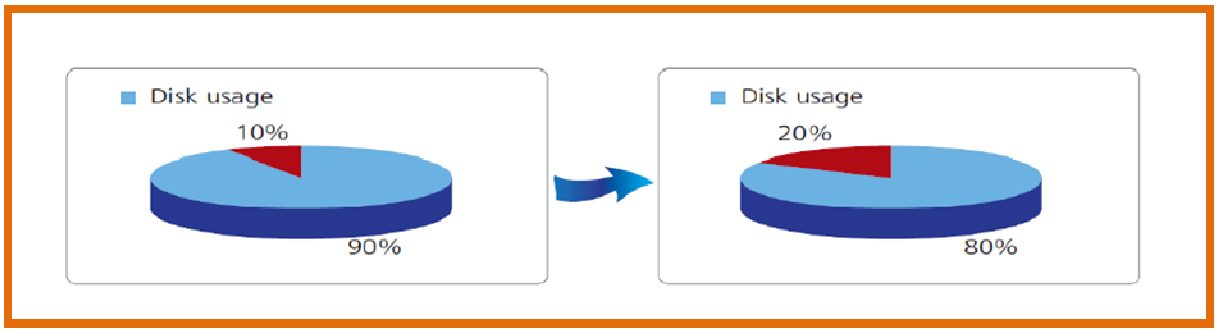


Figure 37: Gestion intelligente de l'espace disque

En général, la solution ICache en termes fonctionnelles répond aux exigences du cahier de charge élaboré, le cache des ressources HTTP et la fonction GZIP sont des critères puissants pouvant optimiser la bande passante internet et améliorer la qualité du service. Pourtant le cache des ressources P2P représente aussi la tendance actuelle de l'opérateur Maroc Télécom. Cette tendance est en cours de traitement par le groupe HUAWEI.

Conclusion

Après avoir explicité ma contribution suivis pour étudier la faisabilité des solutions SIG et ICache en termes de leurs réponses aux exigences de l'opérateur Maroc Télécom. Je procéderai dans ce qui suit, par présenter les différentes phases de déploiement de ces solutions et les différents tests de fonctionnalités établis.

Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Chapitre 4: Déploiement et tests de fonctionnalités

ANNEE UNIVERSITAIRE 2011- 2012

Introduction:

Une fois l'étude de faisabilité des solutions a été validée, la phase suivante sera un déploiement des plates formes SIG et ICache au niveau local pour s'assurer de leurs fonctionnalités.

Pour mener à bien le projet dans cette phase décisive je procéderai en premier temps par préparer les différents types scénarios de tests pouvant répondre aux exigences actuelles. De participer dans un troisième temps dans les différentes étapes de déploiement pour superviser l'avancement du projet, d'entamer finalement une phase de tests à partir de laquelle je peux décider que les solutions conçues sont performantes en termes de leurs réponses aux exigences élaborées et en temps réel.

1. la préparation des tests de fonctionnalités.

Avant d'entamer une phase de déploiement il est indispensable de préparer soigneusement un document de tests fonctionnels pour les deux solutions et le donner ensuite au groupe Huawei.

1.1 La préparation des tests de fonctionnalités pour la solution SIG:

1.1.1 Préparation du test pour la fonction rapports et statistiques:

Pour la fonction rapports et statistiques, il est exigé trois types de tests. Le premier se résume dans l'identification du trafic temps réel du client pendant une heure. Le résultat doit être sous forme des tableaux et des courbes, le PC client doit être muni des logiciels permettant l'accès au Web/P2P/IM/VOIP/Email **(tableau 8).** Le deuxième test se résume dans l'identification de la tendance du trafic des clients, le résultat aussi doit être sous forme de tableaux, courbes diagrammes **(tableau 9).** Le troisième test s'articule autour

l'observation du comportement de chaque utilisateur en donnant le résultat sous forme de diagramme présentant les proportions consommées de chaque abonnée **(tableau 10).**

Type de test	Rapports et statistiques pour le trafic du client en temps réel
Pré-requis	1. Les équipements DPI fonctionnent correctement. 2. Les logiciels P2P/Web/VoIP/Email/IM sont préparés sur le PC client.
Procedure de test	1 L'accès à l'internet et utilisation des applications internet. 2 Observation du trafic en temps réel sous forme de tableau et courbe sur l'interface graphique du système SIG.
Résultat attendu	Le type de protocole utilisé et le volume consommé affichés sur l'interface utilisateur sont les mêmes que ceux sur le PC client.
Résultat du test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 8: procédure du test « identification du trafic en temps réel »

Type de test	Rapport sur la tendance du trafic des clients
Procedure de test	1. L'accès à internet et utilisation des applications internet 2. L'observation du rapport décrivant les tendances du trafic abonné sur l'interface utilisateur du système SIG. 3 Le rapport doit être sous forme de tableau courbe ou table. 4 Les rapports peuvent être exportés en forma PDF,EXCEL OU HTML
Résultat attendu	Le contenu du rapport soit conforme à la circulation réelle.

Résultat du test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 9: procédure du test « rapport sur la tendance du trafic des abonnés ».

Type de test	Rapport sur la tendance du trafic d'un seul abonné
Procedure de test	1 L'accès à internet et utilisation des applications internet. 2 L'observation du rapport décrivant les tendances du trafic d'un seul abonné sur l'interface utilisateur du système SIG. 3 Le rapport doit être sous forme tableau diagramme courbe ou table. 4 Les rapports peuvent être exportés en format PDF, EXCEL ou HTML
Résultat attendu	Le contenu du rapport soit conforme à la circulation réelle.
Résultat du test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 10: procédure du test « rapport sur la tendance du trafic d'un seul abonné »

1.1.2 Préparation du test pour la fonction contrôle de la VoIP:

Pour la fonction contrôle de la VOIP, il est exigé un seul type de tests. Il se résume dans le blocage de la VOIP qui présente actuellement l'application internet la plus intense apportant un lot de pression sur les ressources de l'opérateur Maroc Telecom. Le contrôle consiste seulement sur le blocage de la voix et non pas les données écrites « le Chat ». Les différents tests préparés s'articulent autour le contrôle du Skype **(tableau 11),** le contrôle de Viber (**tableau 12**).

Les mêmes scenarios de tests sont établis pour le contrôle de Yahoo, le contrôle de Google Talk, le contrôle de Fring, le contrôle de Tango, et le contrôle de Nimbuzz.

Type de test	Contrôle du Skype
Pré-requis	1. Le DPI fonctionne correctement 2. Le logiciel Skype est bien installé sur le PC client.
Procedure du test	1. L'accès à internet et utilisation de l'application Skype. 2. La Configuration de la plate forme SIG de façon à appliquer la politique de blocage de l'application Skype pour le client via l'interface graphique.
Résultat attendu	L'application Skype est bloquée après appliquer la politique de blocage (les autres applications internet sont toujours disponibles)
Résultat du test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 11: procédure du test « contrôle de la VOIP (SKYPE) »

Type de test	Contrôle du Viber
Pré-requis	1 Le DPI fonctionne correctement 2 L'application VIBER est bien préparée sur le PC client.
Procedure du test	1 L'accès à internet et utilisation de l'application Skype. 2 La configuration de la plate forme SIG de façon à appliquer la politique de blocage de l'application VIBER pour le client via l'interface graphique.
Résultat attendu	L'application VIBER est bloquée après appliquer la politique de blocage (les autres applications internet sont toujours disponibles)
Résultat du test	

Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 12: procédure du test « contrôle de la VOIP (VIBER) »

1.1.3 Préparation des tests pour la fonction filtrage des URLs.

Pour la fonction filtrage des URLs, il est exigé trois types de tests. Le premier se résume dans le blocage des URLs définies. Dans ce stade il est exigé d'appliquer ce test sur deux sites web www.google.com et www.youtube.com. L'accès sera refusé au deuxième site au niveau de lequel la politique de contrôle est appliquée **(tableau 13). Le** deuxième test s'articule autour **la redirection de l'accès à l'URL** www.google.com vers le portail d'IAM **(tableau 14).**

Type du test	Blocage des URLs prédéfinies
Pré-requis	Les équipements DPI fonctionnent correctement.
Procedure du test	1. L'accès à internet et l'accès à une URL prédéfinie. 2. La configuration de la plate forme SIG via l'interface graphique de façon à appliquer la politique de blocage des URLs sur l'URL prédéfinie précédemment 3. L'accès une deuxième fois à l'URL prédéfinie
Résultat attendu	L'accès à l'URL est refusé après appliquer la politique de blocage (l'accès aux autres URLs est toujours accepté)
Résultat test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 13: procédure du test « blocage des URLs prédéfinies »

Type de test	Redirection pour des URLs prédéfinies
Pré-requis	Les équipements DPI fonctionnent correctement.
Procedure test	1 L'accès à internet et l'accès à une URL prédéfinie. 2 La configuration de la plate forme SIG via l'interface graphique de façon à appliquer la politique de redirection sur l'URL prédéfinie précédemment 3 L'accès une deuxième fois à l'URL prédéfinie
Résultat attendu	L'accès à l'URL est redirigé après appliquer la politique de redirection
Résultat test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 14: procédure du test « Redirection des URLs prédéfinies »

1.1.4 Préparation des tests pour la fonction contrôle parental:

Pour la fonction contrôle parentale, il est exigé un seul type de tests. Il se résume dans la configuration des politiques de contrôle désirées au niveau du portail contrôle parentale (ici le blocage du site web www.facebook.com et la redirection de l'accès à l'application Skype vers le site web www.google.com, En appliquant des politiques de contrôle au niveau du temps) **(tableau 15).**

Type test	Contrôle parental
Pré-requis	1. Les équipements DPI fonctionnent correctement. 2. Le portail contrôle parentale est installé et fonctionne correctement
Procedure test	1 L'administrateur se connecte au portail, pour ajouter l'utilisateur sur lequel les politiques de contrôle seront appliquées 2 L'utilisateur se connecte au portail, et configure les politiques de contrôle désirées, (les politiques doivent être au niveau du temps, les URLs et les applications internet comme le P2P et Streaming). 3 L'utilisateur accède une deuxième fois aux URLs et applications sur lesquelles les politiques de contrôles sont appliquées
Résultat attendu	Le blocage des URLs et applications après appliquer les politiques de contrôles
Résultat test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 15: procédure du test contrôle parentale

La fonction FUP demande beaucoup de test, elle n'est pas planifiée dans cette étape. Elle sera établit dans les phases prochaines.

1.2 La préparation des tests de fonctionnalités de la solution ICache:

1.2.1 La procédure du test:

Avant de préparer les différents tests. Il faut tracer une démarche claire et puissante pouvant assurer l'efficacité de la solution ICache. Dans ce stade une carte SIM avec une APN Test est utilisée pour les tests de fonctionnalités. Le GGCN mis en test supporte le protocole PBR pour orienter le trafic de l'APN test vers le système ICache.

L'outil **Tera Terme**, signalé par le groupe HUAWEI, doit être présent pour visualiser le processus de mise en cache du système en temps réel. Elle va permettre de voir le temps de téléchargement la taille et le statut (en cache ou pas) des ressources.

Après un test de fonctionnalité par une APN test, IAM autorise ensuite l'orientation d'une partie de son trafic internet provenant du « PS core » vers la plate forme ICache. L'objectif de ce test est de présenter des résultats concrets et chiffres précis montrant la consommation de la bande passante internet.

Les politiques de configuration devant être appliquées par la suite, il faut identifier la taille du fichier mis en cache, le seuil de hotspot, et la fonction de compression GZIP.

1.2.2 Préparation du test pour la fonction « Cache http ».

Pour la fonction « Cache http »., il est exigé un seul type de tests **(tableau 16).**

Type test	Cache des ressources HTTP
Pré-requis	1. La Mise en place de l'environnement de test en fonction de la topologie du test. 2. le réseau fonctionne normalement.
Procedure test	1. L'utilisateur se connecte par exemple à http://sourceforge.net sur l'ordinateur d'essai et enregistre la ressource HTTP. 2. Le temps de téléchargement et la vitesse doivent être vérifiés sur l'outil Tera Terme. 3. La fermeture de la fenêtre du site et l'effacement du cache local. 4. La connexion à la même page pour la deuxième fois sur le pc test. 5. Le temps de téléchargement et la vitesse doivent être vérifiés sur l'outil Tera Terme.
Résultat attendu	La vitesse de téléchargement à partir du sous-système de cache est supérieure à celle avant le cache.
Résultat test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 16: procédure du test « Cache http ».

1.2.3 Préparation du test pour la fonction « cache vidéo en ligne ».

Pour la fonction « cache vidéo en ligne ».il est exigé un seul type de tests **(tableau 17).**

Type test	Cache des vidéos en ligne
Pré-requis	1 La Mise en place de l'environnement de test en fonction de la topologie du test. 2 le réseau fonctionne normalement.
Procedure test	1 L'utilisateur se connecte par exemple à http://www.youtube.com/ sur l'ordinateur d'essai et télécharge la vidéo définie. 2 Le temps de téléchargement et la vitesse doivent être vérifiés sur l'outil Tera Terme. 3 La fermeture de la fenêtre du site et l'effacement du cache local. 4 La connexion à la même page pour la deuxième fois sur le pc test. 5 Le temps de téléchargement et la vitesse doivent être vérifiés sur l'outil Tera Terme.
Résultat attendu	La vitesse de téléchargement de la vidéo à partir du sous-système de cache est supérieure à celle avant le cache.
Résultat test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 17: procédure du test « cache vidéo en ligne ».

1.2.4 Préparation du test pour la fonction « Compression GZIP ».

Pour la fonction « Compression GZIP ».il est exigé un seul type de tests **(voir tableau 18).**

Type test	Compression GZIP et cache
Pré-requis	1 La Mise en place de l'environnement de test en fonction de la topologie du test. 2 le réseau fonctionne normalement.
Procedure test	1 L'utilisateur se connecte par exemple à www.xiaoxiangzi.com sur l'ordinateur d'essai et télécharge la ressource non compressé définie. 2 La taille de la ressource téléchargée doit être vérifiée sur l'outil Tera Terme. 3 La fermeture de la fenêtre du site et l'effacement du cache local. 4 La connexion à la même page pour la deuxième fois sur le pc test. 5 La taille doit être vérifiée sur l'outil Tera Terme.
Résultat attendu	La taille de la ressource téléchargée et compressée à partir du sous-système de cache est plus petite par rapport à celle avant le cache.
Résultat test	
Decision	☐OK ☐NOK ☐POK ☐NT

Tableau 18: procédure du test « Compression GZIP ».

2 Le processus de déploiement.

Le déploiement des solutions SIG et ICache dans le réseau local repose sur cinq phases **(figure 38)**, dont La première nommée Site Survey, consiste à une étude de l'environnement du site où les nouveaux équipements vont être installés. Après l'installation, l'étape d'intégration des solutions vient, elle porte sur la configuration de certains paramètres. Ensuite, des tests de conformité sont menés afin de vérifier le bon fonctionnement de nouvelles plates formes mises en service.

Figure 38: Phases de déploiement des solutions SIG et ICache

2.1 Le site Survey:

Le Site Survey est donc la première étape menée pour la préparation au démarrage du déploiement après la validation technique de la solution et l'implémentation de la maquette de test. Il comprend l'étude des environnements d'installation, et la détermination de l'arrangement des équipements.il permet exactement de préciser:

- La méthode de câblage.
- Le nombre et le type des équipements.
- La disponibilité ou non d'un chemin de câble.
- La longueur des fibres et des câbles d'énergies.
- La disponibilité ou non de la barre de la mise à la terre.
- La température convenable (climatisation) au fonctionnement des équipements
- La disponibilité de l'alarme et des différents types de détecteurs pour la surveillance.

2.2 L'installation:

Une fois les positions et les emplacements des équipements sont bien déterminés par le «Site Survey», la deuxième étape nommée «Installation» se déclenche. Pour mener à bien cette étape, l'établissent d'un processus d'installation clair est indispensables **(figure 39).**

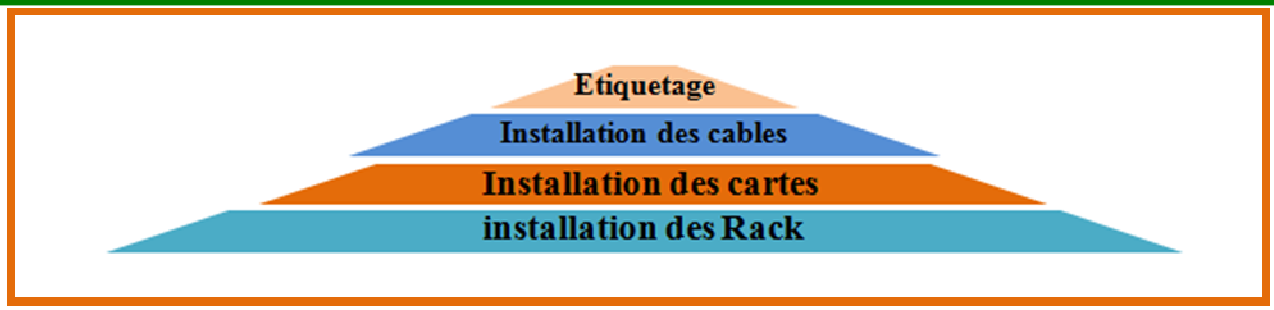


Figure 39: Processus d'installation

2.3 La configuration et l'intégration:

Dés que l'installation est terminée et que les lignes de transmission sont prêtes pour relier les différents éléments des solutions entre eux et avec les autres équipements du réseau. On passe à l'étape de l'intégration qui nécessite tout d'abord une configuration des différents équipements pour les mettre en service. Cette étape nécessite bien la préparation d'un fichier de configuration **(contenu confidentiel).**

2.4 Les tests de conformité:

Après avoir intégré les différents équipements d'un site, il faut vérifier leur fonctionnement, cette phase nommée test de conformité, elle permet de localiser les anomalies et les disfonctionnements.

3 Les tests de fonctionnalités et résultats:

Les tests de fonctionnalités et leurs résultats constituent une phase décisive assurant l'adoption des solutions SIG et ICache. De ce fait je me suis chargée durant cette phase (avec l'équipe HUAWEI) d'établir soigneusement les différents scénarios de tests élaborés ci-dessus. Le suivis de ces tests fonctionnels permettra d'assurer la puissance de ces solutions ou non.

3.1 Les tests de fonctionnalités de la solution SIG et résultats:

3.1.1 Tests:

En respectant le scénario de test élaboré dans la partie préparation des tests. Les tests de la fonction rapports et statistiques sont établis (figures 40, 41, 42):

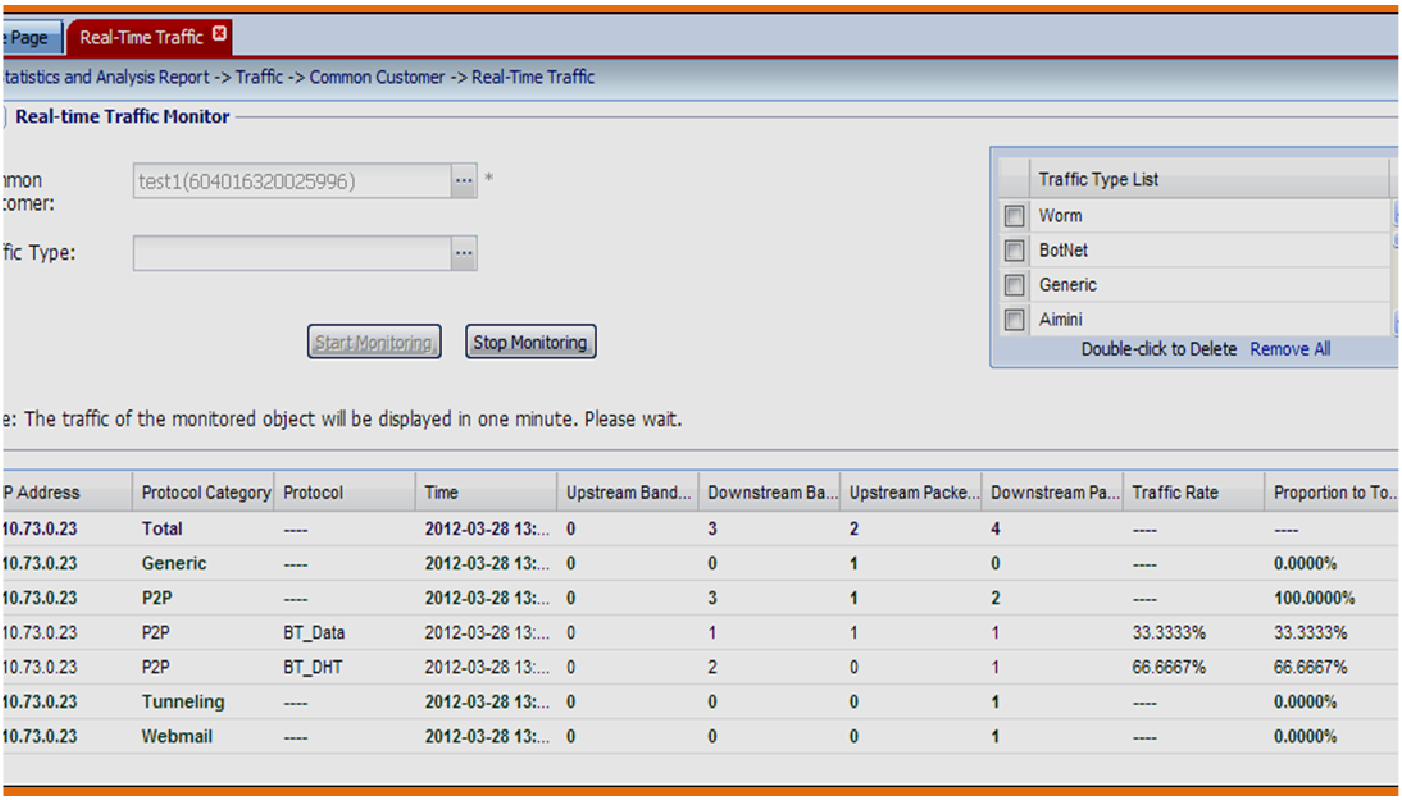


Figure 40: Test identification du trafic réel

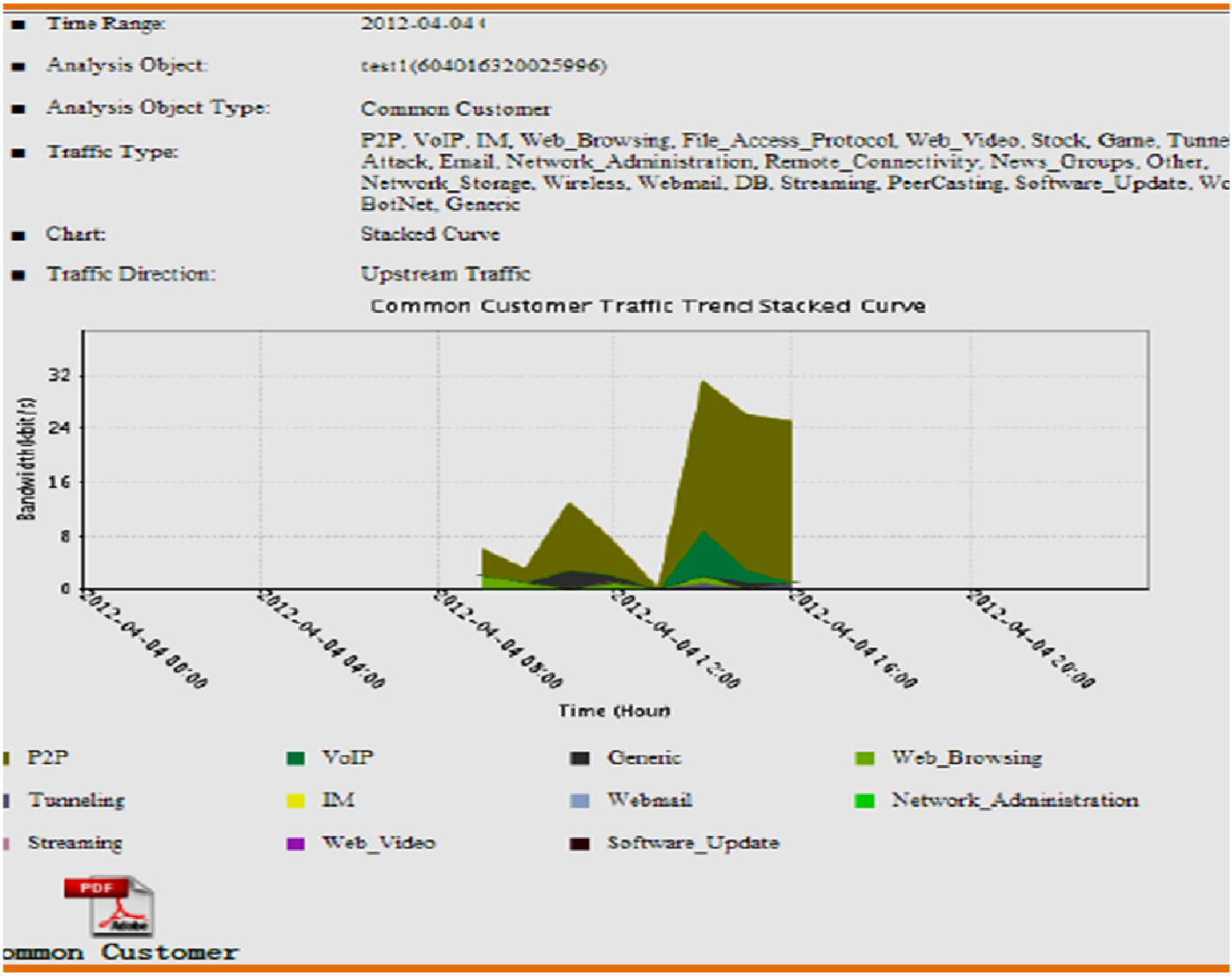


Figure 41: Test rapport sur la tendance du trafic des abonnés

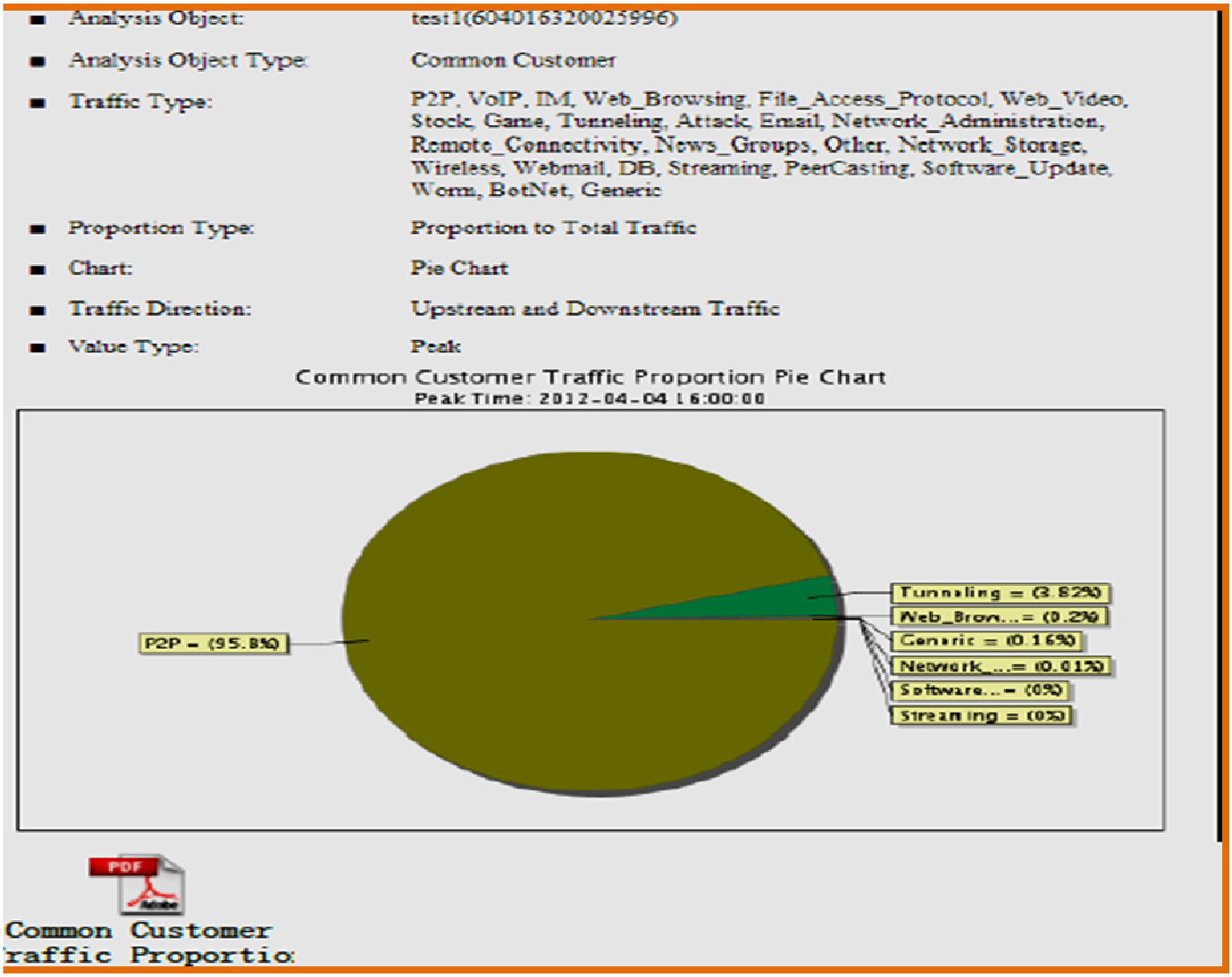


Figure 42: Test rapport sur la tendance du trafic d'un seul abonné

En respectant le scénario de test élaboré dans la partie préparation des tests, les tests de la fonction contrôle de la VOIP sont établis **(figures 43-61).**

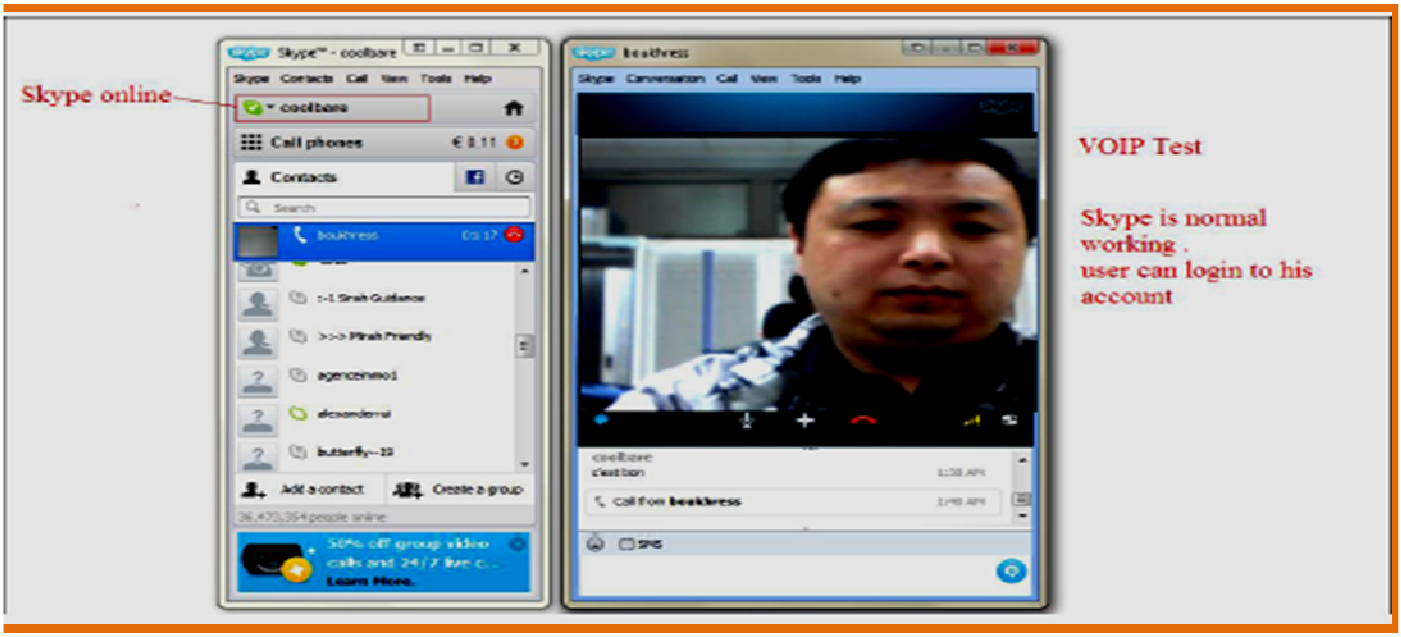


Figure 43: Test contrôle du SKYPE (fonctionnement normal)

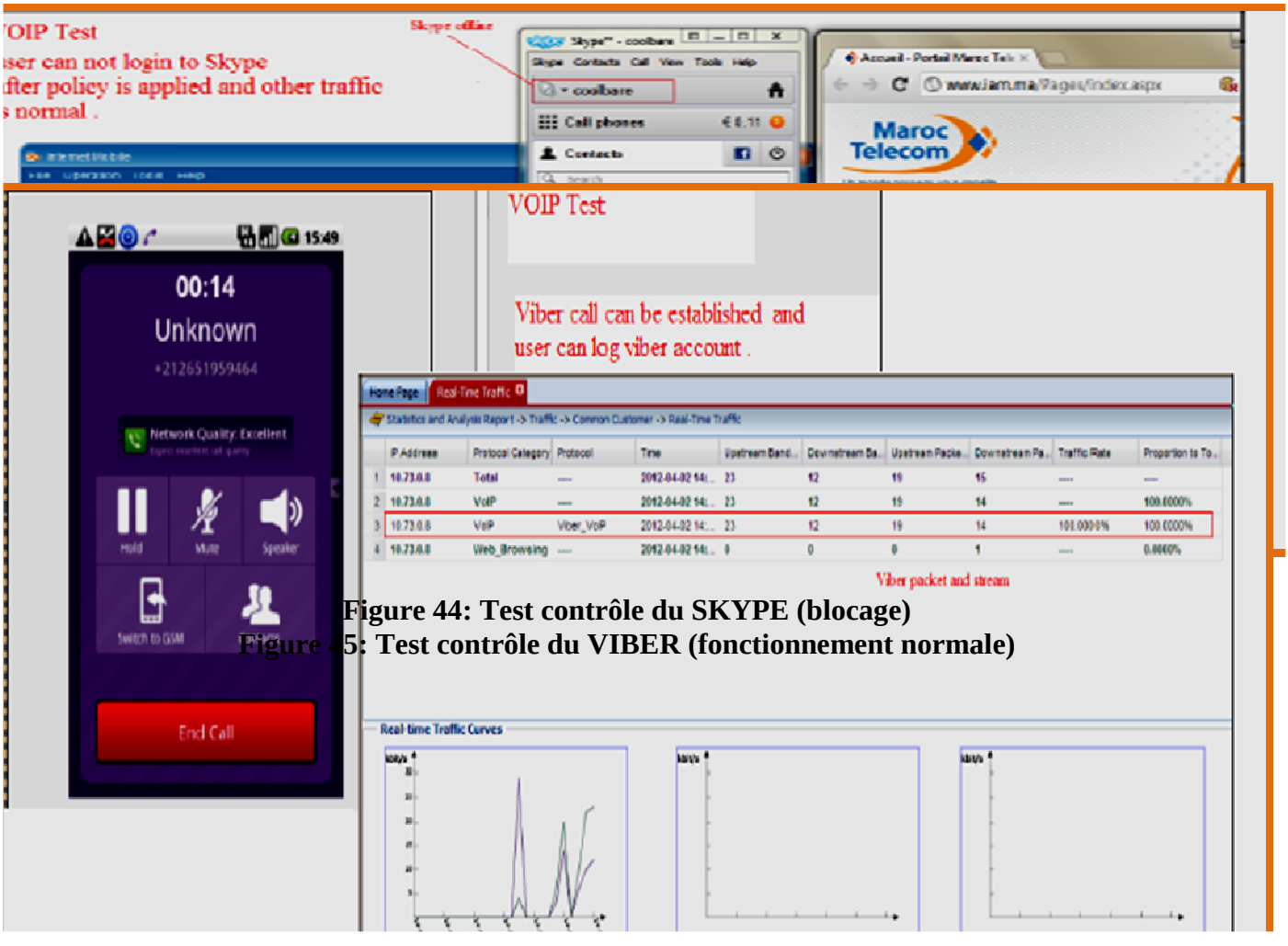


Figure 44: Test contrôle du SKYPE (blocage)

Figure 45: Test contrôle du VIBER (fonctionnement normale)

Figure 46: Test contrôle du VIBER (blocage)

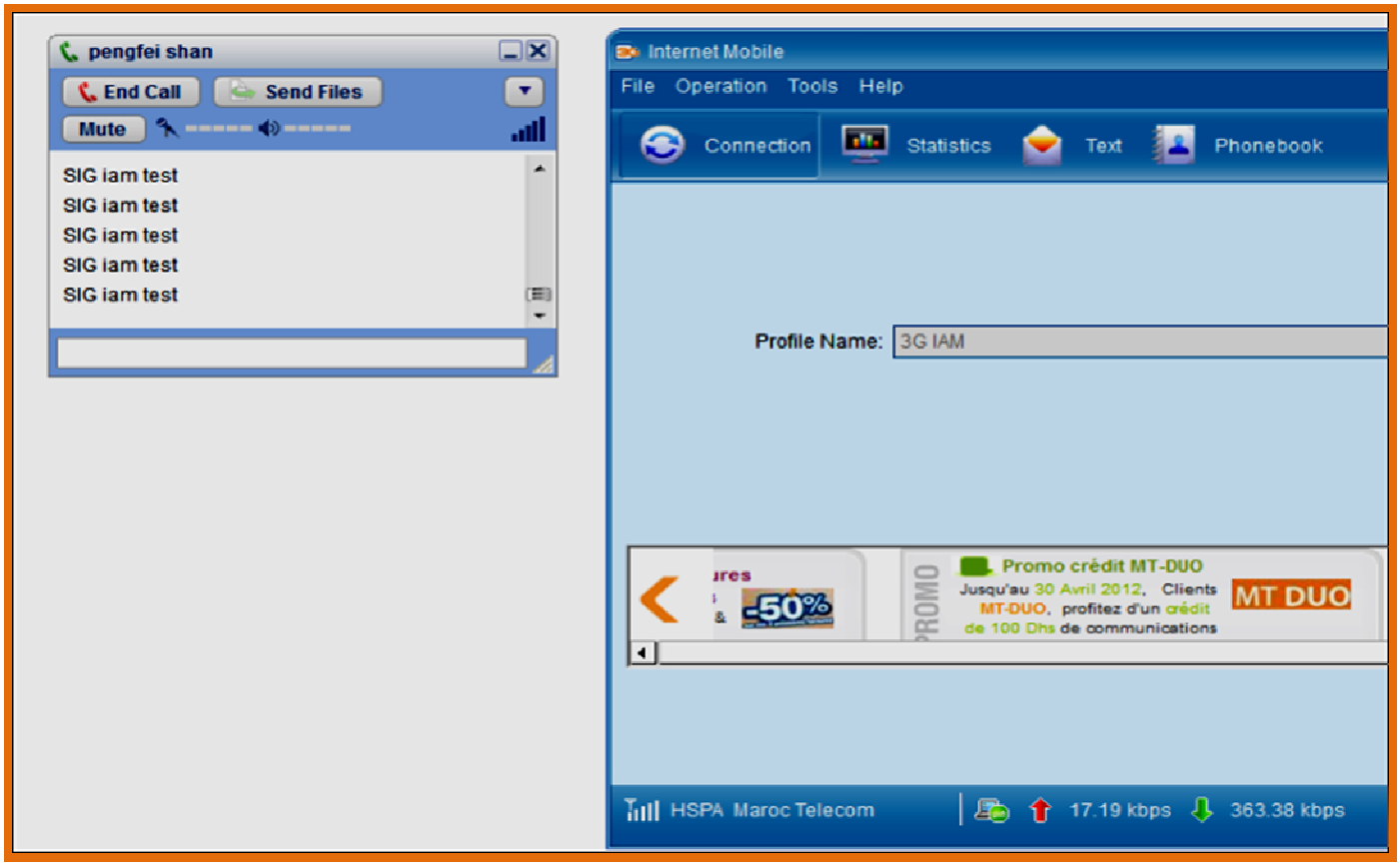


Figure 48:Test contrôle de GOOGLE TALK (fonctionnement normal)

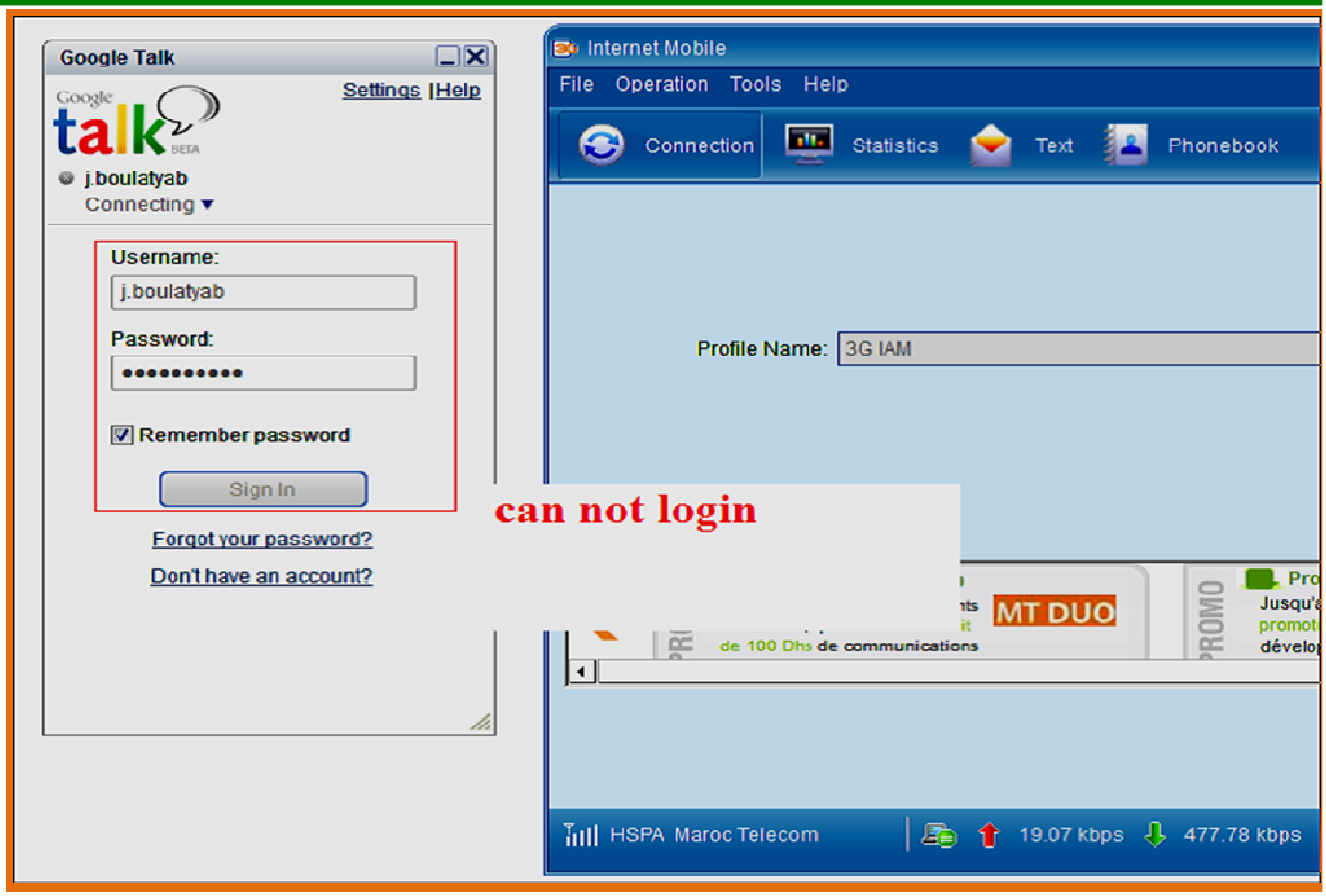


Figure 49: Test contrôle de GOOGLE TALK (blocage)

Figure 50:Test contrôle de TONGO (fonctionnement normal)

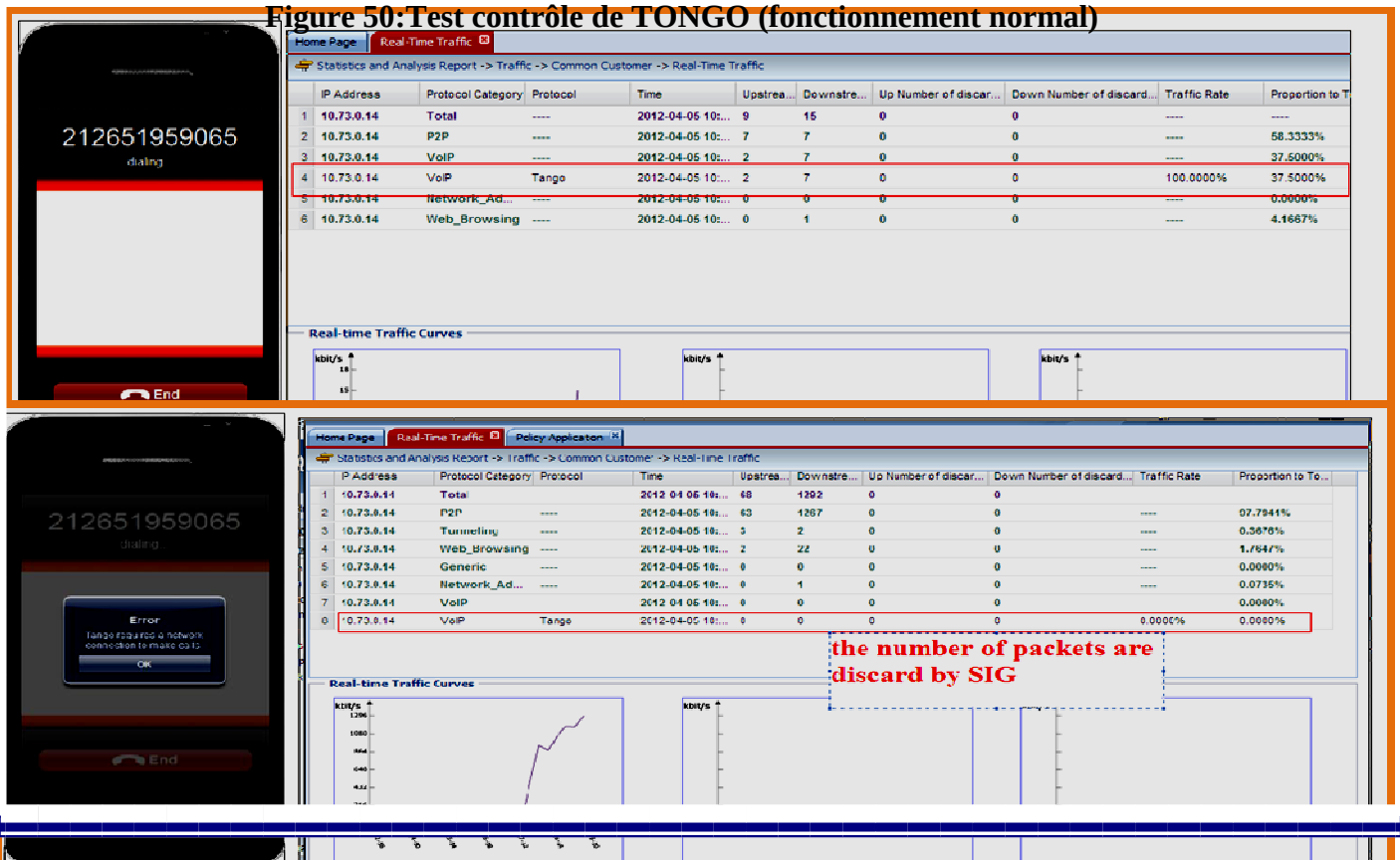


Figure 51:Test contrôle de TONGO (blocage)

Figure 52:Test contrôle de NIMBUZZ (fonctionnement normal)

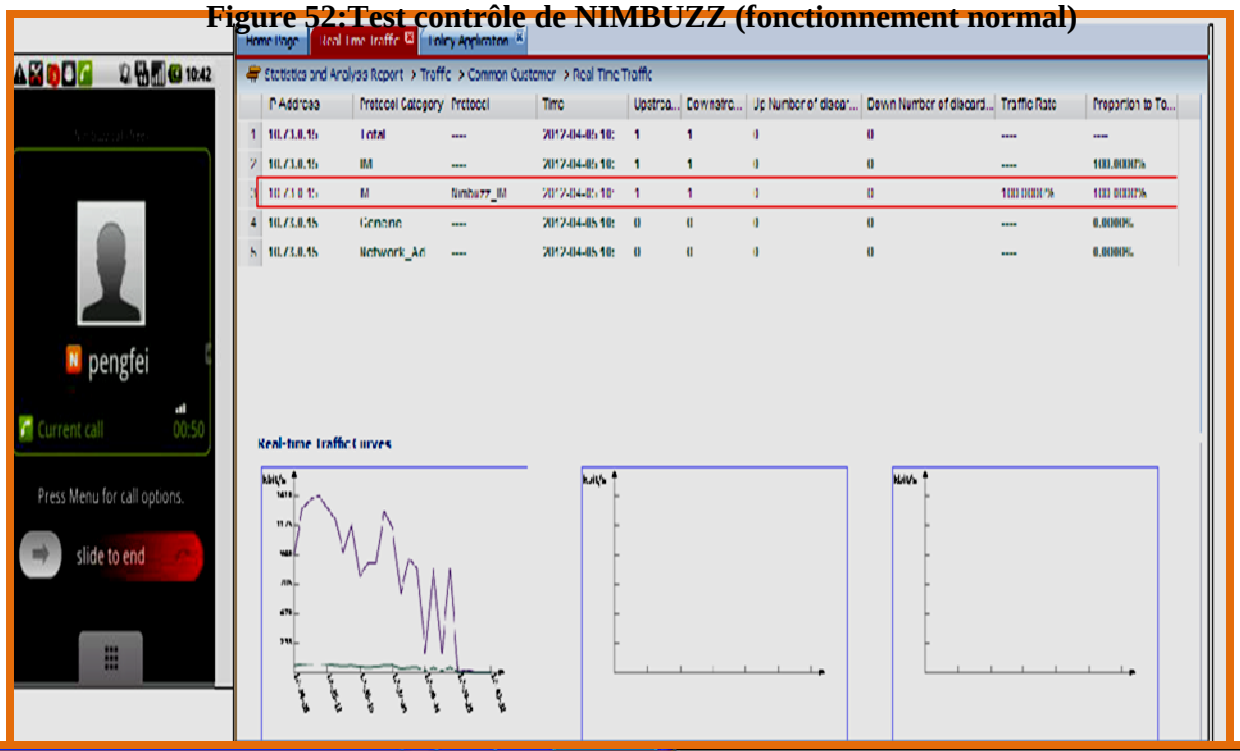
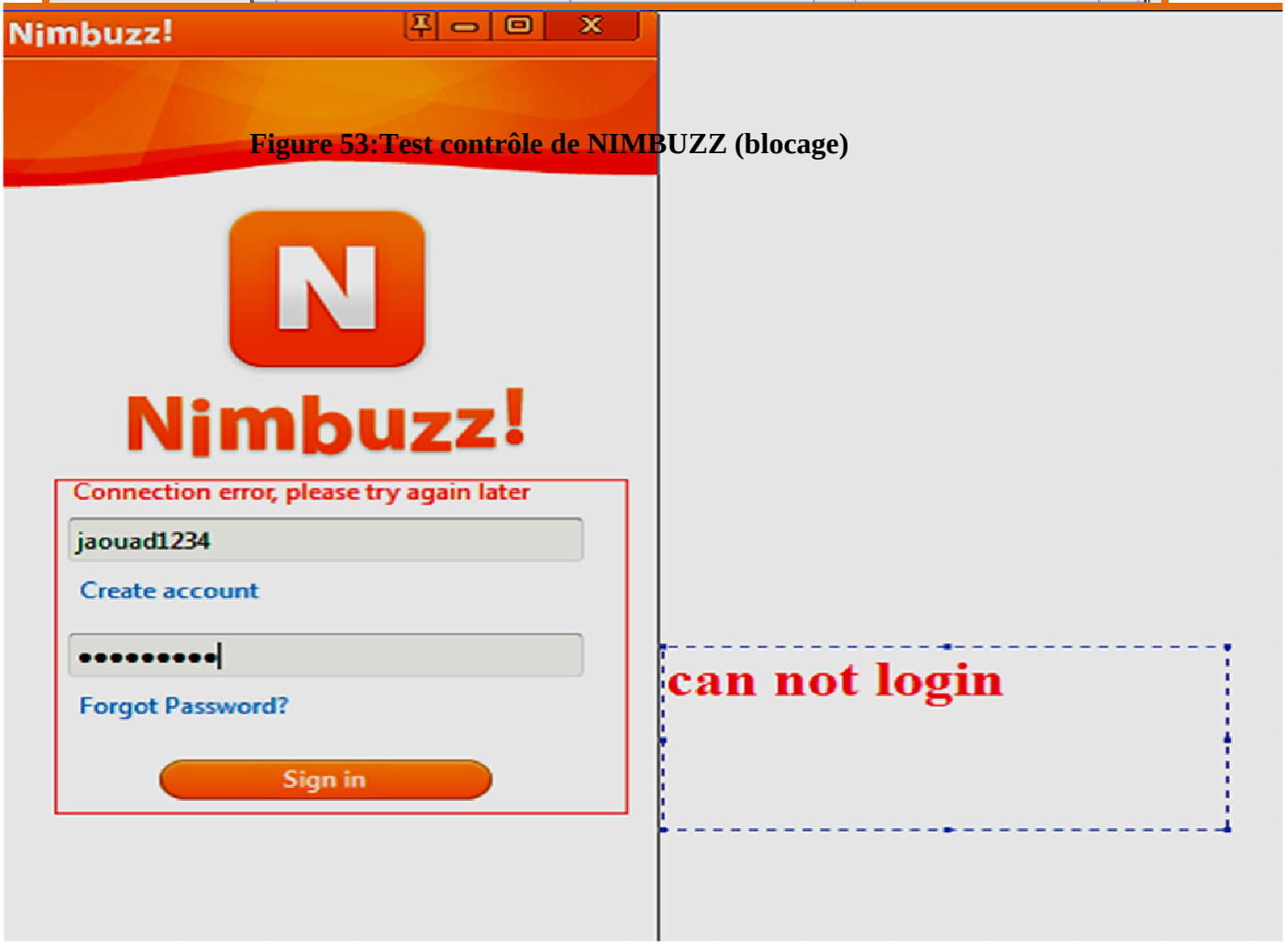


Figure 53:Test contrôle de NIMBUZZ (blocage)



En respectant le scénario de test élaboré dans la partie préparation des tests, le test de la fonction contrôle parental est établi **(figures 54, 55, 56)**

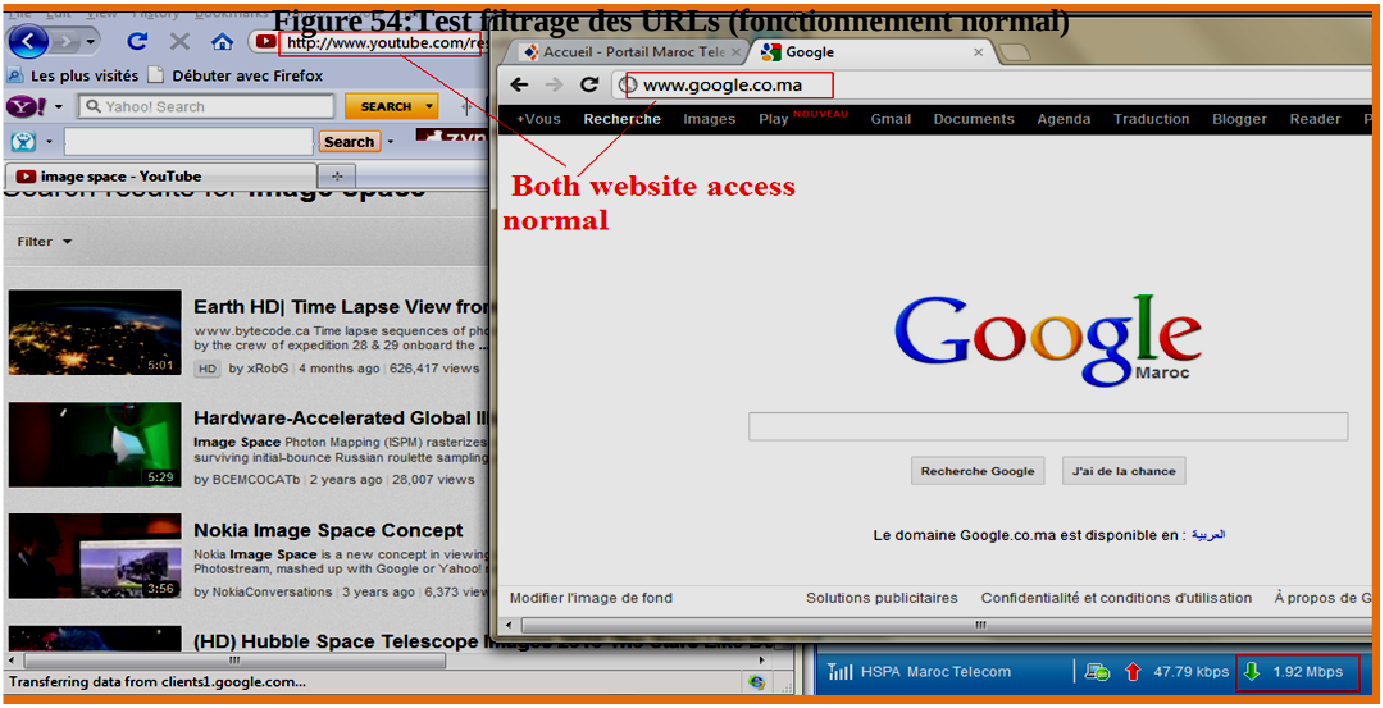


Figure 54:Test filtrage des URLs (fonctionnement normal)

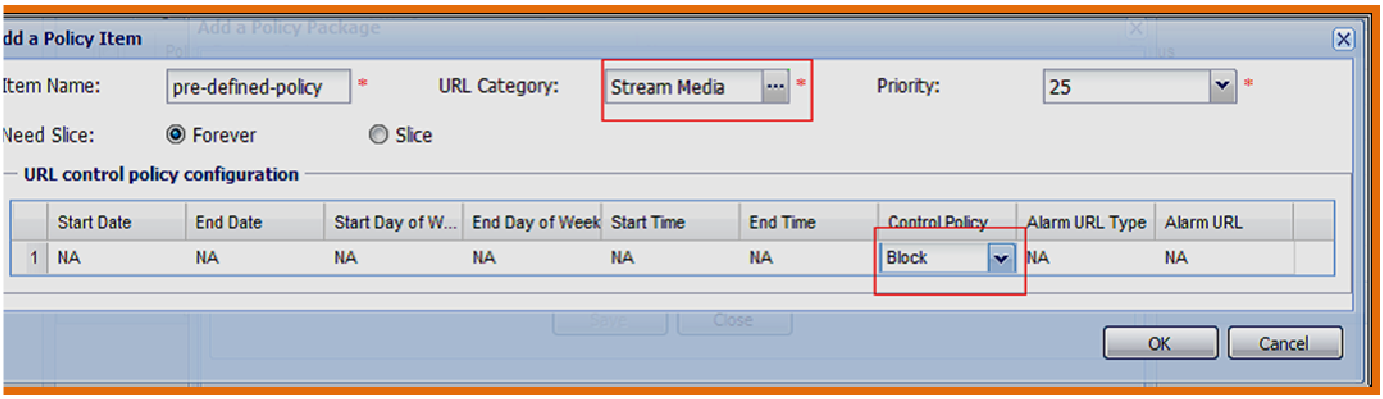


Figure 55:Configuration de la politique de blocage

Figure 56: test filtrage des URLs (blocage)

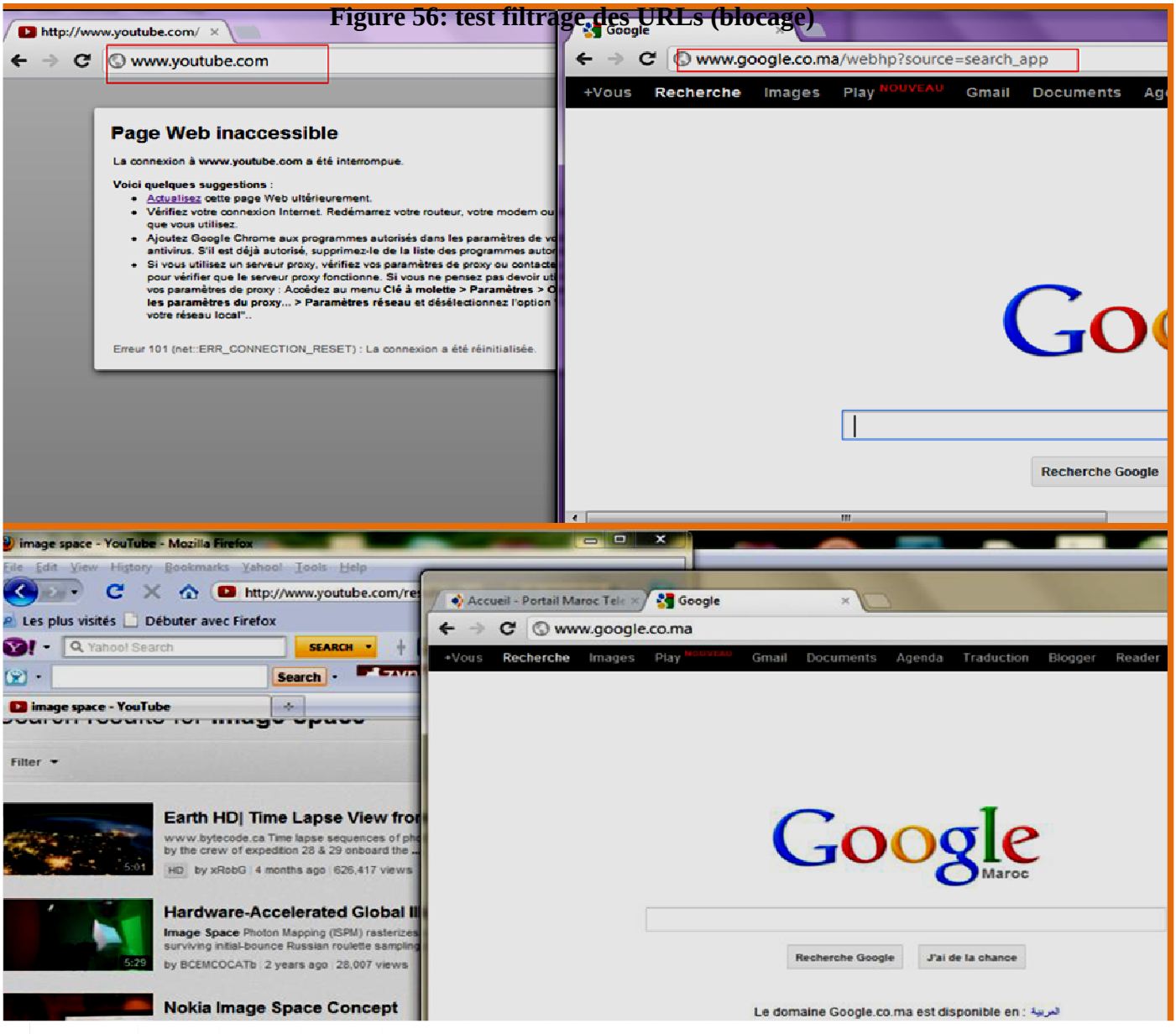


Figure 57:Test filtrage des URLs (fonctionnement normal)

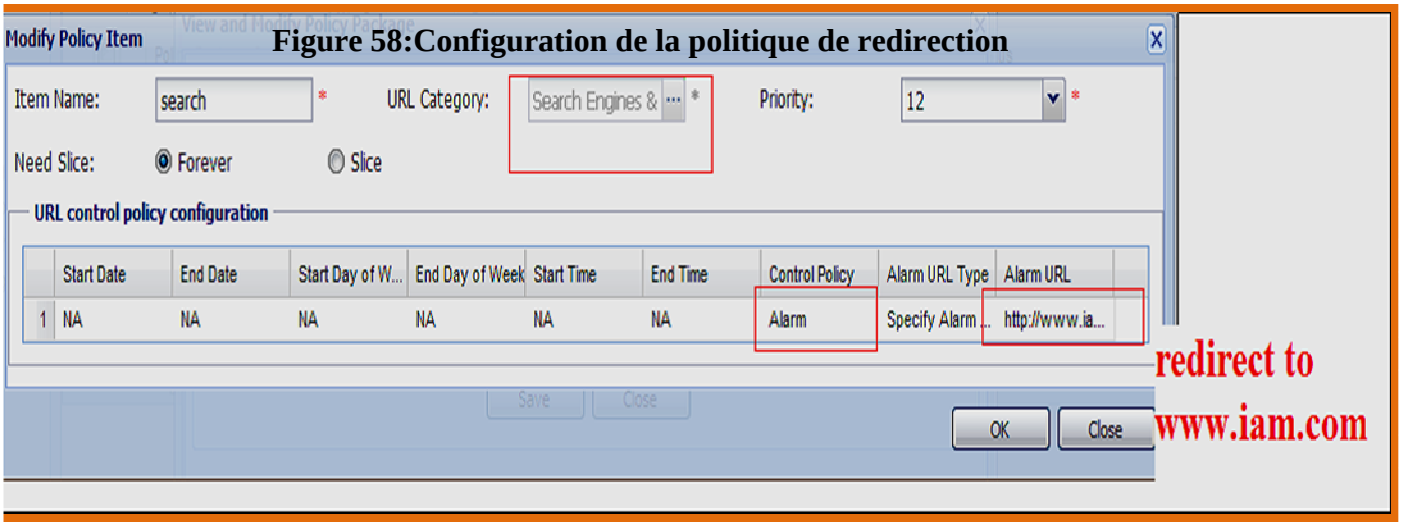


Figure 58:Configuration de la politique de redirection

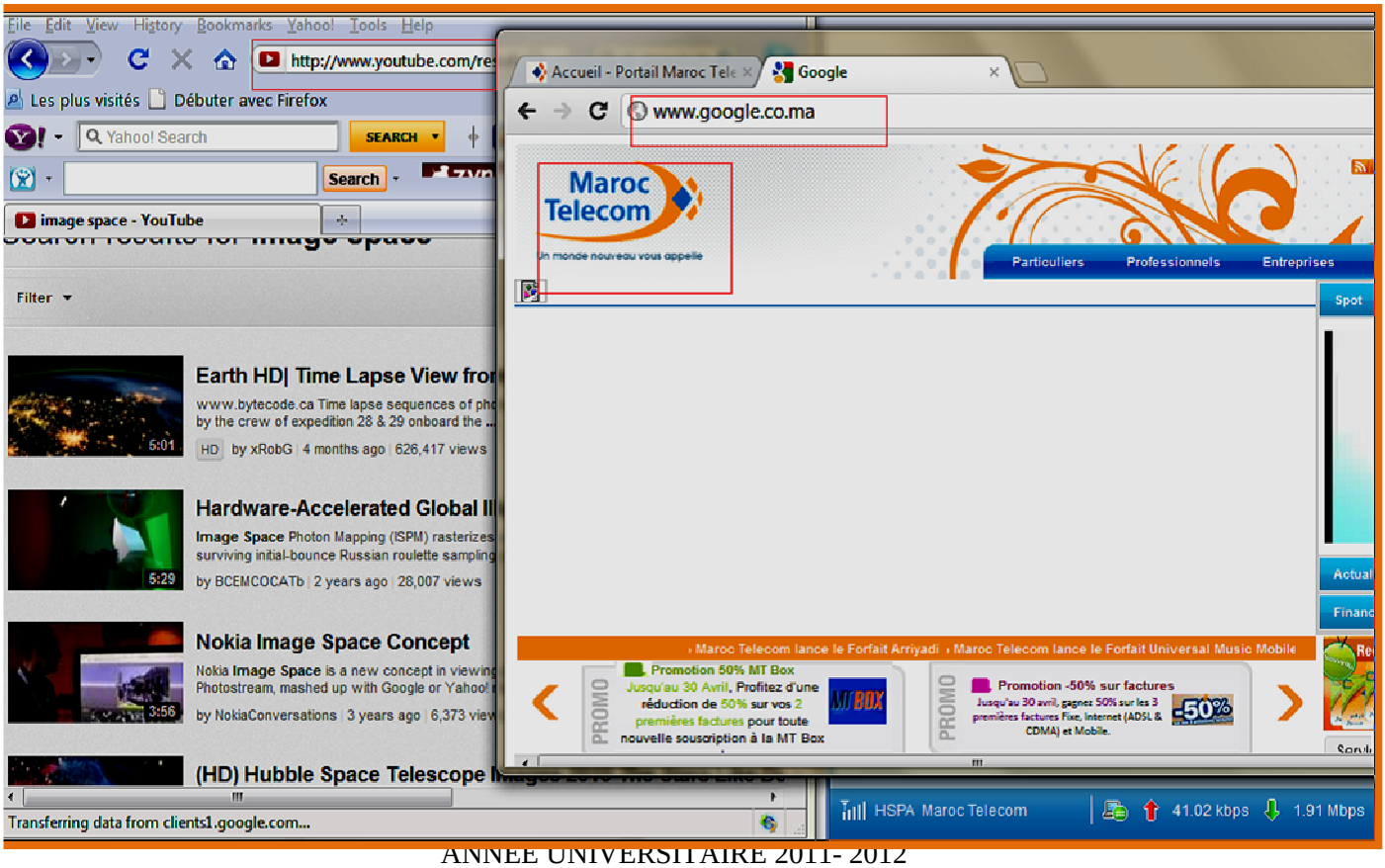


Figure 59:Test filtrage des URLs (redirection vers le portail IAM)

En respectant le scénario du test élaboré, les tests de la fonction contrôle parental sont établis (figures 60, 61, 62)

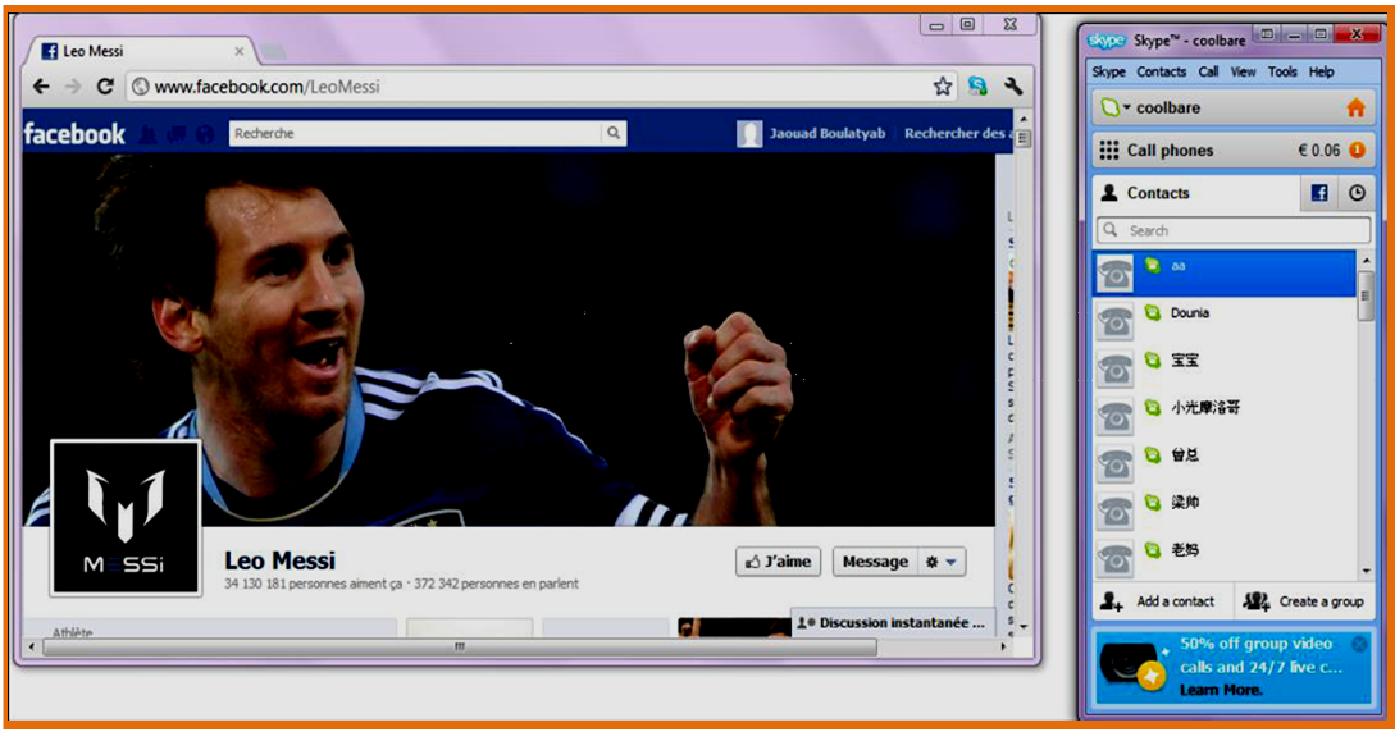


Figure 60: Test Contrôle parental (fonctionnement normal)

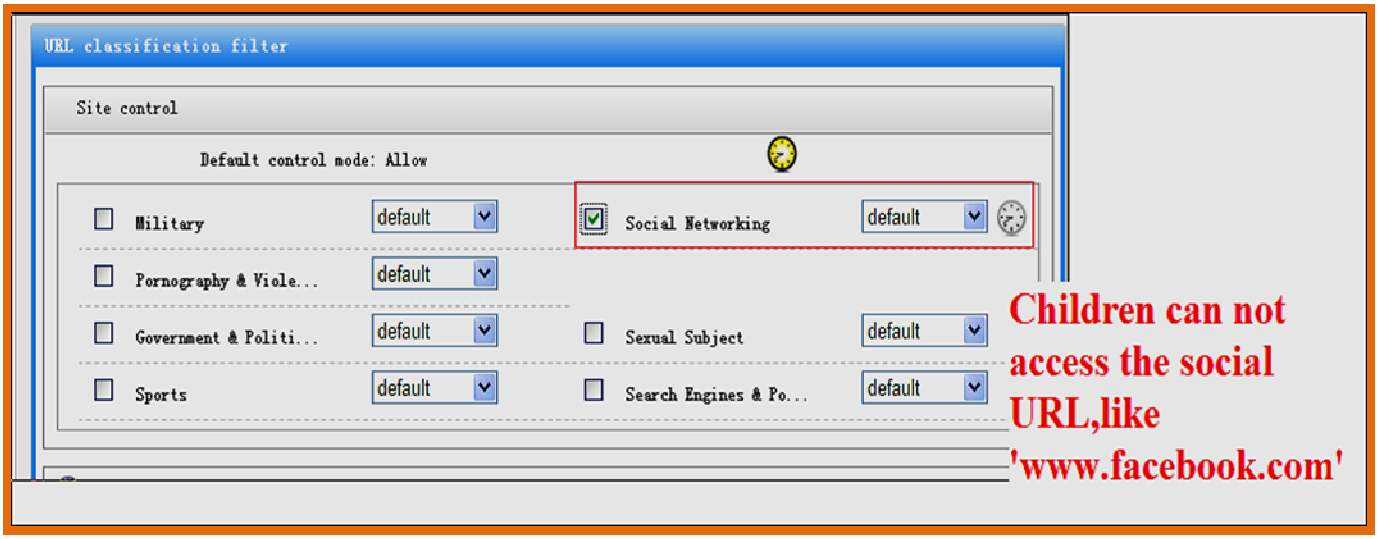


Figure 61: Configuration de la politique contrôle parental

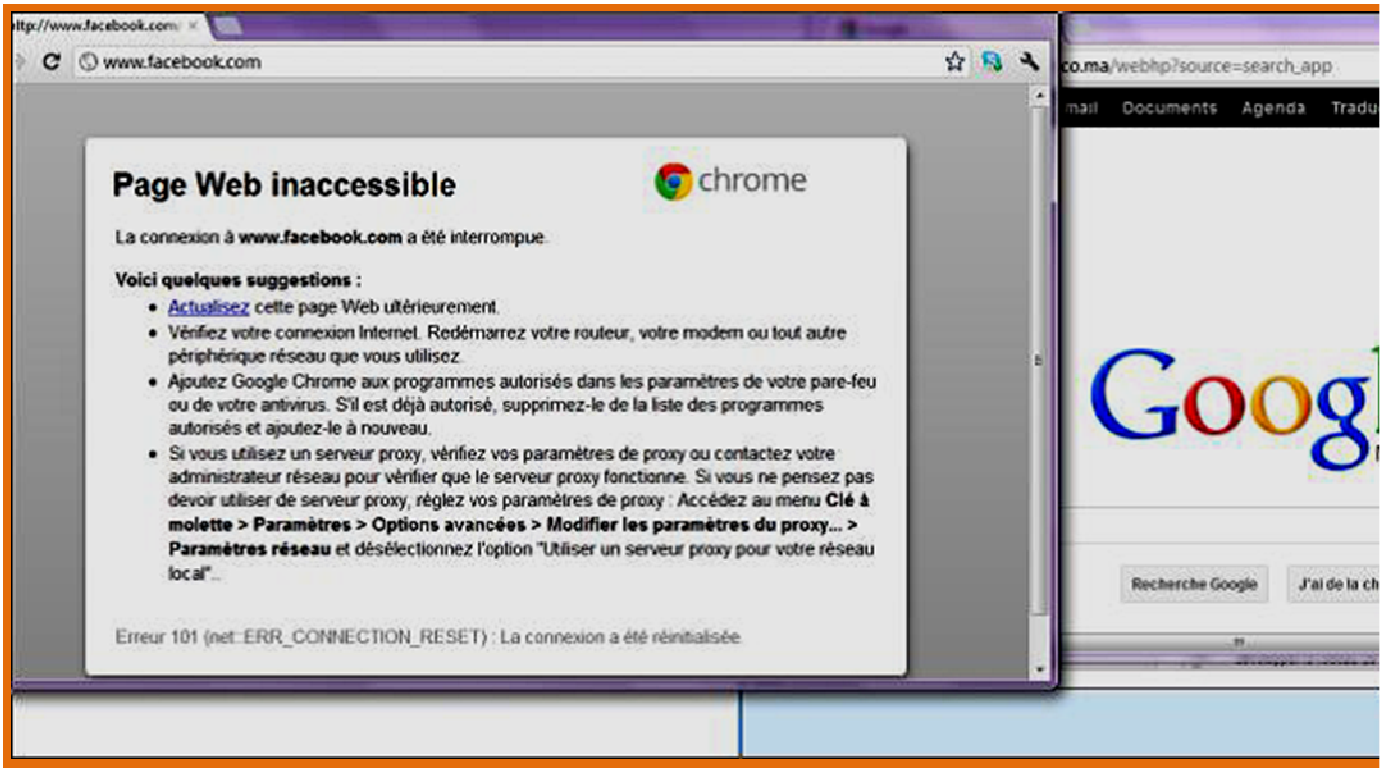


Figure 62: Test control parental

3.1.2 résultat de tests:

Les tests de fonctionnalités de la solution SIG ont donnés des résultats souhaités, pourtant le test de la fonction gestion de la VOIP n'est pas validé puisque le contrôle des applications SKYPE VIBER effectué consiste sur le blocage de la voix et les données écrites (chat) et la vidéo, et cela ne présente pas l'exigence actuelle de l'opérateur Maroc Télécom. Le besoin actuel porte sur le blocage de la voix ip seulement qui nécessite beaucoup de ressources en termes de bandes passantes. Selon HUAWEI, ce point n'est pas un défaut bloquant, il est en cours de développement.

3.2 Les tests de fonctionnalités pour la solution ICache et résultat:

3.2.1 Tests:

En respectant le scénario du test élaboré, les tests de la fonction cache http sont établis voir figure (64-66)

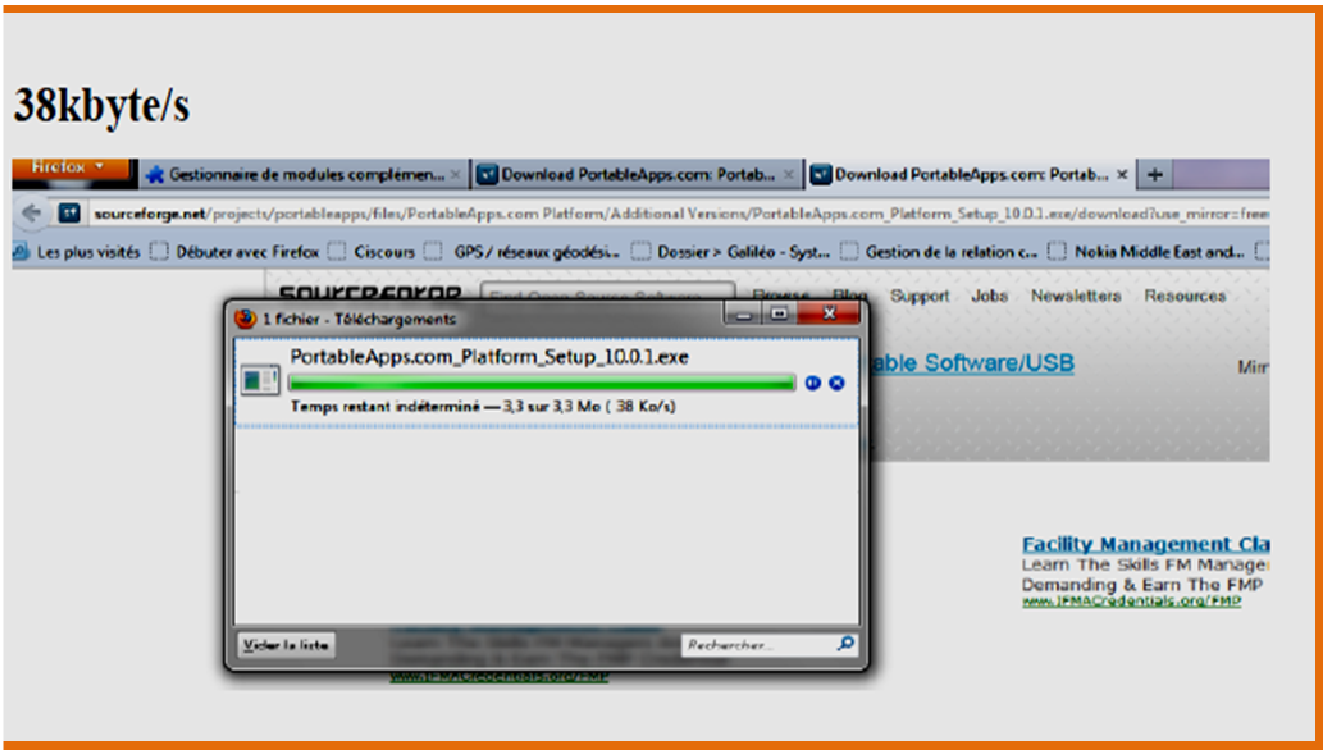


Figure 63: Test 1« cache http » (phase téléchargement de la ressource http software avant le cache: vitesse de téléchargement est de 38kbyte/s)

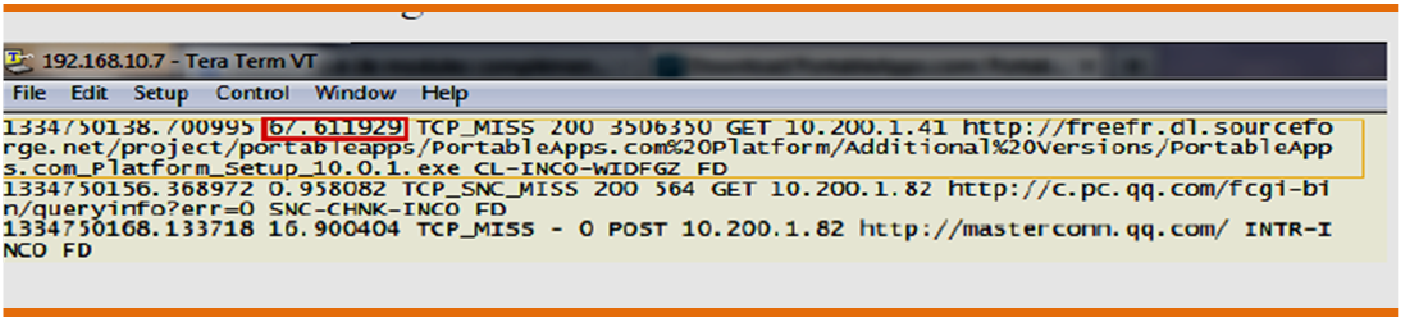


Figure 64: Test 2 « cache http » ((phase téléchargement de la ressource http software avec avant le cache: temps de téléchargement est de 67.61s)
)

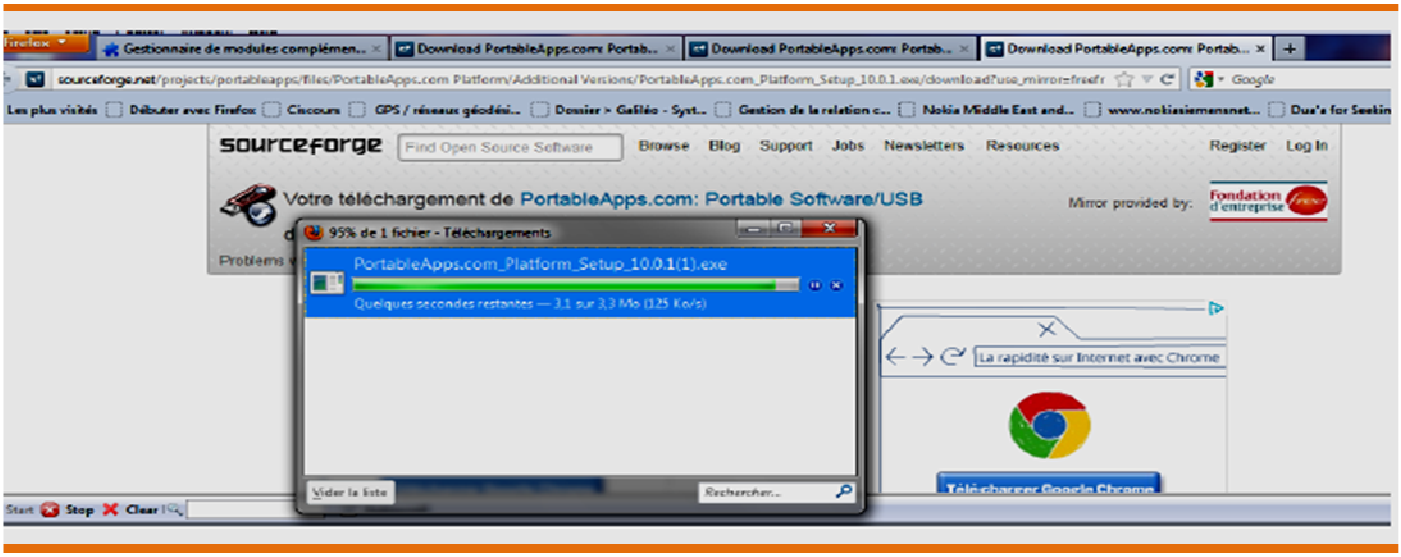


Figure 65: Test 3 « cache http » (phase téléchargement de la ressource http software après le cache: vitesse de téléchargement est de 125kbyte/s)

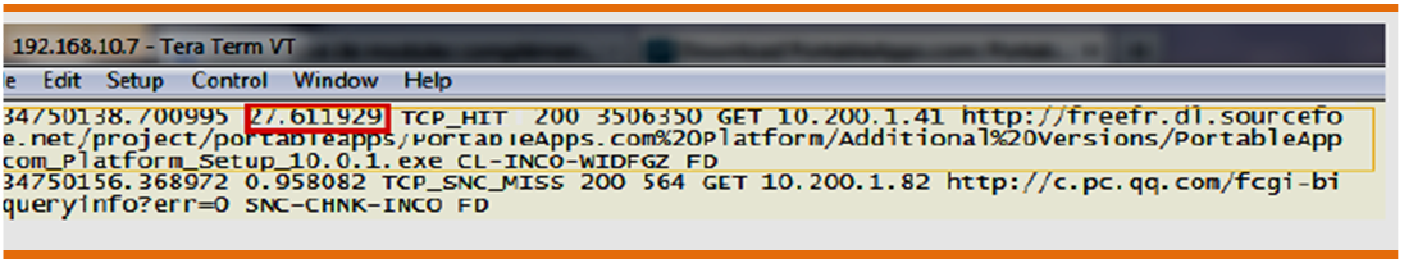


Figure 66: Test 4 « cache http » (phase téléchargement de la ressource http software après le cache: temps de téléchargement est de 27.61s)

En respectant la procédure du test élaboré, les tests de la fonction cache vidéo en ligne sont établis (figures 67, 68).

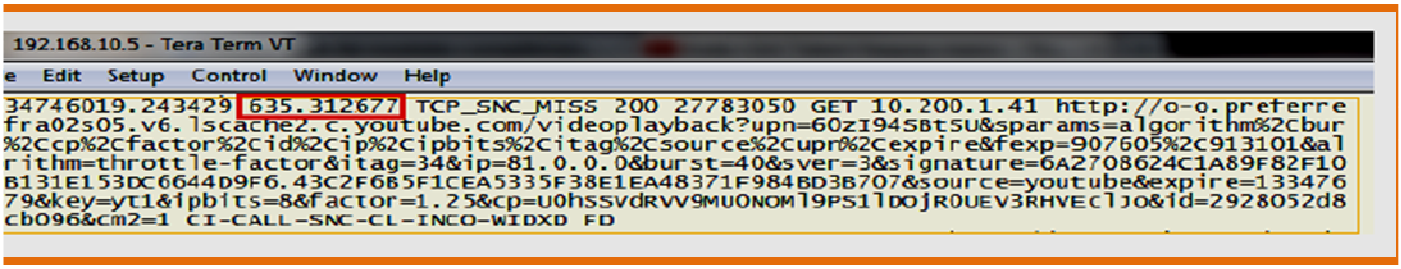


Figure 67: Test « cache vidéo en ligne » (phase téléchargement de la ressource vidéo en ligne avant le cache: temps de téléchargement est de 635.31s)

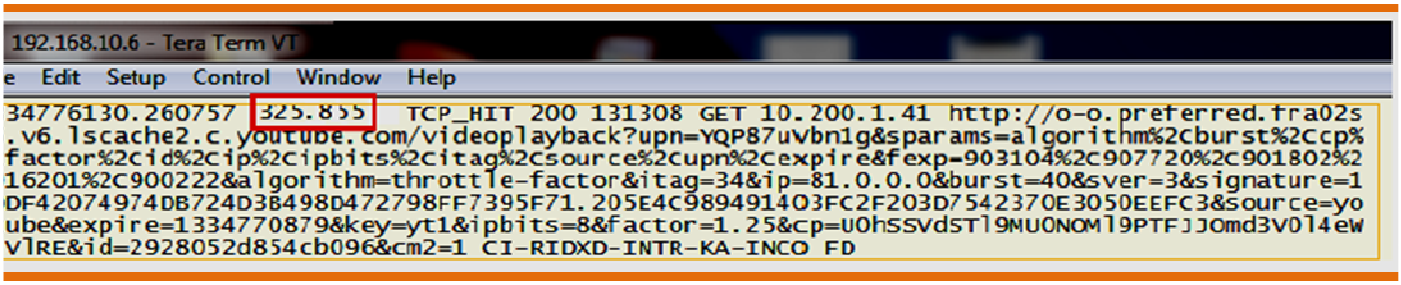


Figure 68: Test « cache vidéo en ligne » (phase téléchargement de la ressource vidéo en ligne après le cache: temps de téléchargement est de 325.85s)

En respectant la procédure du test élaboré, les tests de la fonction compression HTTP sont établis (figures 69, 70, 71, 72,).

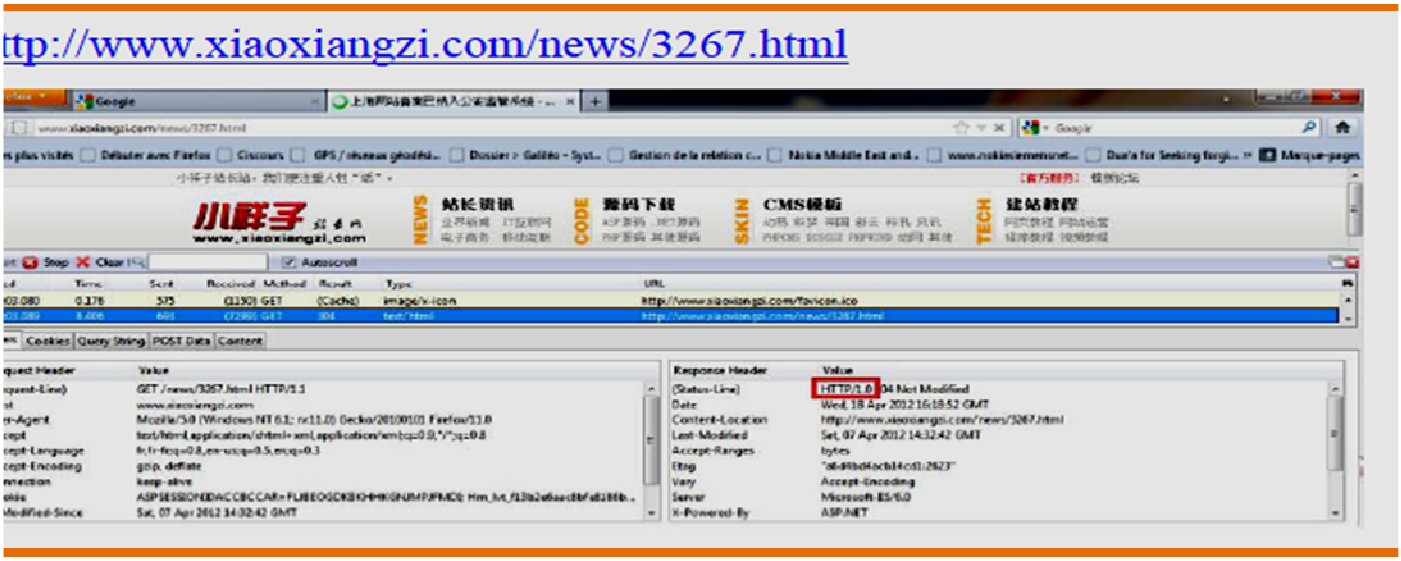


Figure 69: Test « Compression GZIP » (phase téléchargement de la ressource internet avant le cache: ressource est en HTTP / 1,0 ce qui signifie qu'elle n'est pas compressée GZIP)

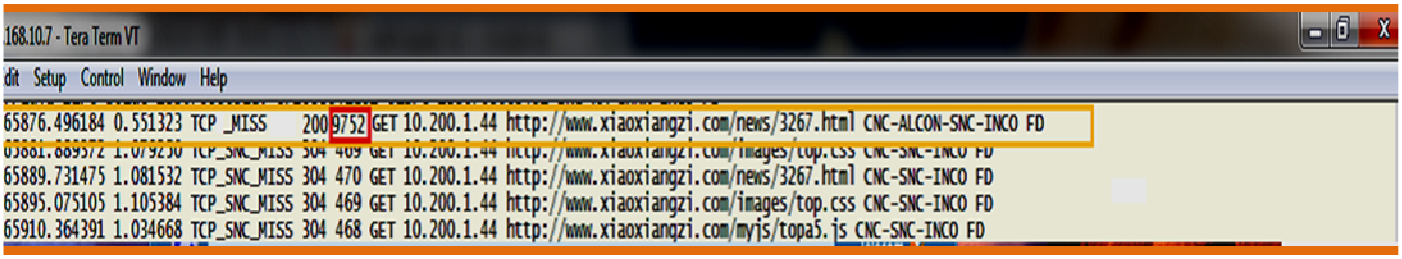
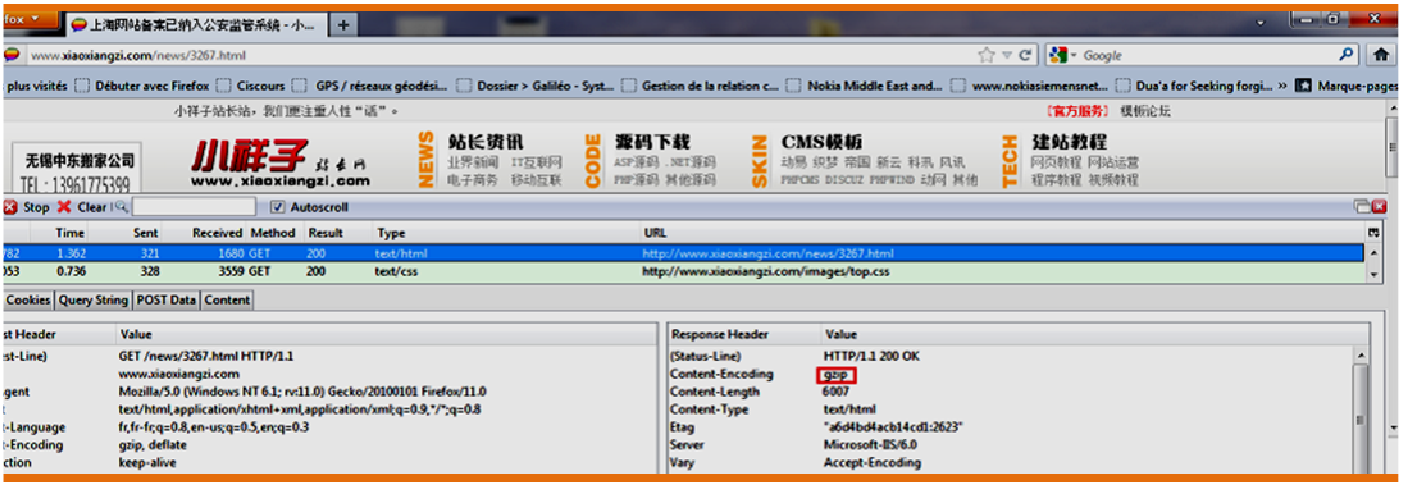


Figure 70: Test « Compression GZIP » (phase téléchargement de la ressource internet



avant le cache: taille de la ressource est de 9.7 kbit

Figure 71: Test « Compression GZIP » (phase téléchargement de la ressource internet après le cache: ressource est compressée GZIP)

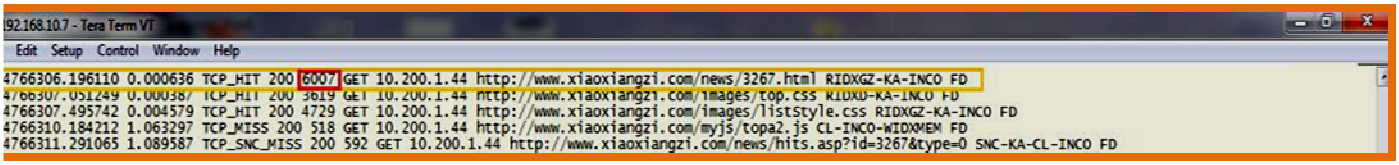


Figure 72: Test « Compression GZIP » (phase téléchargement de la ressource internet après le cache: taille de la ressource est de 6,1 kbit)

- **Test « Bandwidth Saving »:**

La bande passante moyenne économisée par ICACHE est 912.3Mbps (voir tableau 19 et figure 73), donc le pourcentage de la bande passante réduit est 912.3Mbps/2.5Gbps = 38%.

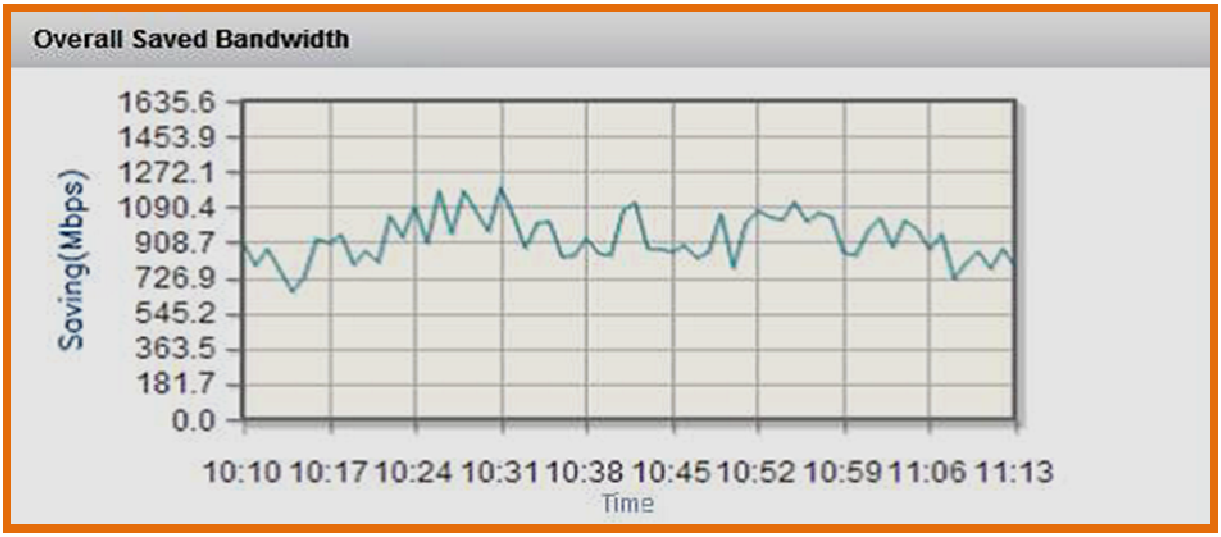


Figure 73:Test « Bandwidth Saving »(Rapport généré par le système MSS durant une heure)

Système ICache	trafic-Out	**Trafic-In**	**Bande passante consommée**
maximum	817.9 Mbps	156.7 Mbps	661.2 Mbps
minimum	1.363 Gbps	196.7 Mbps	1.16 Gbps
moyenne	1.094 Gbps	181.7 Mbps	**912.3 Mbps**

Tableau 19: statistique sur le trafic in et out du système ICache

- **Test « Average response time »**

Pour ce test, un programme Webtimer est lancé, il prend en charge une liste d'URL comme une entrée. Ce programme permet un accès simultané à un groupe de sites, il permet le calcul du temps de réponse pour chaque accès à un site, il permet aussi le calcul du temps de réponse moyen d'accès à tous les sites.
Certains sites sont en « DOWN » et d'autres sont en « SLOW ». Le temps de réponse moyen d'accès avant le cache est de 21.68s (figure 74). Le temps de réponse moyen d'accès après le cache est de 9,37s (figure 75).

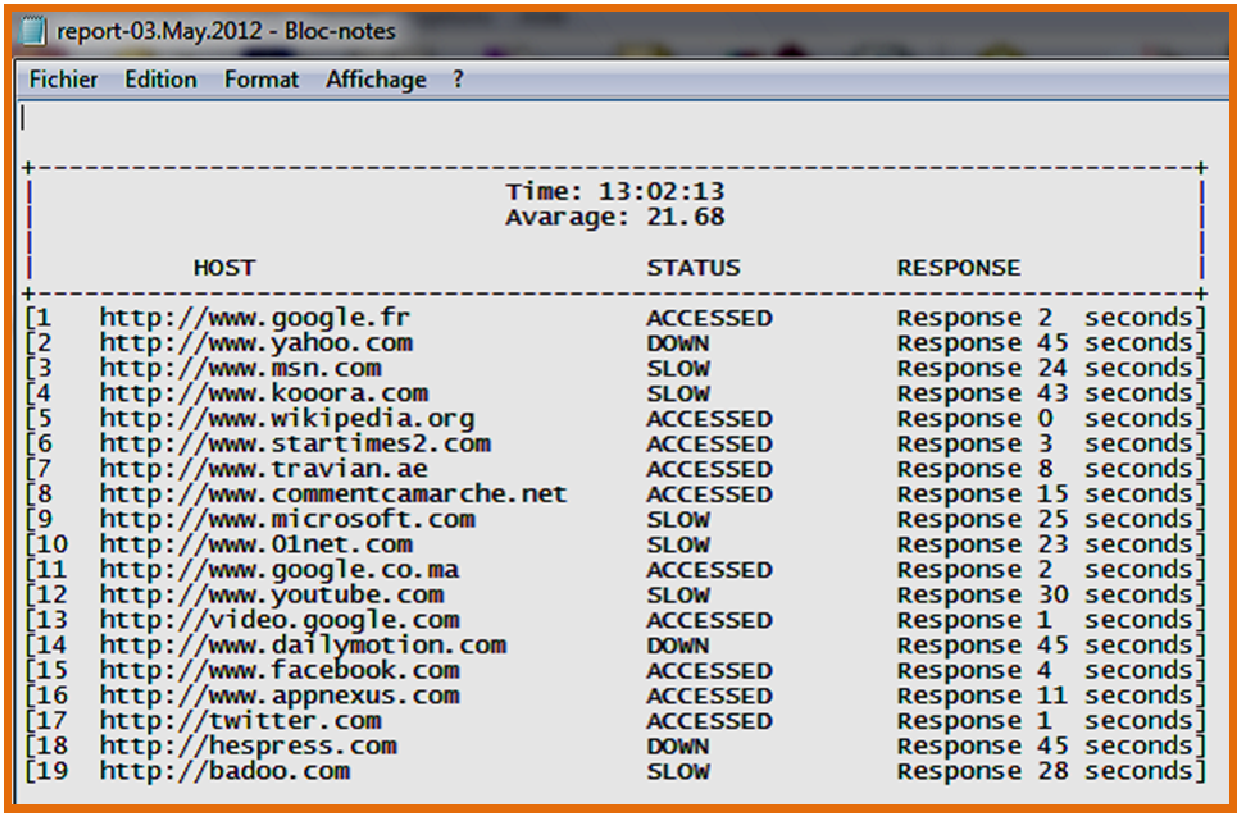


Figure 74: test rapports avant la cache

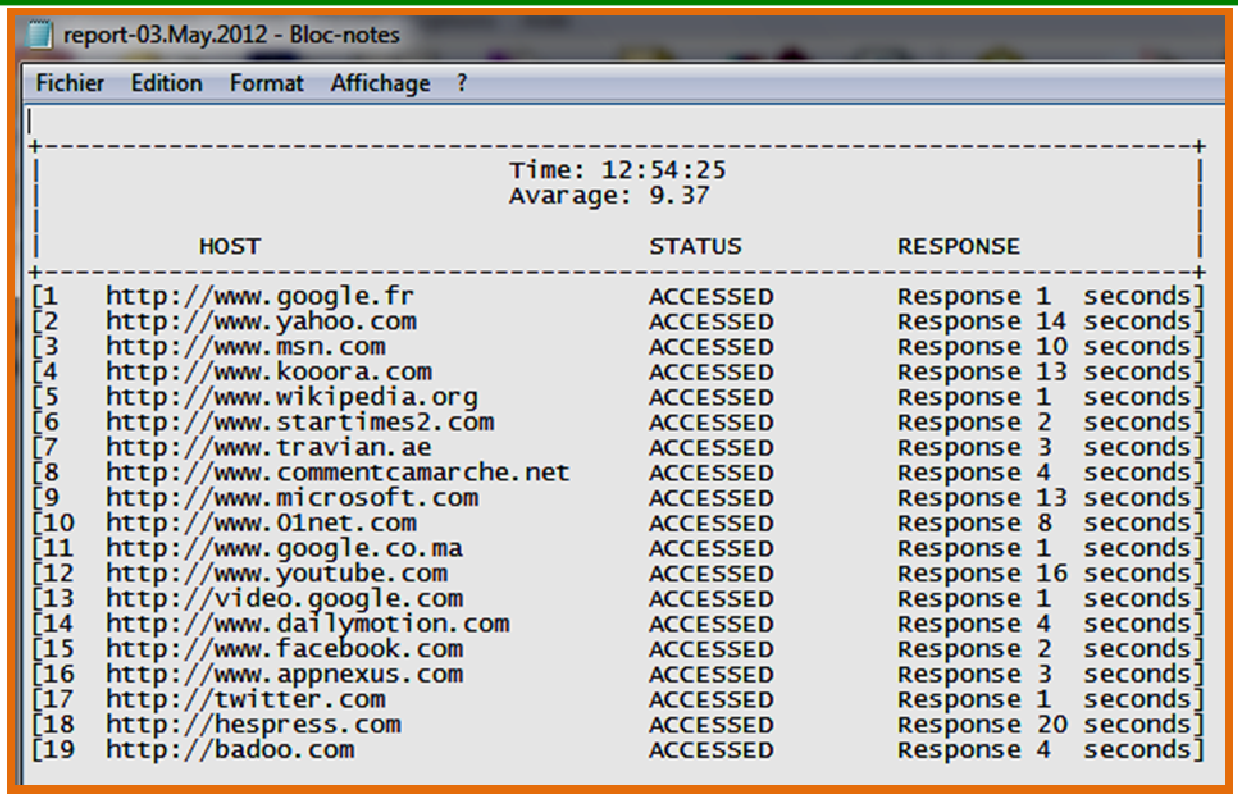


Figure 75: rapports après le cache

Tous les sites ont été consultés à succès et le temps de réponse moyen a été grandement amélioré. Le résultat de cache est mieux que le premier test sans cache.

3.2.2 résultat de tests:

Les procédures de tests de fonctionnalités de la solution ICache sont respectées, les résultats de tests pour les fonctions Cache HTTP, Cache vidéo en ligne et compression GZIP sont acceptables, le temps de réponses, la taille et la vitesse de téléchargement ont été grandement améliorés après le cache.

La fonction GZIP est puissante, elle assure la qualité du service. Pourtant cette fonction n'est appliquée que sur les contenus mis en cache. Cela présente un inconvénient pour IAM, la compression GZIP doit être appliquée sur tous les contenus HTTP et vidéo en ligne.

Les résultats de tests « Bandwidth Saving » et « Average response time » sont acceptables aussi, mais n'assurent pas une efficacité de la solution, dans les phases suivantes, des procédures flexibles de tests de performances seront appliquées. Dans ce cas le test sera basé sur tout le trafic mobile et les statistiques seront prises suivant un planning de temps.

. Conclusion:

Le déploiement des solutions SIG et ICache localement et les tests de fonctionnalités représentent deux phases décisives permettant de s'assurer de la faisabilité des solutions avant leur implémentation sur un réseau mobile à grande échelle.

A ce stade, la pilote SIG présente une solution flexible permettant via ses différentes fonctionnalités validées ci-dessus un control et une gestion intelligente du trafic 3G en adoptant les politiques de gestion convenables.

La solution ICache présente aussi une solution puissante, assurant une qualité de services et une réduction des ressources utilisées. Pourtant la préparation de nouvelles procédures de tests de fonctionnalités et de performances est indispensable.

Conclusion générale

Avec l'évolution, rapide des réseaux télécoms mobiles, les opérateurs se voient confrontés à de nombreux défis, le trafic HTTP, VOIP et P2P croit plus rapidement que l'extension de la bande passante. Ainsi, l'opérateur doit investir de plus en plus afin de s'adapter à l'évolution rapide du trafic.
Les pilotes SIG et ICACHE produits de HUAWEI Technologies déployés localement et gratuitement au niveau de MAROC TELECOM, présentent des solutions idéales permettant une optimisation intelligente des ressources actuelles.
En effet, le pilote ICache assure un stockage et une délivrance directe des ressources internet demandées par l'utilisateur final, Il permet ainsi de réduire les coûts de la bande passante en garantissant une amélioration de la qualité du service. Alors que le pilote SIG, assure un contrôle, une gestion et un blocage dans certains temps du trafic au niveau du GGSN du réseau mobile, il permet alors une consommation de la bande passante utilisée.
S'assurer de la performance de ces solutions avant de les implémenter sur un réseau mobile à grand échelle, a présenté l'objectif de ce projet. Pour le réaliser j'ai commencé par établir soigneusement les exigences qui doivent être vérifiées par les solutions SIG et ICache. Ensuite, j'ai effectué une étude de faisabilité où j'ai réuni les informations nécessaires, auprès du groupe HUAWEI, sur les équipement physiques, leurs capacités et leurs qualités techniques pouvant éviter tout type de redondance ou de panne dans un tel réseau télécom, sur l'architecture logique et sa facilité d'intégration dans le réseau sans aucun impact sur le fonctionnement actuel et sur les différentes fonctionnalités et leurs réponses aux exigences. Après j'ai attaqué une phase de déploiement permettant la mise en place des solutions, selon une planification du temps et des ressources bien déterminée auparavant. Par la suite j'ai effectué un ensemble de tests de fonctionnalités et de performances déjà préparés. Les tests réalisés ont permit de valider les fonctionnalités des solutions, d'autres tests de performances sont planifiés pour la solution ICache pour s'assurer de son efficacité.

La participation active à ce projet m'a permis d'approfondir mes connaissances dans le domaine des réseaux de Télécommunication à savoir le GSM, le GPRS, et l'UMTS, de bien maîtriser le suivi et l'évaluation d'un projet, de participer dans le déploiement des solutions ICache et SIG.
Il convient quand même de signaler que ce projet n'est pas encore achevé, le mois prochain sera destiné à poursuivre la validation de la solution ICache, et l'étude de faisabilité de l'interconnexion des deux solutions.

Annexe:

Annexe 1: l'évolution de l'UMTS

Avec la standardisation de l'UMTS dans le contexte du 3GPP, deux remarquables tendances ont émergé en influant fortement les réseaux UMTS. La première tendance est l'évolution vers une architecture UMTS tout IP basée sur la spécification Release 4 qui a remplacé les technologies en mode circuit par une commutation en mode paquet. Cette spécification a également introduit le support des applications multimédia dans le coeur du réseau UMTS. Pour atteindre une implémentation progressive et globale, 3GPP a subdivisé l'introduction de l'UMTS en plusieurs phases.

1. UMTS Release 99

La R99 est l'héritage du GSM/GPRS. L'architecture UMTS telle que décrite dans la R99 du 3GPP s'appuie sur une nouvelle interface radio. L'UTRAN est une évolution des cœurs de réseau GSM et GPRS (adaptation des équipements existants ou nouveaux équipements) pour gérer les flux des domaines circuit (CS: Circuit Switched) et paquet (PS: Packet Switched).

L'architecture UMTS R99 propose:

Les interfaces de l'UTRA avec le coeur de réseau sont basées sur un transport ATM (AAL2 pour la voix et AAL5 pour les données). Le transport dans le coeur de réseau peut ensuite être effectué selon le choix de l'opérateur soit en ATM pour l'ensemble des flux, soit en ATM puis TDM pour les flux circuit et en IP pour les flux paquet. La signalisation à l'interface avec l'UTRA est transportée soit dans des circuits virtuels ATM, soit avec le protocole de transport de SS7 sur IP.

Les appels multimédia sont supportés, mais de manière transparente: c'est à dire que les appels multimédia ne sont pas considérés comme un mode de communication. En effet, les messages de signalisation multimédia sont transportés de manière transparente dans une connexion circuit ou dans un contexte PDP (Protocol Data Packet). Ce qui permet d'introduire des fonctions multimédia dans les équipements GSM et GPRS, limitant ainsi les impacts aux terminaux et à l'ajout de serveurs multimédia. La R99 prépare donc l'évolution vers la solution cible tout IP en introduisant dès le début de l'UMTS un transport convergeant des flux voix et données.

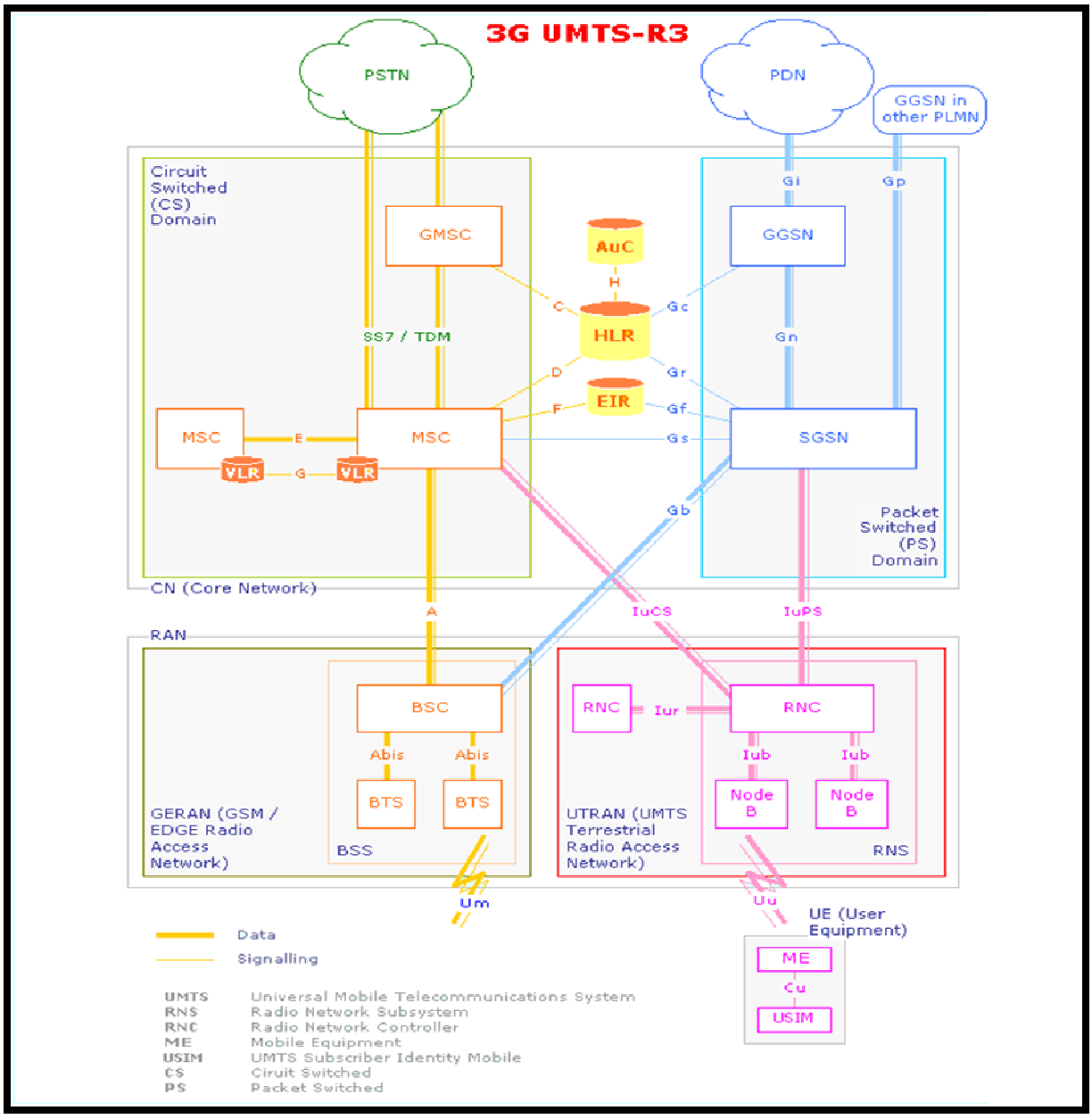


Figure: Architecture détaillée du réseau UMTS release 3

2. UMTS releases R4/R5

Alors que la release 99 UMTS a principalement pour vocation de gérer une transition douce avec le GSM/GPRS, la release 4 de l'UMTS propose une architecture résolument ovatrice afin d'évoluer vers le tout IP multimédia. Suite aux discussions techniques au sein du 3GPP et afin de prendre en compte la maturité des produits et solutions nouvelles, les évolutions de l'UMTS prévues dans cette version ont été échelonnées dans le temps et réparties sur deux versions successives, rebaptisées R4 et R5.

3. UMTS Release R4

La release 4 concerne l'évolution du domaine CS sur la base du NGN (Next Generation Network). La R4 présente des avantages pour le réseau de base en termes de flexibilité et d'évolution. En effet, la R4 peut réutiliser le Backbone IP du domaine PS pour le transport de la voix. Par ailleurs, la R4 dissocie les plans de contrôle et de transport, leur permettant d'évoluer séparément à la différence des commutateurs voix qui sont des structures monolithiques. Enfin, la R4 permet l'évolution vers un réseau tout IP où la voix est directement paquétisée sur la station mobile de l'usager et transportée de bout en bout sur IP, Avec la R4, la voix est transportée sur IP dans le réseau de base uniquement.

Les nœuds MSC et GMSC sont décomposés en deux entités pouvant être déployées de manière distribuée. Le MSC est décomposé en un MSC Server et un Circuit Switched Media Gateway (CS-MGW). Le GMSC est décomposé en un GMSC Server et un CS-MGW. L'échange de signalisation relatif aux appels téléphoniques a lieu entre le BSC ou RNC et le MSC Server. La parole est transportée entre le BSC ou RNC et le CS-MGW. Les entités MSC Server et GMSC Server contrôlent les passerelles CS-MGW à l'aide d'un protocole H.248.

Le MSC Server:

Le MSC Server prend en charge les fonctions de contrôle d'appel et de contrôle de la mobilité du MSC. Le MSC Server est associé à un VLR afin de prendre en compte les données des usagers mobiles. Le MSC Server termine la signalisation usager-réseau et la convertit en signalisation réseau-réseau correspondante. Par contre, il ne réside pas sur le chemin du média. Par ailleurs, il contrôle le CS-MGW afin d'établir, maintenir et libérer des connexions dans le CS-MGW.

Le Media Gateway:

Le CS-MGW reçoit un trafic de parole du RNC et le route sur un réseau IP ou ATM. L'interface Iu-CS (Interface entre RNC et MSC) se connecte dorénavant sur l'entité CS-MGW afin que le trafic audio puisse être transporté sur RTP/UDP/IP ou AAL2/ATM.

Le transport sera typiquement assuré par RTP/UDP/IP afin de réutiliser le Backbone IP du réseau GPRS et ainsi minimiser les coûts, le CS-MGW assure les fonctions suivantes:

- ✓ Le codage/décodage de la voix;
- ✓ L'annulation d'écho;
- ✓ La suppression de silence;
- ✓ La conversion des protocoles de transport.

Le GMSC Server

Pour les appels téléphoniques entrants provenant du RTCP, une entité GMSC est nécessaire. Le GMSC Server prend en charge les fonctions de contrôle d'appel et de contrôle de la mobilité du GMSC. Le GMSC Server termine la signalisation du RTC. Le GMSC Server interroge le HLR afin d'obtenir un numéro de MSRN et de pouvoir ainsi acheminer l'appel. Par ailleurs, le GMSC Server contrôle le CS-MGW afin d'établir, maintenir et libérer des connexions dans le CS-MGW.

La release 4 a introduit le concept du sigtran pour le transport de la signalisation dans un réseau IP, le SIGTRAN est définie par IETF dans la RFC 2719. SIGTRAN est l'acronyme de SIGnaling TRANsport. C'est une partie des réseaux de la nouvelle génération basée sur le protocole IP, le SIGTRAN a été conçu pour le transport des données de signalisation temps réel à travers les réseaux IP.

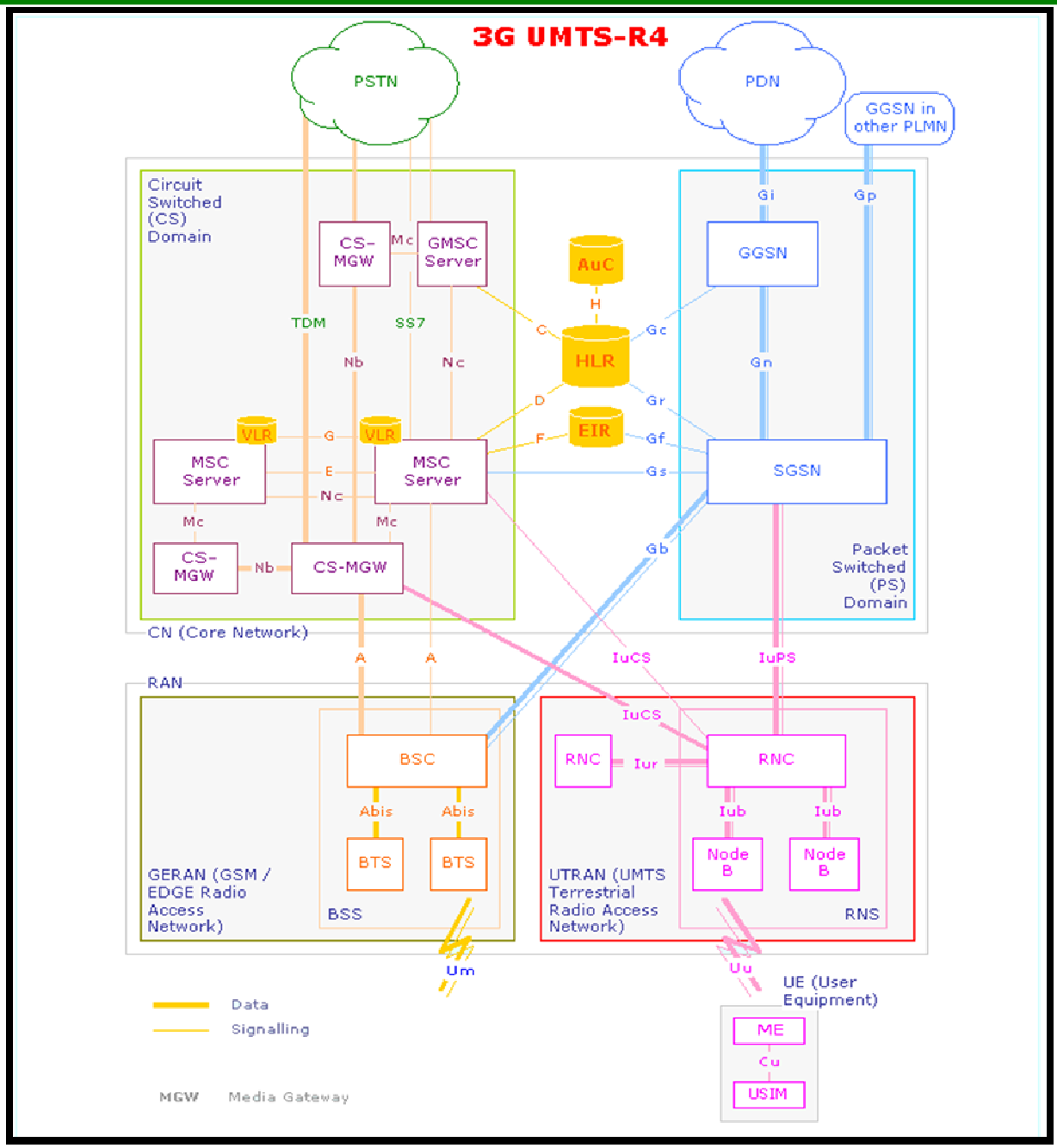


Figure: Réseau UMTS release 4

4. .UMTS Release R5

La Release 5 permet l'établissement de sessions multimédia, un transport de tout type de média de bout en bout sur IP et une offre de nouveaux services. Ces capacités sont prises en charge par un nouveau domaine appelé IMS (IP Multimedia Subsystem) qui se rajoute aux domaines CS et PS. Le domaine IMS qui se superpose au domaine PS, s'appuie sur le protocole SIP (Session Initiation Protocol) pour le contrôle de sessions multimédia. SIP

permet aussi l'accès aux plates-formes de services. Ce protocole est incontournable en raison de sa capacité à s'intégrer aux réseaux mobiles à un coût minimal.

L'organisme 3GPP a apporté plusieurs évolutions notables à l'interface radio de l'UMTS. Parmi ces évolutions on trouve le HSDPA introduite dès 2002 dans la " Release 5 " des spécifications UMTS.

HSDPA (High Speed Downlink Packet Access)

Le HSDPA est une technologie qui fournit des améliorations en termes de vitesse, de capacité et d'efficacité. Le HSDPA représente pour les technologies WCDMA et UMTS ce que la technologie EDGE représente pour le GSM en terme de vitesse de transmission et de capacité. Les débits 3G actuels en flux descendant (environ 384 Kbps et jusqu'à 2 Mbps selon les normes) seront portés à 14 Mbps (débit maximal selon les normes) sur les systèmes HSDPA de première génération. Les opérateurs pourront ainsi prendre en charge un nombre beaucoup plus important d'abonnés haut débit sur la même fréquence radio (porteuse), en garantissant une utilisation optimale des services multimédias existants ou à venir.

L'IMS (IP Multimedia Subsystem)

La release 5 de l'UMTS propose l'ajout d'un nouveau domaine connu sous le nom de l'IMS au domaine PS du réseau cœur pour supporter aussi bien la téléphonie traditionnelle que de nouveaux services multimédia.

C'est une évolution de l'UMTS qui consiste à définir un nouveau sous-système indépendant de l'accès (WLAN, GPRS, UMTS, …) et par la suite de pouvoir implémenter rapidement de nouveaux services et par conséquent de réduire les coûts. L'IMS assure le contrôle des sessions et des appels voix et multimédia ainsi que l'interconnexion de l'UMTS au réseau RTCP et à d'autres réseaux UMTS. Il repose sur un réseau cœur IP capable de fournir la qualité de service nécessaire aux services voix et multimédia. En effet, face à l'émergence des services multimédia utilisant simultanément de la voix et des données, l'IMS permet de contrôler les communications IP de bout en bout tout en garantissant une qualité de transport correcte de ces nouveaux services multimédia.

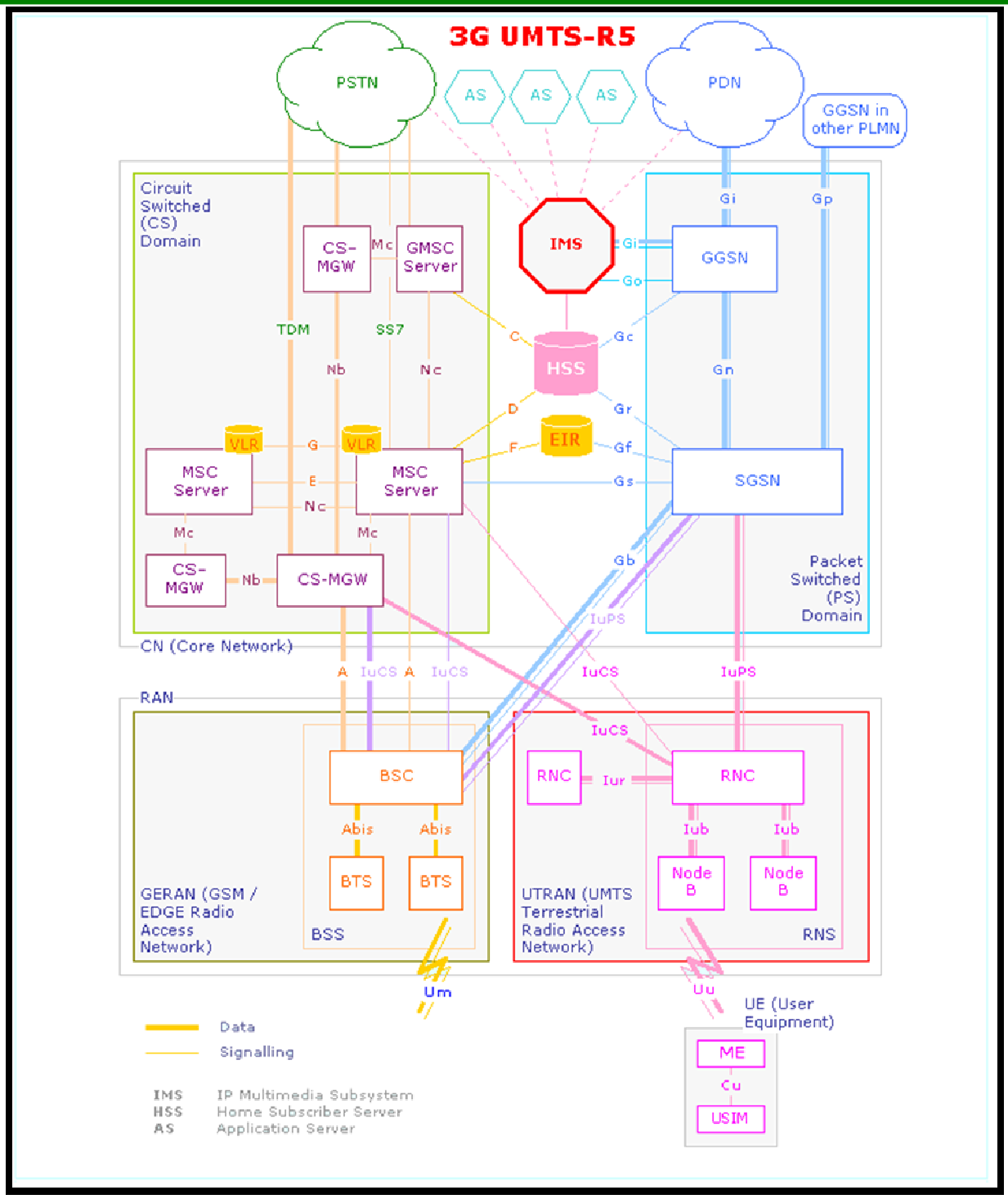


Figure: Réseau UMTS release 5

5. .UMTS Release 6

La tâche principale de cette phase est le perfectionnement d'IMS et l'interconnexion entre le WLAN (Wireless Local Area Networks) et l'UMTS. La Release 6 continuera dans la spécification des fonctionnalités et services existants : OSA, QoS LCS, MMS, Security Au

niveau du protocole de facturation, la R6 a amélioré ce service pour le prépayé, en adoptant une nouvelle application de Diameter dédiée à la facturation temps réel; appelée Credit Control Application DCCA.

6. .UMTS Release 7

La Release 7 introduit quant à elle le concept AIPN « All-IP-Network ». En effet, ce concept prévoit l'intégration des réseaux d'accès à un réseau coeur tout IP. Elle permet aussi d'offrir un ensemble de services indépendamment des réseaux d'accès. La R7 a par ailleurs introduit le NDS (Network Domain Security) qui, associé aux protocoles de mobilité, permet aux utilisateurs d'effectuer une mobilité transparente et sécurisée.

Bibliographie:

[1] Le gprs copyright Syselog 2000
[2] Rani Makke ; "Qualité de Service et Performance des Protocoles de Transport dans L'UTRAN"; thèse de doctorat soutenue le 03 Juillet 2003, TELECOM PARIS.
[3] Quidway SIG9810/9820 Service Inspection Gateway V200R003C00
[4] Huawei iCache Technical white paper.
[5]http://www.f5.com/glossary/load-balancing.html.
[6] http://www.f5.com/solutions/availability/local-load-balancing.
[7] Quidway SIG9810/9820 Service Inspection Gateway V200R003C00.
[8] Huawei iCache Technical white paper.