Étude de la connectivité Internet de l'île de la Réunion

Réhan Noordally

UNIVERSITÉ DE LA RÉUNION

Thèse
de l'Université de la Réunion

Spécialité

RESEAUX INFORMATIQUES

présentée par

M. Réhan NOORDALLY

Étude de la connectivité Internet de l'île de la Réunion

Soutenance le 30 Août 2018 devant le jury composé de :

Pr. Laure PETRUCCI	**Rapporteur**
Pr. Emmanuel LOCHIN	**Rapporteur**
Dr. HDR Prométhée SPATHIS	**Examinateur**
Pr. Rémy COURDIER	**Examinateur**
Dr. HDR Pascal ANELLI	**Directeur de Thèse**
Dr. Richard LORION	**Encadrant**

CETTE THÈSE A REÇU LE SOUTIEN FINANCIER DE LA RÉGION RÉUNION ET DE L'UNION EUROPÉENNE (FONDS EUROPÉEN DE DÉVELOPPEMENT RÉGIONAL - FEDER).

REGION REUNION
www.regionreunion.com

UNION EUROPEENNE

Je dédie cette thèse à l'ensemble des membres de ma famille.

Remerciements

Mes premiers remerciements vont à l'endroit de Monsieur Pascal Anelli, Maître de conférences HDR à l'Université de La Réunion, qui a accepté d'encadrer cette thèse. Je le remercie d'avoir mis toute son énergie pour que je puisse mener ces travaux dans les meilleures conditions. Je le remercie également pour la confiance et la patience sans faille qu'il m'a témoignées durant ces années.

Je remercie Monsieur Richard Lorion, Maître de Conférences à l'Université de La Réunion. Malgré un emploi du temps surchargé, il a su me consacrer du temps pour aiguiller mes travaux.

Je tiens à remercier tout particulièrement Madame Laure Petrucci, Professeur à l'Université Paris 13, et Monsieur Emmanuel Lochin, Professeur à l'ISAE SUPAERO qui m'ont fait l'honneur d'accepter de juger ces travaux et d'en être rapporteurs.

Je remercie le Professeur Rémy Courdier qui a accepté de présider mon jury de thèse. De par cette acceptation, je boucle mon cursus universitaire à l'Université de La Réunion. Mes remerciements vont à l'attention de Monsieur Prométhée Spathis qui consacre de son temps à la participation de mon jury de thèse en tant qu'examinateur.

Je tiens à remercier Messieurs Pierre-Ugo Tournoux et Xavier Nicolay pour les discussions que l'on a eues. Cela m'a permis de me remettre dans le droit chemin quand je m'égarais.

Je remercie également Monsieur Bruno Baynat, Maître de conférences à l'Université de Paris 6, qui a su donner un nouveau souffle à ces travaux à travers ses conseils lors de son passage.

Je remercie également Monsieur Denis Fabrègue, Responsable du pôle TIC à La Réunion, Monsieur Thierry Pretet, travaillant à la cellule Investissements publics de la Région Réunion, Monsieur Thomas Silverston, Chercheur au NICT, d'avoir accepté de faire partie de mon comité de suivi de thèse.

Je remercie également le Laboratoire d'Informatique et de Mathématiques, dirigé par Monsieur Jean Diatta, Professeur à l'Université de La Réunion, ainsi que l'ensemble des membres, pour l'accueil et les moyens qui m'ont été mis à disposition pour le bon déroulement de cette thèse.

Je remercie également la Région Réunion qui a soutenu financièrement ces travaux de thèse.

Je remercie également Messieurs Jean-Christophe Lan-Yan-Fock et Arnaud Ravoavahy pour les travaux réalisés durant leurs stages.

Je remercie également mes collègues, mes amis et mes proches pour leurs contributions et leurs encouragements.

Je remercie particulièrement, Aurélie, Miora, Florence et Anne-Claire, qui ont été dans la même galère que moi.

Je tiens à remercier du fond du coeur l'ensemble des membres de ma famille qui m'ont toujours apporté leur soutien et leur encouragement. Merci à vous.

Enfin, je tiens à remercier toutes les personnes, qui ont contribué de près ou de loin à la réalisation de ces travaux.

Résumé

L'accès à Internet des îles de la Zone Océan Indien a la particularité d'utiliser deux longs câbles sous-marins. Les routes ont en commun de passer par un de ces liens et d'introduire une composante de délai qui peut être significative. La performance de TCP est liée à l'état des routes et au délai. Dans la situation de l'île de la Réunion, comment se comporte un protocole ayant une dépendance au délai tel que TCP ?

Dans cette thèse, nous proposons une étude de l'Internet à la Réunion. Les travaux visent à pouvoir dresser un bilan de la connectivité Internet. Ils s'orientent d'une part à caractériser la connectivité au niveau du réseau et d'autre part à traduire ses caractéristiques au niveau de la couche de transport. Ainsi, les travaux présentés reposent sur deux études de métrologie sur le réseau réunionnais.

Le premier examen a pour objectif la caractérisation des délais et des routes empruntées depuis et en direction de l'île. Ces travaux reposent sur une plate-forme de mesures mise en place à cet effet. Un outil d'identification des routes a été développé afin d'analyser les chemins depuis et vers la Réunion. Cet outil utilise une base de données de géolocalisation construite à partir des adresses IP rencontrées, des délais associés et d'informations provenant des Registres Internet Régionaux. L'analyse des résultats montre des caractéristiques propres à la région Réunion.

La seconde étude de métrologie vise l'analyse des flux TCP. Des métriques associées à l'observation des captures de trafic sont identifiées afin d'établir les performances de TCP mais également les types de trafic entrant et sortant de l'île. Le volume des écoutes étant important, un outil d'analyse pour des traitements efficaces et rapides a également été développé.

Les contributions de cette thèse sont d'abord rattachées au contexte réunionnais et sont extrapolées vers l'internet de la Zone Océan Indien. Cette thèse se veut être un élément pour une réflexion avec l'ensemble des acteurs de l'Internet à la Réunion.

Mots clés :

Métrologie active, Délais, Routage, Métrologie passive, Performance, TCP, Zone Océan Indien, Réunion

Abstract

The access to the Internet of the Islands of the Indian Ocean Area has the particularity of using two long submarines cables. The routes have in common to go through one of these links and introduce a delay component that can be significant. The performance of TCP is linked to the state of the route and the delay. In the situation of Reunion Island, how does a protocol having a dependence on delay such as TCP behaves ?

In this thesis, we propose a study of the Internet in Reunion Island. The work aims to be able to take stock of Internet connectivity. They are oriented on the one hand to characterize the connectivity at the level of the network and on the other hand to translate these characteristics at the level of the transport layer. Thus, the works presented are based on two metrology studies on the Reunion network.

The first review aims to characterize the delays and the routes taken from and to the island. This work is based on a platform of measures put in place for this purpose. A road identification tool has been developed to analyze roads to and from Reunion Island. This tool uses a geolocation database built from IP addresses encountered, associated delays and information from the Regional Internet Registries. The analysis of the results shows characteristics specific to the Réunion region.

The second metrology study aims to analyze TCP flows. Metrics associated with the observation of the catches of traffic are identified in order to establish the performances of TCP but also the types of traffic entering and leaving the island. Since the volume of the intercepts is important, an analysis tool for efficient and rapid treatments has been developed.

The contributions of this thesis are first of all related to the Reunionese context and are extrapolated to the Internet of the Indian Ocean Zone. This thesis is meant to be an element for a reflection with all the actors of the Internet in Reunion Island.

Keywords :

Active Metrology, Delay, Routage, Passive metrology, Performance, TCP, Indian Ocean Area, Reunion Island

Table des matières

Liste des acronymes

ACK *Acknowledgement*.
ADSL *Asymmetric Digital Subscriber Line*.
AIMD *Additive Increase and Multiplicative Decrease*.
API *Application Programming Interface*.
ARCEP *Autorité de Régulation des Communications Electroniques et des Postes*.
AS *Autonomous System*.

BDP *Bandwidth Delay Product*.

CAIDA *Center for Applied Internet Data Analysis*.
CDCS *Comoros Domestic Cable Sytem*.
CDF *Cumulative Density Function*.
CIL *Correspondant Informatique et Libertés*.
CWND *Congestion Window*.
CWR *Congestion Window Reduce*.

DNS *Domain Name System*.
DSI *Direction des Services Informatiques*.
DupAck *Duplicate Acknowledgement*.

EASSY *Eastern Arfrica Submarine SYstem*.
ECE *ECN Echo*.
ECN *Explicit Congestion Notification*.

FAI *Fournisseurs d'Accès Internet*.
FTTH *Fiber To The Home*.

GIX *Global Internet eXchange*.
GNU *GNU's Not Unix*.
GPL *General Public Licence*.

HTTP *HyperText Transfer Protocol*.
HTTPS *HyperText Transfer Protocol Secured*.

IANA *Internet Assigned Numbers Authority*.
ICMP *Internet Control Message Protocol*.
IETF *Internet Engineering Task Force*.

IGMP *Internet Group Management Protocol*.

IMAP *Internet Message Access Protocol*.

IP *Internet Protocol*.

IPPM *IP Performance Metrics*.

IW *Initial Window*.

IXP *Internet eXchange Point*.

LAN *Local Area Network*.

LER *Label Edge Router*.

LFN *Long Fat Network*.

LIM *Laboratoire d'Informatique et de Mathématiques*.

LION *Lower Indian Ocean Network*.

LSP *Label Switched Path*.

LSR *Label Switch Router*.

MAN *Metropolitan Area Network*.

MPLS *MultiProtocol Label Switch*.

MSS *Maximun Segment Size*.

NRA *Noeud de Raccordement d'Abonnés*.

NS *Nonce Sum*.

OS *Operating System*.

PDF *Probability Density Function*.

POP *Post Office Protocol*.

PSAMP *Packet Sampling*.

RENATER *REseau NAtional de communication électroniques pour la Technologie, l'Enseignement et la Recherche*.

RIR *Regional Internet Registry*.

RITE *Reducing Internet Transport Latency*.

RSSI *Responsable Sécurité et Systèmes d'Information*.

RTO *Retransmission TimeOut*.

RTT *Round-Trip delay Time*.

SAFE *South-Africa Far East*.

SAT-3 *South Africa Transit-3*.

SCP *Ssh CoPy*.

SEAS *Seychelles to East Africa System*.

SMTP *Simple Mail Transfert Protocol*.

SSH *Secure SHell*.

ssthresh *slow-start threshold*.

TAI *Technologies d'Accès à Internet*.

TCP *Transmission Control Protocol*.

TTL *Time-To-Live*.

UDP *User Datagram Protocol*.

VDSL *Very-high-bit-rate Digital Subscriber Line*.

VLAN *Virtual Local Area Network*.

VOD *Video on demand*.

VPN *Virtal Private Network*.

WAN *Wide Area Network*.

WASC *West Africa Submarine Cable*.

ZOI *Zone Océan Indien*.

Introduction

1 Contexte général

Depuis sa première démonstration publique en 1972, Internet a fortement évolué [Leiner1997]. Dans une première phase, nous avons les changements de services. Les utilisateurs ont basculé des services historiques que sont l'échange d'e-mail et la navigation web, vers une utilisation interactive de l'Internet. Ces nouveaux services, tels que la *Voix sur IP*, les *Jeux en ligne*, le *Streaming*, etc. sont maintenant possibles peu importe l'endroit où l'on se situe. Cela grâce à la seconde phase des innovations de l'Internet : l'évolution des technologies logicielles et matérielles. Les technologies sont devenues de plus en plus mobiles, et proposent des débits d'accès à l'Internet de plus en plus importants. Ainsi, nous sommes passés d'un accès physique de chez soi, connectés à un ordinateur fixe et une liaison 56 kbit/s (kilo-bits/seconde) à des *smartphones* et des connexions mobiles avec un débit théorique minimal descendant de 20 Gbit/s (Giga-bits/seconde) dans un futur proche pour la technologie 5G. En parallèle, l'accès à Internet s'est démocratisé. D'après une étude de l'Organisation des Nations Unies, le nombre de téléphones mobiles est devenu supérieur au nombre d'habitants sur la planète [ONU2013]. Ces évolutions parallèles ont bouleversé l'usage de l'Internet. Est-ce que ces évolutions ont eu un impact sur l'Internet réunionnais ?

2 Contexte régional

2.1 L'Internet à La Réunion

Pour comprendre la situation de l'Internet à La Réunion, il est nécessaire de relater l'histoire de la connectivité Internet et de dresser un bilan de l'état actuel. Cet historique est effectué à partir du document [Pretet2000] qui présente l'avancement du projet de connexion de l'île de La Réunion au câble sous-marin *South-Africa Far East* (SAFE).

La première connexion de La Réunion à l'Internet date de 1992, avec la mise en service du projet Telecom-2. À cette époque, la seule liaison connectant La Réunion à Internet était une connexion satellitaire. Jusqu'en 2001, et l'arrivée du câble SAT-3/WASC/SAFE, les débits d'accès résidentiels ne dépassaient pas les 56 kbit/s. La bande passante totale de l'accès Internet de l'île par ce canal satellite était de 400 Mbit/s (Méga-bits/seconde), tous opérateurs confondus. Le coût d'utilisation de la liaison satellite avoisinait les $17\,000$€/Mb/mois et par opérateur. La technologie d'accès et le tarif élevé limitaient les usages de l'Internet privé à des services basiques comme l'échange d'e-mail. L'arrivée des câbles *South Africa Transit-3* (SAT-3)/*West Africa Submarine Cable* (WASC)/SAFE, en 2001, visaient à désenclaver numériquement l'île.

Ce câble d'une longueur totale de $28\,000$ Km (Kilo-mètres) connecte l'Europe (Espagne et Portugal) à l'Asie (Inde et Malaisie), en longeant la côte Ouest africaine, tel qu'illustrée par la carte figure 1. Le lien est composé de deux paires de fibres optiques avec une capacité globale de 135 Gbit/s. La répartition des capacités fut faite en fonction

du montant investi par les opérateurs. France Télécom fut sélectionnée pour la France avec un débit total de $13,6$ Gbit/s, dont 155 Mbit/s furent alloués à la connexion de La Réunion. Ce débit était équivalent à la capacité maximale théorique du lien satellite de France Télécom. Outre la sécurité apportée par la fibre optique, c'est la qualité de la transmission qui a été améliorée avec ce support. Ce câble a été une première étape dans la mise en place d'une autoroute de l'information entre l'Europe, l'Asie et l'Afrique. Pour La Réunion, cette autoroute a été un facteur pour la baisse des coûts de communication et en parallèle le déploiement de la technologie *Asymmetric Digital Subscriber Line* (ADSL). Les tarifs de consommation de la bande passante du lien ont connu une baisse importante suite à une décision de l'*Autorité de Régulation des Communications Electroniques et des Postes* (ARCEP) en 2004 [ARCEP2004]. Les tarifs sont passés de $17\,000$ €/Mb/mois à $1\,550$ €/Mb/mois.

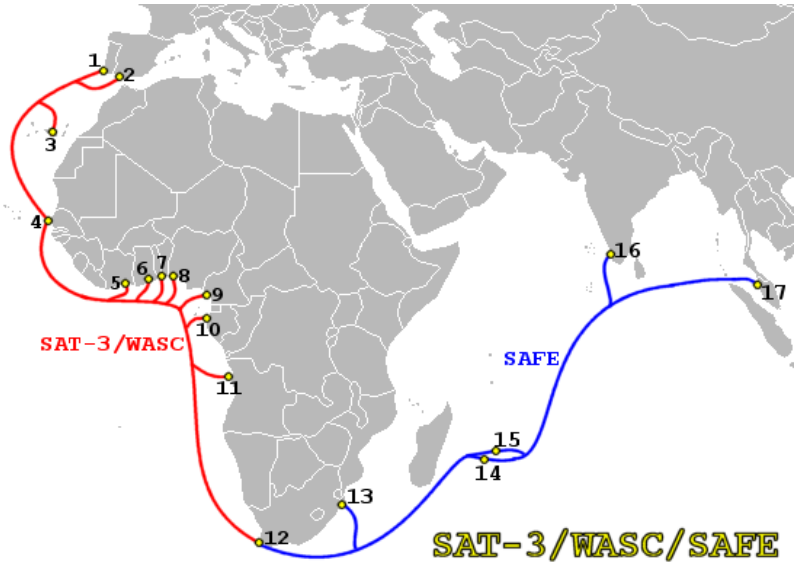


FIGURE 1 – Carte des points d'atterrissement du câble SAT-3/WASC/SAFE. (Source : [Pretet2000]).

Malgré la baisse des tarifs, l'ADSL n'était présent que dans 6 villes à forte densité de population. Afin d'augmenter la couverture de l'accès Internet de l'île, une dorsale faisant le tour de l'île est installée. C'est le réseau nommé *Gazelle* dont le début du déploiement fut effectué dans le courant de l'année 2003 [SDTAN2013]. Cette fibre est installée en hauteur en suivant le réseau Haute Tension d'EDF selon le plan de la figure 2 (en trait bleu ou foncé). Le but de ce réseau est de raccorder l'ensemble des *Noeud de Raccordement d'Abonnés* (NRA). Un NRA est un local hébergeant un central téléphonique de l'opérateur historique France Télécom dans lequel aboutissent les lignes téléphoniques des abonnés communément appelées boucles locales. Au delà de ces locaux, les boucles locales forment le réseau capillaire. L'interconnexion entre le réseau Gazelle et les NRA est représentée en vert sur la figure 2.

En 2004, La Réunion s'est dotée d'un point d'échange (*Global Internet eXchange* (GIX) ou *Internet eXchange Point* (IXP)) nommé *Reunix*. Il fut pendant près de 10 ans, le seul IXP présent dans la *Zone Océan Indien* (ZOI). Géré par le *REseau NAtional de communication électroniques pour la Technologie, l'Enseignement et la Recherche* (RENATER), il vise à interconnecter les fournisseurs d'accès Internet de La Réunion afin d'éviter que le trafic local ne sorte de l'île et consomme des capacités sur le câble sous-marin. En plus de cet équipement, des technologies de cache ont été déployées sur le territoire. L'Université de La Réunion a été un des acteurs de ce déploiement.

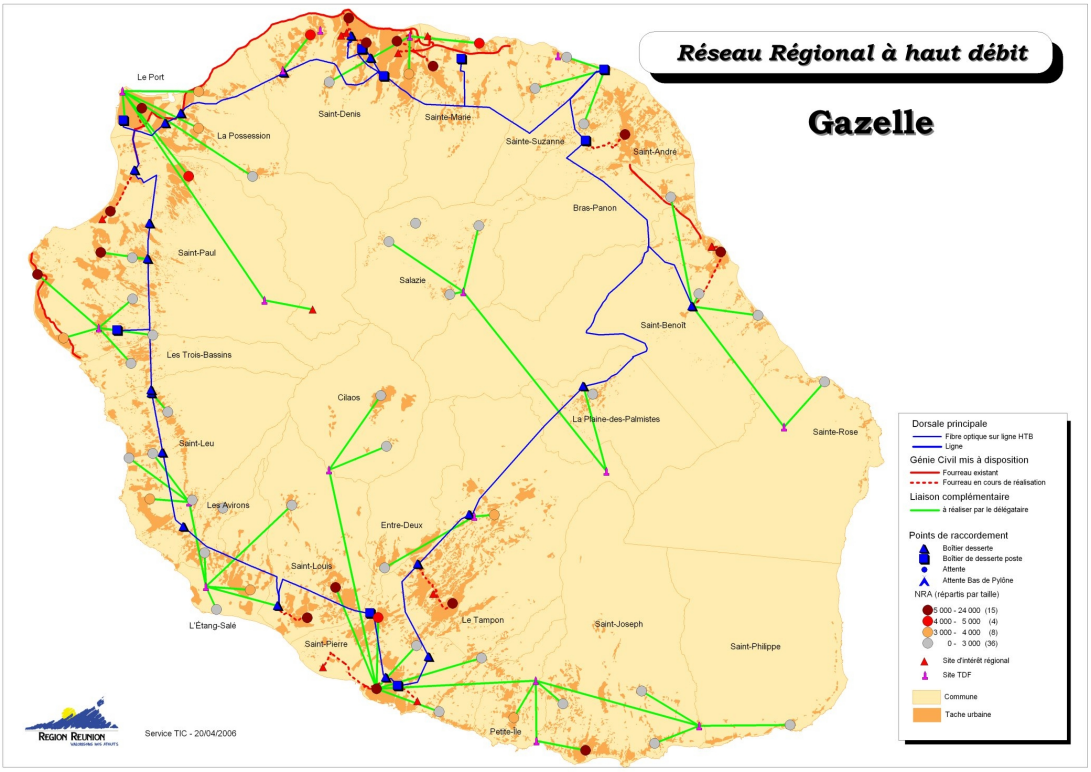


FIGURE 2 – Plan de câblage du réseau Gazelle en 2006. (Source : [Pretet2000]).

Depuis la décision de l'ARCEP en 2004, chaque année une baisse de 20 à 40% du prix du Mégabit sur le câble sous-marin est enregistrée. En 2006, pour 50€ un abonné n'avait droit qu'à la connexion ADSL de 1 Mbit/s sans aucun service additionnel. L'année suivante, pour le même tarif, la téléphonie illimitée vers certains pays a été ajoutée au forfait. Dans le courant de l'année 2010, le forfait est resté le même mais le débit alloué est augmenté pour atteindre 8 Mbit/s. La Réunion n'a vu l'arrivée du *triple play* (Télévision, Téléphone, Internet) qu'à partir des années 2011/2012 avec l'arrivée d'un nouveau câble : Lower Indian Ocean Network *(LION)*. Le LION est un câble sous-marin reliant La Réunion, Maurice et Madagascar depuis 2009. En 2012, une extension est rajoutée, sous le nom de LION-2, connectant le *LION* à Mayotte et au Kenya. Ce nouveau câble propose dès sa mise en service une capacité dépassant le 1 Tb/s (Térabit/seconde).

L'augmentation continue des débits et de la capacité disponible sur le câble SAT-3/WASC/SAFE, actuellement à 900 Gbit/s, a accéléré le déploiement de nouveaux services et de nouvelles technologies d'accès à Internet pour les abonnés. L'île de La Réunion dispose actuellement, en dehors des connexions mobiles, de trois *Technologies d'Accès à Internet* (TAI). La première est la technologie ADSL présente depuis 2001. Elle propose des débits asymétriques allant jusqu'à 20 Mbits/s en descente. C'est le débit qu'aura l'utilisateur en téléchargement. Depuis 2014, l'opérateur historique Orange (ex-France Télécom) propose la technologie *Very-high-bit-rate Digital Subscriber Line* (VDSL) 2 avec des débits allant jusqu'à 100 Mbit/s descendant. La limite physique de cette TAI impose une distance entre l'abonné et le distributeur inférieure à 1 Km. La dernière technologie présente sur l'île est la fibre optique. Déployée depuis 2007 par l'opérateur privé ZEOP, elle était, jusqu'à peu, principalement déployée dans les villes du Port, Sainte Marie et Saint Pierre.

Chaque opérateur dispose d'une ou plusieurs technologies d'accès. Chaque technolo-

gie est associée à un débit maximal théorique. La carte 3 [1] présente les débits théoriques qui sont présents sur l'île [France2017].

Cette carte montre une disparité des débits selon les zones géographiques de l'île. Le *Plan France Très Haut Débit* a pour objectif d'uniformiser, sur l'ensemble du territoire français, les débits avec le déploiement de la technologie d'accès fibre optique.

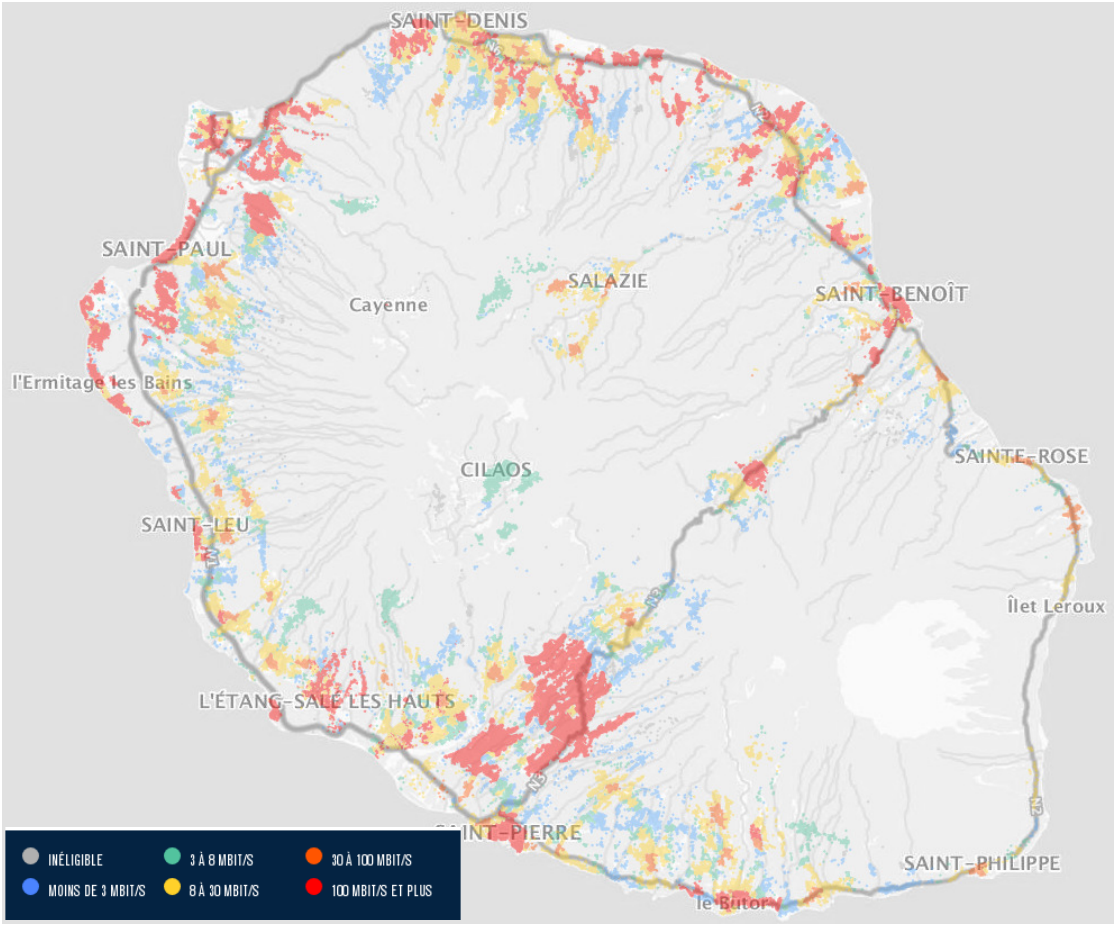


FIGURE 3 – Carte des débits à La Réunion.

Récapitulatif

La connexion à Internet donne à La Réunion des capacités importantes. La présence d'un GIX sur le territoire a limité le trafic réunionnais sur les câbles sous-marins. La figure 4 montre l'ensemble des événements qui ont marqué le développement de l'Internet à La Réunion jusqu'à nos jours.

Depuis la décision de l'ARCEP en 2004 [ARCEP2004] et l'arrivée du câble LION, les opérateurs ont fait le choix d'augmenter les services proposés avec un prix résidentiel stable. Les derniers services ajoutés sont ceux de la *Video on demand* (VOD) et de la *rediffusion (Replay)*. En 2014, le prix moyen du Mégabit/Mois sur le câble SAT-3/WASC/SAFE avoisinait les 25 €. En près de 15 ans, on note la baisse du coût moyen du Mégabit/mois de 17 000 € à 25 €.

L'évolution de la connectivité Internet à La Réunion est liée au développement de la connectivité des différents pays présents dans la Zone Océan Indien.

1. Source : Observatoire France Très Haut Débit

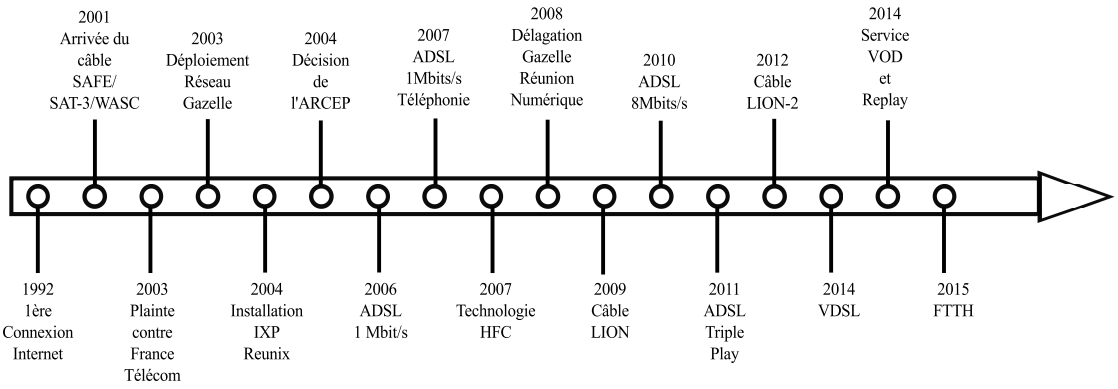


FIGURE 4 – Frise chronologique du développement de l'Internet à La Réunion.

2.2 L'Internet dans la Zone de l'Océan Indien

Les acteurs du développement du numérique dans la Zone Océan Indien

Dans le cadre de nos études, nous restreignons la ZOI à 6 îles ou archipels suivants (rangés par ordre alphabétique) : les Comores, Madagascar, Maurice, Mayotte, La Réunion et les Seychelles. À l'exception de Mayotte et de La Réunion qui sont des régions françaises, les autres îles et archipels cités sont des pays indépendants. Nous allons dans un premier temps faire une présentation des principaux acteurs du développement numérique dans chaque territoire. Le développement de l'Internet dans la ZOI se fait en collaboration avec l'ensemble des pays. Nous poursuivrons avec les futures installations des câbles sous-marins dans la ZOI.

L'**Union des Comores** est une république fédérale d'Afrique. L'archipel est connecté à Internet depuis le 19 Janvier 1998 via une connexion satellite. En 2010, le gouvernement déploie le *Comoros Domestic Cable Sytem* (CDCS) qui relie l'ensemble des îles de l'archipel entre elles, avec en parallèle le raccordement au câble *Eastern Arfrica Submarine SYstem* (EASSY) [Comores2002]. Ce câble relie l'Afrique du Sud au Soudan, en longeant la côte Est du continent. En 2009, l'*Autorité Nationale de Régulation des TIC* (*ANRTIC*) voit le jour. De nombreuses missions sont données à cette autorité comme appliquer et faire respecter la loi des *Technologies de l'Information et de la Communication* (*TIC*), réguler le secteur des TIC, favoriser la coopération entre les acteurs et gérer les différends, garantir une concurrence saine et loyale entre les opérateurs et de développer la recherche, la formation et les innovations technologiques [ANRTIC2016]. En décembre 2016, un troisième câble connecte l'archipel à Mayotte. Actuellement, un Vice-Président chargé des TIC travaille en collaboration avec un Conseiller du président en matière de transports et télécommunications.

La République de Madagascar est reliée à Internet par deux câbles sous-marins. Le premier est l'EASSY. Le second câble est le LION. Au niveau des prises de décisions, 3 organismes principaux existent. Le plus important est le ministère des Télécommunications et des Nouvelles Technologies. Il a mis en place le *Projet d'Infrastructure de Communication pour Madagascar* (*PICOM*). L'objectif est la réduction des coûts d'accès aux services de télécommunications. Le second est l'*Autorité de Régulation des TEchnologies de Communication* (*ARTEC*). Cet administration octroie les licences aux propriétaires des réseaux, arbitre les différends entre opérateurs et assure la gestion des spectres [ARTEC2016]. Le dernier organisme est le *Groupement des Opérateurs en Technologies de l'Information et de la Communication* (*GOTICOM*). Il a pour objectif d'accompagner et d'améliorer les infrastructures de télécommunication et de favoriser l'intégration des TIC [GOTICOM2011]. Depuis 2016, un GIX est présent sur l'île grâce au projet *AXIS* de l'Union Africaine [MGIX2017].

La République de Maurice regroupe les îles Rodrigues et Maurice. Sous l'impulsion du gouvernement anglais, la première ligne téléphonique fut installée en 1883. Actuellement, en plus d'une connexion satellitaire reliant les deux îles, le SAFE et le LION connectent Maurice à Internet. Un ministère des Technologies, de l'Innovation et des Communications existe au sein du gouvernement. C'est ce même gouvernement qui nomme le directeur de l'*Information and Communication Technologies Authority* (*ICTA*). C'est l'autorité de régulation des Télécoms et des Postes. Il existe 2 principaux opérateurs que sont Mauritius Telecom et Emtel. Une dizaine d'opérateurs cohabitent sur l'île [ICTA2017]. Depuis 2016, un nouveau GIX est présent sur l'île grâce au projet *AXIS* de l'Union Africaine [MIXP2017].

Mayotte est un département français depuis Mars 2011. Le raccordement au câble *LION-2*, extension du câble LION, en avril 2012 rend possible l'arrivée du haut débit sur ce territoire. En 2013, un GIX géré par RENATER est installé au sein du Rectorat. Il se nomme *Mayotix*.

Les **Seychelles** ont vu leur première connexion Internet introduite dans l'archipel par Atlas Seychelles Ltd en septembre 1996. En 2012, les Seychelles sont connectés à une fibre en provenance de Tanzanie. C'est le câble *Seychelles to East Africa System* (SEAS) . C'est l'unique câble sous-marin connectant l'archipel. Le *Ministère des Technologie de l'Information et des Communications* (*MITC*) fait office d'autorité de Régulation des Télécommunications dans le pays [DICT2017].

Chaque autorité de régulation à un impact sur le développement de l'Internet dans son pays. Ce développement se répercute sur l'amélioration de l'accès Internet dans la ZOI.

Développement de l'interconnexion de la Zone Océan Indien

Cette région a connu un premier bouleversement de sa connectivité à Internet avec le déploiement du câble sous-marin SAT-3/WASC/SAFE en 2001 pour La Réunion et Maurice. L'arrivée du LION en 2009 a connecté Madagascar aux deux îles. En 2010, les Comores et Madagascar se sont ouverts une voie vers l'Afrique avec le câble EASSY. L'interconnexion du LION 2 a développé l'Internet à Mayotte tandis que le déploiement du câble SEAS a ouvert les Seychelles à l'Internet haut débit. La carte 5 indique les différents câbles sous-marins présents dans la ZOI.

La ZOI s'engage dans le déploiement de nouveaux liens.

Le câble *MElting poT Indianoceanic Submarine System (METISS)* d'une longueur de $3\,500$ kilomètres reliera Madagascar, Maurice, et La Réunion à l'Afrique du Sud. La bande passante du câble sera de 24 Tb/s. Sa mise en service est prévue pour le courant de l'année 2019 [Lemauricien].

Africa-1 est un câble reliant l'Afrique du Sud, le Moyen Orient et l'Asie centrale. Ce câble de plus de $12\,0000$ kilomètres passera le long de la côte Est africaine avant de relier l'Arabie Saoudite, l'Égypte et le Pakistan. La mise en service du câble est prévue pour le courant de l'année 2020 [Africa1].

En 2019, sera mis en service le câble IOX. *IOX* est un câble sous-marin dédié à l'île Maurice. Il a pour but d'offrir une nouvelle liaison à Maurice en reliant l'île à l'Afrique et au reste du monde. Il sera doté d'une capacité de $54\ Tb/s$ [IOX].

La carte 6 représente l'ensemble des IXP présents dans la Zone Océan Indien. En vert, ce sont les points d'échanges déjà en service. La France a, dès l'année 2004, mis en place le point d'échange à La Réunion et en 2012 celui de Mayotte. Ceux de Maurice et de

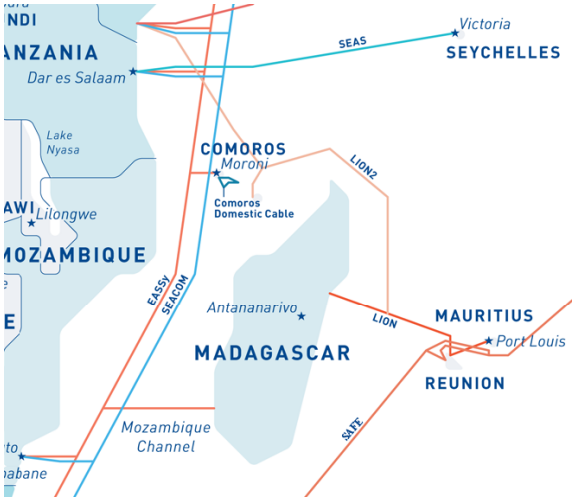


FIGURE 5 – Cartes des câbles sous-marins dans la Zone de l'Océan Indien. (Source : [Cablesmap]).

Madagascar ont été mis en service en 2016 avec l'aide de l'Union Africaine, de l'Internet Society et du projet AXIS [AXIS]. Les points bleus représentent les points d'échange qui sont prévus d'être déployés dans la zone océan indien par le projet AXIS dans le futur. D'ici quelques années, l'ensemble des territoires de la zone sera équipé d'un point d'échange. Cet équipement vise a maintenir le trafic de type *Metropolitan Area Network* (MAN) du pays où il est installé. Il facilite les échanges entre les opérateurs locaux en réduisant la latence et en augmentant la qualité de service.

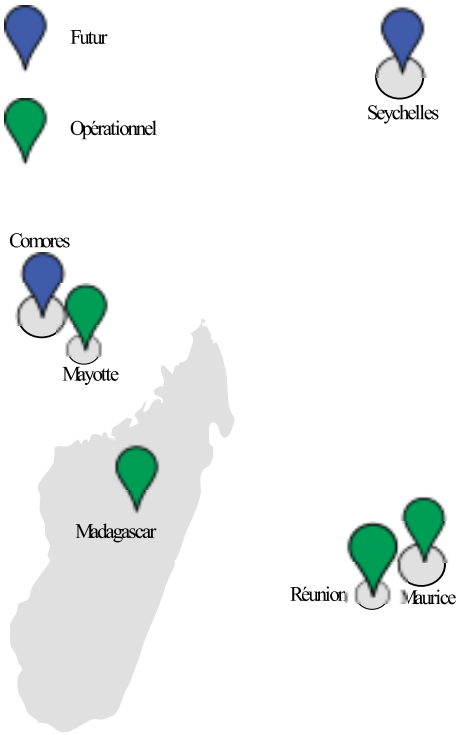


FIGURE 6 – Carte des points d'échange présents actuellement et dans un futur proche dans la ZOI.

3 Problématique

L'Internet et ses applications ont été développés dans des territoires où les routes sont nombreuses. L'île de La Réunion, comme beaucoup de territoires insulaires, ne bénéficie pas d'un nombre de liaisons physiques directes important. L'évolution de l'Internet allant des applications tolérantes aux délais vers des applications temps-réel nécessite une robustesse et une qualité de service dépendantes d'un maillage fort et de délais courts.

L'étude d'[Anelli2012] a démontré que les délais à destination d'adresses aléatoires sont sensiblement plus longs depuis La Réunion que depuis Paris, avec un écart d'environ 180 ms. Suite à ce constat, l'auteur a réalisé des simulations estimant les débits associés avec un taux de pertes de 10%. Ces simulations ont mis en avant des débits écoulés plus faibles pour un usager situé à La Réunion qu'un usager basé à Paris. Une augmentation de la bande passante n'entraînerait pas une diminution des délais. Le groupe de travail européen *Reducing Internet Transport Latency* (RITE) a réalisé une vidéo explicative de ce phénomène [RITE2014-2].

Cette thèse vise à mettre en lumière les principaux freins des débits écoulés.

Dans une première étape, nous étudierons l'évolution des délais depuis La Réunion en prenant comme base l'étude réalisée par [Anelli2012].

Dans un second temps, nous étudierons les routes logiques de l'Internet réunionnais.

Dans un dernier temps, nous réaliserons une proposition d'étude de métrologie. Cette étude vise à identifier la corrélation des événements de congestion entre les flots, l'importance des anomalies affectant *Transmission Control Protocol* (TCP) (pertes initiales, faux événements de congestion), la répartition des flots (en taille, en protocole, en application) et les paramètres de performances (taux de pertes,RTT, débit écoulé).

4 Organisation de la thèse

Suite à l'exposition de notre problématique, le chapitre 1 présente le contexte scientifique de nos travaux. Dans un premier temps, nous allons présenter les caractéristiques de TCP et sa problématique liée aux réseaux à forte capacité de stockage. Nous continuerons avec une présentation de quelques solutions. Nous déterminerons si l'accès Internet de La Réunion doit être considéré comme un réseau à forte capacité de mémorisation. La suite du chapitre inclura la définition de la métrologie dans les réseaux et une présentation des techniques de mesures active et passive.

La première étude est décrite dans le chapitre 2 et débute par la présentation des objectifs. Un cahier des charges permettant de répondre aux objectifs a été rédigé. Ce cahier des charges a débouché sur le déploiement de la plate-forme de métrologie active RunPL et du développement de deux outils d'aide à l'analyse : rgeoloc et rtraceroute. La présentation du protocole de mesure a été réalisée dans la partie précédant celle des résultats. Le chapitre se conclut par une synthèse des résultats qui ont servi à nos contributions.

La seconde étude est présentée dans le chapitre 3. Les objectifs du chapitre sont présentés dans un premier temps et divisés en deux. Ce chapitre présente la mise en oeuvre d'une plate-forme de métrologie et du protocole de mesure associé. Une section résultat associée à une conclusion termine le chapitre. Ce chapitre a fait l'objet d'une contribution scientifique.

Nous concluons notre thèse par un résumé des différentes contributions. Un apport sur les perspectives qu'autorisent nos travaux est proposé dans le chapitre 3.5.

Chapitre 1

État de l'art

Transmission Control Protocol (TCP) est le protocole de transport le plus utilisé sur l'Internet. L'étude réalisée par *Center for Applied Internet Data Analysis* (CAIDA), sur une durée de 2 ans, du trafic passant par le point d'échange (IXP) *EQUNIX* de Chicago, a montré que $90,97\%$ des paquets *Internet Protocol* (IP) acheminent des segments TCP [EQUINIX]. TCP est un protocole de transport qui rend un service de transfert fiable de données. Lorsque la somme du débit des émetteurs TCP partageant une même ressource du réseau excède la capacité de cette ressource, il se produit de la congestion. La congestion est un phénomène indésirable qui met le réseau dans un état où le service rendu est dégradé. Cette dégradation peut être sévère en fonction de l'intensité du phénomène. Pour éviter que l'effet de la congestion empire quand elle apparaît, TCP intègre une fonction de résolution connue sous le nom de contrôle de congestion. Le principe est que chaque émetteur détecte la congestion et diminue son débit d'émission. Pour se faire, le contrôle de congestion s'appuie sur la boucle de contrôle constituée entre l'émission d'un segment de données et la réception de l'acquittement correspondant. Le contrôle de congestion agit sur le débit d'émission de l'émetteur avec une latence liée au *Round-Trip delay Time* (RTT). Lorsque le produit du RTT avec la capacité d'écoulement offerte par le réseau est relativement important, le contrôle de congestion de TCP peine à utiliser les ressources du réseau efficacement. Ce produit du délai et du débit représente la quantité de données non acquittées qui peut circuler. On peut assimiler ce produit à la capacité de stockage de données dans le réseau.

Ces dernières années, l'augmentation de la bande passante a fait croître significativement cette capacité de stockage. En effet, comme les délais n'ont pas diminué dans les mêmes proportions, la capacité de stockage n'a fait que croître. Cette évolution pose un défi au contrôle de congestion de TCP pour maintenir ses performances. Cette évolution a entraîné une activité intense de recherche pour traiter ce problème de produit délai-bande passante pour TCP. Ainsi de nouvelles versions du contrôle de congestion de TCP ont été étudiées pour l'adapter aux spécificités des réseaux à forte capacité de stockage, *Long Fat Network* (LFN).

Si le stockage important de données dans le réseau pose un problème pour le contrôle de congestion de TCP qu'en est-il en pratique dans le cas de l'Internet à La Réunion ? Pour répondre à cette question, il faut pouvoir mesurer l'existant. Depuis quelques années, il y a un intérêt croissant pour la mesure. Une science de la mesure sur l'Internet se développe. Il faut chercher dans la croissance continue et soutenue de l'Internet ainsi que dans l'absence d'une exploitation coordonnée les motivations à développer la métrologie sur Internet. Cette métrologie vise à mieux comprendre le fonctionnement de l'Internet.

Ce chapitre se compose de deux sections thématiques. La première section 1.1 traite de la problématique du contrôle de congestion de TCP utilisé sur les réseaux à grande

capacité de stockage. La sous-section 1.1.1 rappelle le principe du contrôle de congestion et sa mise en œuvre dans TCP. Dans la partie 1.1.2, les problèmes spécifiques du contrôle de congestion de TCP appliqué dans le contexte des réseaux à forte capacité de mémorisation sont indiqués. Face à ces problèmes, des propositions ont été étudiées que nous présenterons dans les parties 1.1.3 et 1.1.4. Pour conclure cette section, nous poserons, dans la sous-section 1.1.5, les arguments qui permettent d'avancer que l'île de La Réunion a une connectivité qui s'apparente à celle des réseaux à forte capacité de stockage.
La seconde section 1.2 est consacrée à la métrologie du trafic Internet. La définition et les méthodologies de la métrologie sont indiquées dans la partie 1.2.1. La présentation de la métrologie active sera réalisée dans la section 1.2.2, suivie par celle de la métrologie passive dans la section 1.2.3. La comparaison entre la métrologie active et passive terminera cette présentation et sera faite dans la partie 1.2.4. Pour conclure ce chapitre, une synthèse est réalisée par la section 1.3 dans laquelle nous tirons les enseignements pour mener des études depuis et vers La Réunion.

1.1 Le contrôle de congestion TCP et les réseaux à grande capacité de stockage

TCP est un protocole de transport créé en 1980 et, décrit pour la première fois dans le [RFC793], il a subi depuis de nombreuses évolutions comme l'indique le [RFC7414]. Le succès de TCP repose sur son service de transmission fiable et ordonnée d'un flux de données asynchrones. C'est un protocole fonctionnant de point à point et de bout en bout autrement dit entre l'émetteur et le récepteur des données sans concerner les équipements intermédiaires. TCP offre un service de communication équivalent à un canal virtuel bidirectionnel entre 2 entités applicatives. Le canal de communication se caractérise par sa transparence sémantique c'est-à-dire par l'absence d'altération des données transférées. Pour réaliser cette fiabilité de l'échange, TCP supervise les échanges de données par des acquittements (*Acknowledgement* (ACK)). Cette supervision forme une boucle de contrôle correspondant à l'émission de données et à la réception de l'acquittement correspondant. Elle se caractérise par le délai pris nommé RTT. La correction des données perdues ou altérées en cours de transit s'effectue par retransmission de ces données. Si le principe de fonctionnement de TCP s'énonce facilement, sa mise en œuvre est complexe du fait de la non fiabilité du protocole IP sous-jacent et de la diversité des contextes d'utilisation de TCP. L'article [Ros2005] détaille les différentes caractéristiques du protocole liées à l'établissement de connexion, la numérotation des données et à la fiabilisation des échanges.

Outre l'objectif de fiabilité, TCP a aussi un objectif de performance pour le service rendu en termes de débit écoulé et d'utilisation des capacités de transmission du réseau. Pour atteindre cet objectif pour le service, TCP intègre une fonction de contrôle de flux qui repose sur une fenêtre glissante gérée par le récepteur. Ainsi le débit d'émission peut s'aligner sur le débit de réception, de sorte qu'un récepteur lent ne puisse être saturé par un expéditeur rapide. La spécification initiale de TCP a été conçue sans prendre en compte les ressources du réseau. Cet oubli a été à la source de dysfonctionnements sévères du réseau comme l'effondrement dû à la congestion (*congestion collapse*) [Afanasyev2010]. La fonction de contrôle de congestion vise à une prise en compte des ressources disponibles du réseau et à leurs utilisations efficaces. Le contrôle de congestion a suscité un travail de recherche intensif et ce sujet reste encore d'actualité comme l'indique le [RFC6077].

1.1.1 Contrôle de congestion de TCP

D'après [Jain1990], la congestion s'exprime par l'équation mathématique 1.1.

$$\sum Demande > Ressources \tag{1.1}$$

Du point de vue d'un réseau par commutation de paquets, les ressources sont principalement les mémoires tampon des nœuds de commutation et la capacité de transmission des artères de communication. La congestion apparaît au niveau des nœuds de commutation et plus particulièrement sur leurs interfaces de sortie. La condition pour voir apparaître une congestion est « si la somme des débits des flux arrivant sur l'interface de sortie est supérieure à la capacité de transmission du lien en sortie ». Dans cette situation, une file d'attente se constitue et quand elle déborde, les effets néfastes de la congestion se concrétisent. A savoir que le taux de pertes des paquets augmente dans le réseau, ce qui se traduit au niveau du service par un débit écoulé qui chute et un délai de transfert qui augmente. Dans [Chiu1989], les auteurs montrent que la performance du réseau est liée à la charge appliquée au réseau. Formellement la charge s'exprime comme taux d'arrivée sur le taux de service. Informellement, la charge représente la proportion de la demande autrement dit du trafic émis par rapport à la capacité de transfert. La figure 1.1 illustre l'évolution du débit écoulé (*throughput*) et du RTT en fonction de la charge appliquée au réseau (*load*). Au début, le débit écoulé s'accroît avec la charge alors que les délais n'augmentent presque pas. On est dans une phase de remplissage des liens. Lorsque la charge s'approche du taux de remplissage maximum des liens du réseau, Le débit écoulé n'augmente presque plus alors que les délais augmentent fortement. C'est la phase de remplissage des files d'attente. Ces deux phases sont séparées par un point caractéristique qui s'appelle le point d'inflexion (*knee*). Lorsque les files d'attente sont pleines et que la charge du réseau continue de s'accroître, les files d'attente vont déborder. À partir de ce point appelé le point de retournement (*cliff*) le réseau rentre dans l'état dit d'effondrement dû à la congestion (*congestion collapse*).

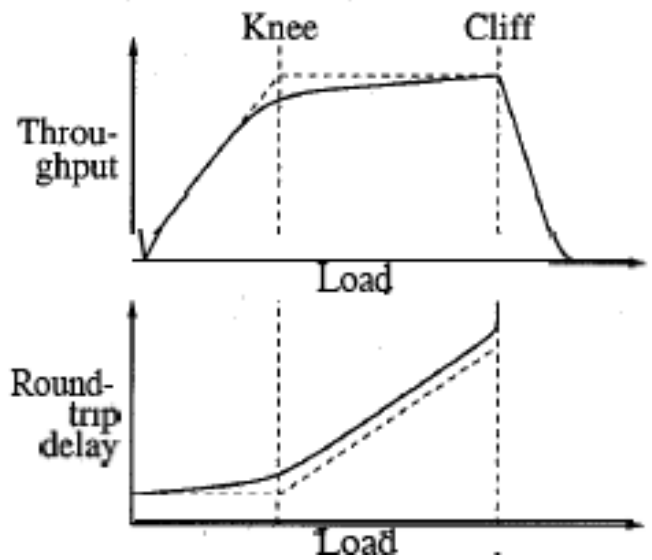


FIGURE 1.1 – Performance du réseau en fonction de la charge appliquée. (Source : [Chiu1989]).

L'effondrement dû à la congestion est rapporté par [Nagle1984]. Dans cet état, le réseau enregistre des retransmissions abusives, effectue des transferts avec des délais tendant vers l'infini et rend un service avec un débit écoulé proche de zéro. L'effondrement dû à la congestion s'explique par le gaspillage des ressources utilisées en amont du point

de perte du paquet. La solution à l'effondrement dû à la congestion réside en l'alignement du débit de l'émetteur à la capacité d'écoulement du canal de communication offert par le réseau afin de ne produire aucune perte. Ainsi les objectifs assignés au contrôle de congestion de TCP sont d'éviter l'état d'effondrement dû à la congestion, d'allouer équitablement les ressources du réseau entres les flux concurrents et d'optimiser les performances obtenues par chaque flux [RFC2914].

Le contrôle de congestion de TCP fonctionne sur le principe de la boucle fermée avec le réseau vu comme une boîte noire ainsi présenté par la figure 1.2. Après une stimulation sous la forme de l'envoi de paquets, l'observation du comportement de la boîte noire à ce stimulus sera analysé par le contrôleur situé dans l'émetteur. Le contrôleur rapproche l'observation faite en retour du stimulus (*feedback*) par rapport à l'objectif affecté au contrôleur. Celui-ci par rétro-action ajustera le nombre des paquets suivants envoyés. Cet ajustement est le résultat d'une fonction de contrôle qui se base sur une perception binaire des retours à savoir : absence ou présence de congestion.

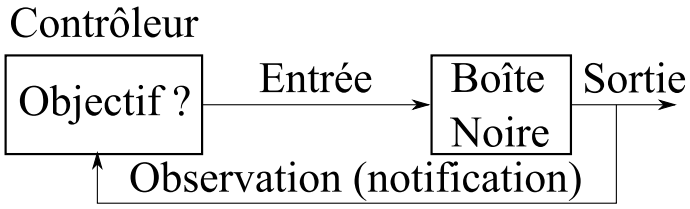


FIGURE 1.2 – Boucle fermée du CC de TCP.

Dans [Gevros2001], l'auteur liste les moyens pour effectuer les observations que l'on nomme en fait des notifications dans le contexte des réseaux. Les notifications de la congestion dans le réseau peuvent être implicites ou explicites. Dans le premier cas, elles sont déduites par l'absence d'ACK. L'augmentation des délais et les pertes des données sont des causes possibles pour la non-réception de l'ACK. A l'inverse, l'absence de congestion est déduite par la réception d'un ACK. Cette réception autorise l'envoi d'un nouveau paquet comme le montre [Jacobson1988-1]. Les notifications peuvent être explicites si les paquets véhiculent une marque mise par l'élément congestionné comme c'est le cas avec la proposition *Explicit Congestion Notification* (ECN) [RFC3168]. Nous reviendrons sur cette proposition dans la sous-section 1.1.3. Lorsque le contrôleur déduit la présence de congestion il réduit le débit d'émission de la source. Le débit est contrôlé à l'aide d'une fenêtre appelée la fenêtre de congestion (*Congestion Window* (CWND) ω). Elle indique la quantité de données qui peut être émise sur un RTT. Autrement dit, elle indique combien de données non acquittées peut recevoir le canal de communication. Sa taille évolue dans le temps en fonction de l'état du réseau et selon une fonction de contrôle *Additive Increase and Multiplicative Decrease* (AIMD). La fenêtre d'émission utilisée par un émetteur TCP est le minimum entre la fenêtre de congestion et la fenêtre glissante du contrôle de flux. Le contrôle de congestion comporte deux phases distinctes [Gevros2001] :

— La première phase se nomme évitement de la congestion (*congestion avoidance*) et se situe autour du point d'inflexion de la figure 1.1.

— La seconde phase se nomme résolution de la congestion (*congestion recovery*). Elle se déclenche quand l'état du réseau se situe au delà du point d'inflexion.

Dans la phase de *congestion avoidance*, le contrôle de congestion de TCP utilise deux algorithmes : le démarrage en douceur (*slow-start* (SS)) et l'évitement de congestion (*congestion avoidance* (CA)). Au début de la connexion, TCP n'a aucune connaissance de l'état du réseau, autrement dit de l'état du canal de communication entre l'émetteur et le récepteur. TCP utilise l'algorithme du démarrage en douceur pour sonder le canal. L'objectif

est d'atteindre le point d'inflexion rapidement et sans risquer de congestionner le canal par des rafales. Pour cela, l'algorithme du démarrage en douceur va étaler sur plusieurs RTT la croissance de la taille fenêtre de congestion jusqu'à atteindre une estimation du point d'inflexion. Ainsi l'émetteur commence avec une fenêtre de congestion assez petite et l'ouvre au fur et à mesure et de plus en plus vite avec l'arrivée des acquittements. Plus précisément, le rythme de croissance de la taille de la fenêtre de congestion est sur le doublement tous les RTT. Quant la fenêtre de congestion atteint un certain seuil, noté *slow-start threshold* (ssthresh), le démarrage en douceur s'arrête et l'algorithme d'évitement de congestion est maintenant utilisé. Cet algorithme augmente linéairement et plus lentement que le démarrage en douceur la taille de la fenêtre de congestion. En l'absence d'indication explicite par le réseau du débit disponible sur le canal de communication, l'émetteur TCP continue de faire le sondage du canal et vérifie si le débit écoulé peut être encore augmenté. Pour l'auteur de [Sallantin2014], lorsque la connexion TCP utilise l'algorithme d'évitement de congestion, elle entre alors dans un état stable. Dans cet état, la connexion doit se dérouler avec un débit écoulé élevé. C'est une indication que le point d'inflexion est atteint.

La figure 1.3 donne une représentation simplifiée des états du contrôle de congestion de TCP. Elle indique que l'état stable peut être quitté si la connexion est libérée ou si il y a un événement de congestion. TCP assimile les pertes implicitement à un événement de congestion. L'événement de congestion fait basculer le contrôle de congestion de TCP dans la phase de résolution de la congestion. Dans cette phase, la reprise de la perte ou des pertes est effectuée et la taille de la fenêtre de congestion est diminuée et ceci afin de diminuer le débit d'émission.

On distingue deux façons de détecter un événement de congestion. Une méthode s'appuie sur la reprise de perte de TCP par retransmission des données perdues sur expiration d'un temporisateur (*Retransmission TimeOut* (RTO)). Une autre méthode utilise la caractéristique de TCP qui consiste à ce que le récepteur envoie un acquittement à chaque segment de données reçu en séquence. Ce segment porte le numéro des dernières données reçues séquentiellement. Ainsi, la réception de données entraînant une rupture de la numérotation en séquence génère l'émission d'un acquittement dupliqué (*Duplicate Acknowledgement* (DupAck)) par le récepteur. À la réception de trois DupAck par l'émetteur, les données indiquées par la rupture de séquencement sont considérées perdues et retransmises sans attendre l'expiration du RTO. Ce principe de retransmission rapide porte le nom de *fast retransmit* (FR). L'algorithme de récupération rapide (*fast recovery* (FR)) va maintenir la quantité de données en transit dans le canal de communication pour éviter l'émission d'une rafale lorsqu'un nouvel acquittement sera reçu. En l'absence du *fast recovery*, à la réception d'un nouvel acquittement, la fenêtre pourrait se vider par une rafale correspondant à des émissions de paquets de données dos à dos sur un débit supérieur à celui du débit d'écoulement du canal. Ceci aurait pour effet de saturer le canal et de renvoyer la connexion TCP dans une phase de résolution de la congestion.

Lorsque les émissions de l'émetteur sont bloquées par des données émises et jamais acquittées, le blocage est rompu par le RTO et ceci quel que soit l'état. Les détails de la mise en œuvre des algorithmes du contrôle de congestion TCP sont décrits par le [RFC5681].

Historiquement, la version dénommée TCP Tahoe incorporait la fonction de contrôle de congestion développée en 1888. Elle comportait les algorithmes de *slow-start*, *congestion avoidance* et de *fast retransmit* [Jacobson1988-1]. La reprise de perte par *fast retransmit* souffrait d'inefficacité, elle a été corrigée avec l'algorithme du *fast recovery*. Cette version à quatre algorithmes est la version connue sous le nom de Reno et publiée la première fois en 1997 par le [RFC2001]. Le couplage *fast retransmit - fast recovery* souffrait de défauts

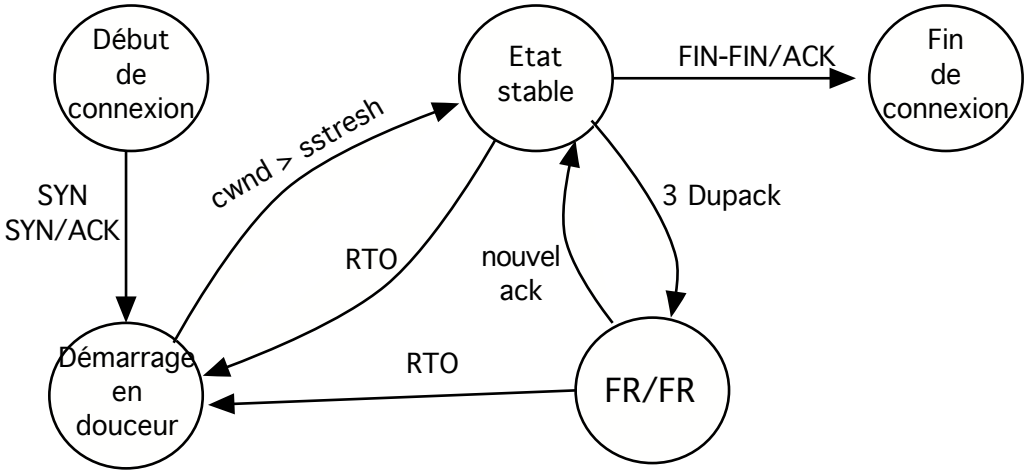


FIGURE 1.3 – Etats du contrôle de congestion de TCP.

lorsqu'un événement de congestion comportait plusieurs pertes. Le [RFC2582] apportait un correctif en 1999. On parla alors de version NewReno du contrôle de congestion. En 2005, une étude montra que c'était la version du contrôle de congestion de TCP la plus utilisée sur l'Internet [Medina2005]. Depuis, de nouvelles versions ont été déployées dans les systèmes d'exploitation tels que Windows et Linux appelés respectivement C-TCP [Tan2006] et CUBIC [Ha2008]. Dans la section 1.1.2, ces versions seront détaillées.

Le fonctionnement caractéristique du contrôle de congestion de TCP est illustré par la figure 1.4 extraite de [Huston2000]. Elle montre l'évolution de la fenêtre de congestion dans le temps (exprimée en terme de RTT) sur un canal de communication virtuel entre 2 stations. Il s'agit ici d'un scénario idéalisé dans lequel la connexion TCP n'est pas en concurrence avec d'autres connexions. La congestion se produit toujours à la même valeur de fenêtre et pour laquelle la file d'attente déborde. Cette figure montre les deux caractéristiques du contrôle de congestion de TCP qui découlent de la phase d'évitement de congestion et de résolution de la congestion et qui sont :

— L'agressivité, elle provient du sondage du canal de communication. L'émetteur TCP va chercher à accroître le débit écoulé en augmentant graduellement son débit d'émission par l'agrandissement de la taille de la fenêtre de congestion.

— La réactivité, lorsque le canal de communication est plein et qu'il déborde, quand cette perte est détectée, l'émetteur TCP réagit et diminue la taille de sa fenêtre afin de diminuer son débit d'émission.

Ces deux caractéristiques donnent cette figure en dents de scie de la fenêtre de congestion.

1.1.2 La problématique de l'utilisation d'un réseau à grande capacité de stockage

Un réseau à forte capacité de stockage est un réseau avec un produit délai-bande passante (*Bandwidth Delay Product* (BDP)) élevé. Dans l'ouvrage [Peterson2007], l'auteur effectue une analogie du produit délai-bande passante avec un tuyau. Le délai correspond à la longueur du tuyau et la bande passante au diamètre du tube. Ainsi le BDP est le volume du tube. Dans le cas d'un réseau informatique, le volume du tuyau s'exprime en bits. Ainsi, lorsqu'un canal de communication entre un émetteur et un récepteur présente un produit délai-bande passante important, un volume important de bits (autrement dit de données) peut être émis avant de recevoir une notification. Du point de vue

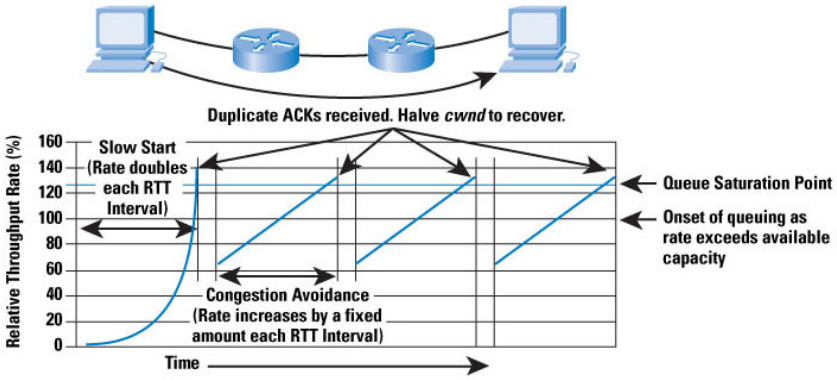


FIGURE 1.4 – Évolution caractéristique de la fenêtre de congestion de TCP.

de l'émetteur TCP, ce volume de données injecté dans le réseau sont des données non encore acquittées. Les réseaux qui offrent des canaux de communication avec un produit délai-bande passante important sont nommés en anglais *Long Fat Network* (LFN). Le [RFC1072] précise qu'un LFN à un produit délai-bande passante supérieur à $12,5$ Ko.

Sachant que le contrôle de congestion de TCP s'appuie sur une rétro-action selon une période de RTT et que le débit écoulé maximal est atteint lorsque la fenêtre d'émission est au moins supérieure au produit délai(RTT)-bande passante du canal de communication, l'utilisation de TCP sur un réseau LFN a des conséquences négatives sur la performance. Les causes sont à chercher du côté du RTT et du produit délai-bande passante qui prennent tous les deux des valeurs importantes.
Dans le cas du RTT, c'est le délai de réactivité de TCP qui est impacté. En effet quand le RTT est élevé, la dynamique de TCP est ralentie car l'émetteur TCP doit attendre plus longtemps pour recevoir un ACK et savoir quoi faire par la suite.

Pour ce qui concerne le produit délai-bande passante, c'est le débit écoulé qui peut être faible par rapport au débit du canal de communication (sa bande passante). La fenêtre d'émission de TCP n'atteint pas la valeur du produit délai-bande passante, l'émetteur se trouve alors bloqué en attente de l'ACK pour émettre de nouvelles données. Ces périodes de blocage concourent à faire chuter le taux d'utilisation du canal de communication.

Par la suite, nous allons détailler les conséquences de la faible réactivité et d'une fenêtre d'émission importante à atteindre sur l'efficacité de TCP. La problématique se pose en terme de démarrage de connexion et son implication pour le transfert des flots courts, de taille maximale possible de la fenêtre de congestion et de résolution de la congestion.

Le démarrage de connexion

Le début des connexions de TCP se fait à l'aide de l'algorithme du démarrage en douceur. Nous avons vu précédemment que ce mécanisme double la fenêtre de congestion en un RTT. Lorsque la fenêtre de congestion atteint la valeur seuil ssthresh, l'algorithme d'évitement de congestion est utilisé. La valeur initiale du seuil est fixée arbitrairement ce qui soumet TCP à deux problèmes. Le doublement de la fenêtre de congestion quand elle atteint des valeurs importantes constitue des incréments avec une granularité de plus en plus grosse. Si la valeur de ssthresh est trop grande par rapport au BDP, avec un gros incrément, le dépassement du BDP peut conduire à émettre trop de paquets, causant des pertes multiples induisant une augmentation de la latence et une réduction du débit écoulé. Dans le cas où la valeur du ssthresh est trop basse par rapport au BDP, la

connexion TCP va utiliser prématurément l'algorithme d'évitement de congestion avec une incrémentation linéaire. Ce changement prématuré aura pour conséquence une sous-utilisation de l'algorithme de démarrage en douceur, spécialement dans le cas où le BDP est très élevé. [Wang2004].

Le démarrage de connexion est particulièrement important pour les flots courts TCP (*short lived TCP flow*). Un flot court TCP se définit comme un flot dont la taille est inférieure ou égale à 10 segments TCP [Sallantin2014]. La problématique des flots courts provient du fait qu'ils n'ont pas assez de données pour quitter l'étape du démarrage en douceur. En effet, la taille de la fenêtre de congestion n'a pas le temps d'atteindre la valeur du produit délai-bande passante que la totalité des données ont été transmises. La conséquence est qu'ils ont fonctionné avec une fenêtre de congestion qui est restée relativement petite. Dans le cas, d'un LFN, le rapport de la taille de la fenêtre de congestion sur le produit délai-bande passante tend vers zéro et nécessite plusieurs RTT. Il s'ensuit que le débit écoulé est extrêmement faible. De plus si le flot court souffre d'un événement de congestion, il sera particulièrement pénalisé. Il a de fortes chances que la reprise s'effectue avec un RTO avec un délai maximum de 1 à 3 secondes [RFC6298]. Ce genre de flots n'a pas toujours assez de données émises après la perte pour générer trois DupAck et procéder à une reprise par *fast retransnmit*. Comme ces flots représentent, d'après [Ciullo2009], 90% des flux présents dans l'Internet, leur sous-performance sur les LFN est problématique.

La résolution de la congestion

TCP détecte une perte par l'expiration du RTO ou par la réception de trois DupAck. TCP va réagir en deux temps en renvoyant le paquet perdu et en divisant par deux la fenêtre de congestion. Si la taille de la fenêtre est importante, la division par deux va entraîner une chute significative de la capacité d'envoi. Par rapport au produit délai-bande passante, cette division par deux peut entraîner une sur-réaction de l'émetteur. Le débit écoulé après un événement de congestion peut devenir faible et se pose le problème de la dynamique de sondage.

Dynamique du sondage

TCP a un objectif de performance en terme de débit écoulé et d'utilisation des capacités de transmission du réseau. TCP possède un comportement conservateur. Avec la fonction de contrôle AIMD, TCP aura besoin d'un cycle égal à $\omega/2$ RTT pour récupérer une taille de fenêtre égale à celle avant réduction. Dans les réseaux à forte capacité de stockage, TCP tend à être trop prudent, à ouvrir sa fenêtre de congestion trop lentement. La capacité de stockage importante demande un nombre de cycles important pour que la fenêtre de congestion puisse couvrir le BDP. Durant ce temps, il est important de ne pas avoir de pertes. L'exemple donné par le [RFC3649] présente un réseau à une capacité de 10 Gbit/s, un délai de 100 ms et une taille de paquets d'un maximum de 1500 octets. Cela demanderait un échange d'une durée de deux heures environ. De plus, la totalité des paquets devront être transmis dans la durée indiquée précédemment. Le taux de perte maximal permettant l'usage de la totalité de la bande passante est de l'ordre de 10^{-10}. C'est un taux de perte irréaliste. Il faut donc appliquer une autre fonction de contrôle pour utiliser efficacement la capacité des liens et pour répondre rapidement aux changements d'états du réseau.

1.1.3 Un contrôle de congestion de TCP adapté aux LFN

Pour rappel, dans la partie 1.1.1, nous avons vu que le contrôle de congestion de TCP se découpait en deux phases. La première phase de *congestion avoidance* comporte les algorithmes de sondage alors que la seconde phase dite de *congestion recovery* comporte les algorithmes de résolution de la congestion. Nous présentons les propositions qui visent à changer le contrôle de congestion de TCP sur ces deux phases pour les adapter aux contraintes des LFN et donc traiter les problèmes que nous avons mis en évidence dans la sous-section 1.1.2. L'utilisation de TCP sur des réseaux à forte capacité de stockage a suscité des propositions qui sont classées dans le tableau 1.1. Ces propositions vont être détaillées dans la suite de ce manuscrit.

TABLE 1.1 – Tableau de synthèse des propositions.

Phase	Problème	Solutions
Congestion avoidance	Démarrage de connexion	Initial Spreading, Réduction du RTO, Quick-start, Jump Start,
Congestion recovery	Résolution de congestion	MulTCP
	Dynamique du sondage	HighSpeed TCP, C-TCP, BIC, CUBIC

Le démarrage de connexion

L'idée de la première solution est de réduire le nombre de cycles au démarrage d'un flot. Le doublement de la taille lorsque la fenêtre de congestion vaut 2 segments, par exemple, conduit à un incrément qui reste faible sur un RTT. Le principe de la première solution est d'augmenter la taille initiale de la fenêtre de congestion (*Initial Window* (IW)) [RFC6928]. Avec une taille initiale de fenêtre de congestion équivalent à 10 *Maximun Segment Size* (MSS), l'émetteur peut transmettre dès le début de connexion une rafale de 10 segments. Parmi les avantages de cette solution, on peut citer la réduction de la latence du transfert de données, en considérant que le canal ne sera pas congestionné. Un des inconvénients de cette solution est la possibilité de congestionner la file d'attente du goulot d'étranglement. Afin de résoudre ce problème, [Sallantin2014] propose l'*Initial Spreading*. Cette proposition combine l'augmentation de la fenêtre d'émission et le mécanisme d'espacement, mécanisme limitant la présence de rafales. Ces travaux ont fait l'objet d'une proposition auprès de l'*Internet Engineering Task Force* (IETF) [Arnal2014].

La détection d'une perte au départ du démarrage en douceur se fait à travers l'expiration du RTO, soit trois secondes. Pour améliorer la reprise sur erreur, le [RFC6298] propose de réduire la durée du RTO à une seconde. Cette réduction du RTO autorise une retransmission plus rapide des paquets perdus et apporte un gain relativement important pour des flots qui ont une latence très faible comme celle des flots courts.

Une autre solution, évaluée par [Scharf2008-1] et décrite par le [RFC4782], se nomme *Quick-start*. L'émetteur émet une requête contenant le débit d'émission qu'il souhaite utiliser. Chaque nœud traversé peut alors accepter, rejeter, ignorer ou modifier la requête en fonction de son débit disponible. Pour bien fonctionner, ce mécanisme de négociation nécessite que l'ensemble des routeurs traversés aient répondu à la requête. La figure 1.5 compare les performances du démarrage en douceur (en rouge) et de *Quick-start* sur un téléchargement vu depuis le serveur. Le serveur a émis deux requêtes : la première à un débit de 81.92 Mbit/s (en vert) et l'autre pour un débit d'une valeur de 5.12 Mbit/s (en

bleu). L'axe des abscisses représente la latence (durée de la connexion) depuis l'émission de la demande d'établissement de connexion et en ordonnée le débit d'émission. Les débits ont été calculés à partir de la quantité de données moyenne émises en un RTT. Les résultats montrent des performances supérieures de *Quick-start* par rapport au démarrage en douceur. En effet, une requête de *Quick-start* avec un débit suffisamment élevé permet d'atteindre rapidement l'utilisation maximale de la bande passante disponible. Le démarrage en douceur limite la croissance du débit d'émission. On remarque également, que si la valeur seuil du démarrage est trop basse, le débit d'émission croît beaucoup moins rapidement (lien en pointillé sur la figure 1.5). *Quick-start* reste performant sur les flots courts en appliquant un débit d'émission qui sera équivalent à un flot long.

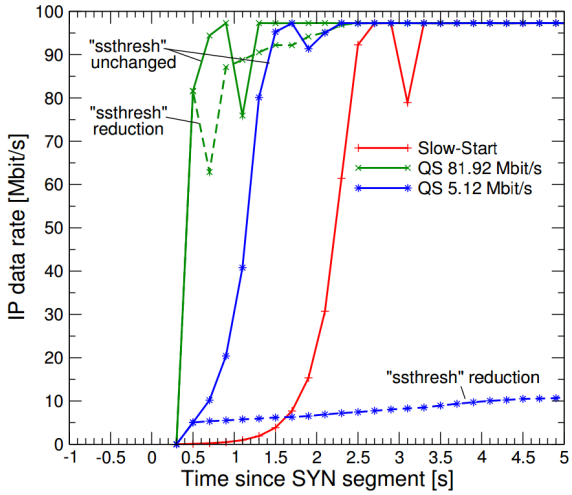


FIGURE 1.5 – Principe de Quick-Start. (Source : [Scharf2008-1]).

Dans l'article [Liu2007], l'auteur présente *Jump Start*. Cette proposition réalise une estimation des données prêtes à être envoyées ainsi que du RTT. L'objectif est d'émettre les segments de façon régulière en un RTT. Ce mécanisme s'avère trop agressif dans les environnements congestionnés. Le nombre de segments envoyés en un RTT peut être important et ainsi causer de sévères dégradations de performance.

La résolution de la congestion

Quand TCP a atteint l'état stable et qu'une perte est détectée, la fenêtre de congestion va être divisée par deux. Cette réduction diminuera le débit écoulé. Il est important pour TCP d'être réactif vis à vis des pertes. Pour cela, de nouveaux algorithmes doivent être mis en place dans la phase d'évitement de congestion. Ces algorithmes devront être réactifs aux pertes mais sans sur-réagir. Ces nouveautés doivent permettre de retrouver rapidement un débit écoulé important.

Lorsque plusieurs flux TCP empruntent une route congestionnée, ils sont soumis au même taux de pertes. Le but étant de répartir équitablement la bande passante disponible. Une approche de diminution moins agressive de la fenêtre de congestion consiste a réaliser des connexions TCP parallèles. L'objectif est d'avoir un flux TCP se comportant comme l'agrégation de plusieurs flux.

Dans l'article [Crowcroft1998], les auteurs proposent une version du contrôle de congestion de TCP qui se comporte d'une manière équivalente à N sessions TCP parallèles. Il s'agit de *MulTCP*. *MulTCP* génère un flux TCP unique où les sessions virtuelles sont réparties uniformément afin d'obtenir le résultat maximal en terme de débit. Le contrôle de congestion de TCP change lorsqu'il utilise l'algorithme d'évitement de congestion et qu'il

détecte un événement de congestion (par détection d'au moins une perte d'un segment dans une fenêtre de congestion). Les équations suivantes sont utilisées dans chacun des cas *MulTCP* :

$$\begin{aligned} ACK &: \omega \leftarrow \omega + \frac{N}{\omega} \\ DROP &: \omega \leftarrow \omega \times (1 - \frac{1}{2N}) \end{aligned} \tag{1.2}$$

En évitement de congestion, lorsqu'un ACK est reçu, *MulTCP* augmente sa fenêtre de congestion (ω) de N segments par RTT. Lors de la perte de segments (*DROP*), *MulTCP* réduit sa fenêtre de $\omega/(2N)$, plutôt que la valeur par défaut de $\omega/2$. La figure 1.6 montre l'évolution de la fenêtre de congestion de *MulTCP* par rapport à TCP. On voit sur la figure 1.6 que *MulTCP* a de meilleures performances qu'un flux TCP normal. Lorsque les performances sont combinées, le résultat est supérieur à un flux unique.

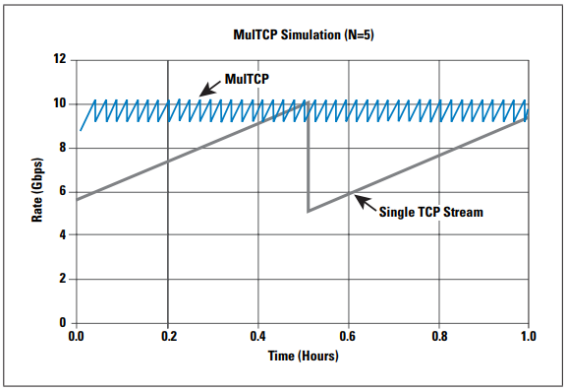


FIGURE 1.6 – Simulation de *MulTCP* avec N=5. (Source : [Huston2006]).

Dynamique du sondage

L'objectif de l'émetteur de TCP est d'envoyer le plus de données le plus vite possible. Mais à condition qu'elles arrivent sans produire de la congestion sinon, les données seront perdues et il faudra les ré-émettre. Il faut également tenir compte des autres flots, en partageant équitablement les ressources du réseau. Une approche pour traiter le problème de la dynamique du sondage consiste à changer la fonction de contrôle de TCP.

L'objectif de *HighSpeed-TCP (HS-TCP)* est d'atteindre les hauts débits en ayant des performances comparables à TCP classique dans les environnements à faible BDP [RFC3649]. La version du contrôle de congestion *HighSpeed-TCP* utilise le mécanisme d'*Additive Increase and Multiplicative Decrease* combiné à un facteur calculé en fonction de la taille de la fenêtre de congestion, tel qu'indiqué par les équations 1.3. En deça d'un certain seuil de ω, la réponse de *HighSpeed-TCP* est équivalente à TCP *Reno*. *HS-TCP* est limité durant la phase de démarrage en douceur. Durant cette phase, *HS-TCP* peut normalement envoyer un grand nombre de paquets. L'envoi d'un trop grand nombre de données risque d'occasionner de la congestion. Le [RFC3742] propose de limiter à 100 paquets la capacité d'envoi d'*HS-TCP* durant la phase de démarrage en douceur.

$$\begin{aligned} ACK &: \omega \leftarrow \omega + \frac{\alpha(\omega)}{\omega} \\ DROP &: \omega \leftarrow (1 - \beta(\omega)) \times \omega \end{aligned} \tag{1.3}$$

La figure 1.7 illustre le comportement de la fenêtre de congestion de *HighSpeed-TCP*. Lorsqu'une perte est détectée, la diminution de la fenêtre est moins importante grâce au facteur β. Le retour a la valeur précédente se fait beaucoup plus rapidement qu'avec *Reno* ou *NewReno* (en gris clair sur la figure) grâce au facteur α. Ainsi *HS-TCP* offre une meilleure utilisation de la capacité disponible sur le lien.

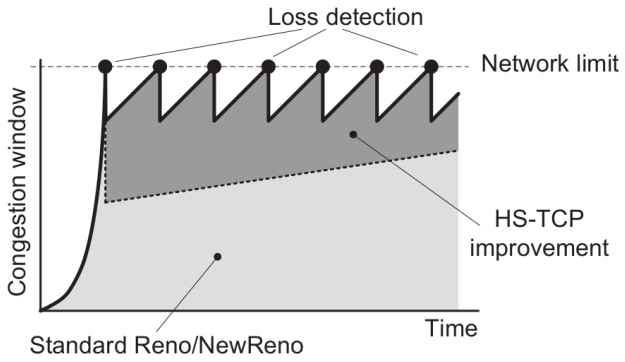


FIGURE 1.7 – Comportement de la fenêtre de congestion de *HighSpeed-TCP*. (Source : [Afanasyev2010]).

Dans [Tan2006], l'auteur propose une version de TCP alliant l'approche pro-active et réactive. Une approche pro-active utilise les variations du RTT pour estimer l'état du réseau. Alors qu'une approche réactive agit quand l'événement de congestion s'est produit. L'objectif est de maintenir de bonnes performances sur réseaux avec un haut débit et un grand RTT. *Compound-TCP (C-TCP)* maintient deux fenêtres de congestion. L'une croît de façon linéaire mais décroît via un certain coefficient en cas de perte. La seconde fenêtre est liée à l'approche pro-active de TCP-*Vegas* [Brakmo1994]. La taille de la fenêtre de congestion réellement utilisée est la somme des deux fenêtres. L'équation 1.4 illustre cette addition.

$$ACK : \omega \leftarrow \omega_{reno} + \omega_{fast} \tag{1.4}$$

Si le RTT est bas, alors la fenêtre ω_{fast} va croître rapidement. Si *C-TCP* rencontre une perte, alors ω_{reno} diminuera rapidement pour compenser l'augmentation précédente de ω_{fast}. Ce système cherche à garder une valeur constante de la fenêtre d'émission. *C-TCP* utilise efficacement des liens sur les réseaux à forte capacité de stockage. *C-TCP* est sujet au même défaut que TCP-*Vegas* sur l'exactitude des mesures RTT. Si les flux en concurrence les uns avec les autres dans le réseau observent des valeurs RTT minimales différentes, le flux se voyant un RTT plus élevé sera beaucoup plus agressif et injuste pour l'autre flux. La figure 1.8 illustre le fonctionnement de la fenêtre de congestion de *C-TCP*. La partie convexe de la courbe représente un fonctionnement plus proche de TCP *Reno*. Cela indique donc une valeur de ω_{fast} faible. Nous remarquons qu'après une perte, TCP essaye de récupérer rapidement la valeur précédente. Lors de pertes multiples, la fenêtre de congestion suit une forme proche à ce moment de la courbe de *HighSpeed*-TCP (voir figure 1.7). Ce comportement est la conséquence d'une valeur élevée de ω_{fast}. *C-TCP* permet ainsi d'atteindre le débit maximum disponible sur le lien tout en lissant sa capacité d'envoi en se basant sur le RTT. *C-TCP* est la version de TCP installée nativement sur le système d'exploitation *Windows* de Microsoft.

L'algorithme de contrôle de congestion de TCP connu sous le nom *Binary Increase Congestion control (BIC)* vise à une convergence rapide [Xu2004]. La fenêtre doit atteindre la taille maximale possible sans qu'il y ait de pertes. Pour cela, il met en œuvre une nouvelle fonction du contrôle de la taille de la fenêtre de congestion. La fonction de contrôle

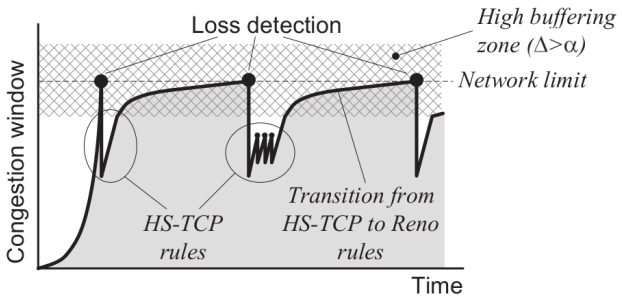


FIGURE 1.8 – Comportement de la fenêtre de congestion de *Compound-TCP*. (Source : [Afanasyev2010]).

de *BIC* est structurée en trois phases (*Additive Increase*, *Binary Search*, *Max Probing*), telles qu'illustrées par la figure 1.9a. Au démarrage de la connexion, BIC va incrémenter linéairement la fenêtre de congestion. C'est la phase d'*Additive Increase*.

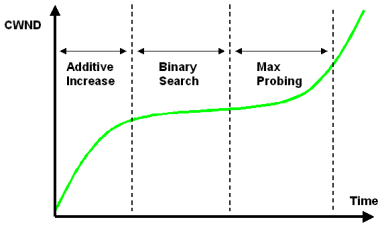
Durant la phase *Binary Search*, *BIC* va essayer de découvrir la taille optimale de la fenêtre de congestion. La taille optimale est la taille permettant d'émettre le maximum de données sans essuyer de pertes. Elle se base sur l'étude entre la valeur minimale (ω_{min}) et la valeur maximale (ω_{max}) de la fenêtre de congestion. Ces variables vont permettre d'affiner la valeur de la fenêtre de congestion. Au début de la connexion, ω_{min} est mise à 1 et ω_{max} est mis arbitrairement à une valeur élevée.

Lorsqu'une perte est détectée, la fenêtre de congestion va être réduite et prendre pour valeur la moyenne entre ω_{min} et ω_{max}. ω_{min} prend alors pour valeur la taille de la fenêtre de congestion après réduction et ω_{max} la valeur de la fenêtre de congestion avant la perte. Si l'écart entre la valeur de la fenêtre de congestion avant et après la perte est supérieur à une constante S_{max}, alors la fonction de contrôle de *BIC* entre en phase dite *Additive Increase*. Durant cette phase, S_{max} va servir de valeur d'incrémentation pour la fenêtre de congestion à chaque RTT. Par la suite, et si aucune perte n'est de nouveau détectée, la fonction de contrôle de *BIC* retourne en phase de *Binary Search*. L'objectif est de stabiliser la taille de la fenêtre aux alentours de la valeur de ω_{max} rencontrée avant la perte précédente.

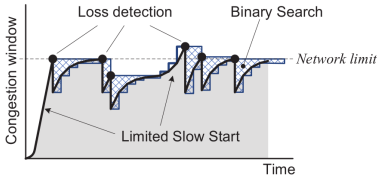
Lorsque cette valeur est dépassée, BIC entre dans la phase dite *Max Probing*. L'augmentation de la fenêtre de congestion est alors linéaire. L'objectif étant la recherche d'un nouvel ω_{max}. La figure 1.9b illustre le fonctionnement de la fenêtre de congestion dans le temps. Lors du début de connexion, *BIC* se comporte comme *Reno* avec le mécanisme du démarrage en douceur. Dès qu'une perte est détectée, la diminution de la fenêtre est alors moins agressive qu'avec *Reno*. Au centre de la courbe, nous remarquons la fonction d'accroissement avec les trois phases.

BIC est un contrôle de congestion performant dans les réseaux à forte capacité de stockage. Néanmoins, *BIC* peut être trop agressif pour les flux qui ont des courts délais. Cela a pour conséquence un partage inéquitable de la bande passante disponible avec les flux qui ont des longs délais.

Afin de résoudre le problème d'iniquité lié au RTT, l'algorithme *CUBIC* propose de changer la fonction de contrôle de la taille de la fenêtre de congestion pour la rendre plus agressive. La fonction retenue est cubique et son évolution est représentée par la figure 1.10a. Contrairement à la figure d'accroissement de *BIC* (fig. 1.9a) qui comporte trois phases, la fonction d'accroissement de *CUBIC* n'en compte que deux (fig. 1.10a). Sur la figure 1.10b, on constate que ces deux phases sont présentes tout au long de l'évolution de la fenêtre de congestion de *CUBIC*. Ces deux phases ne sont pas forcément consécutives l'une de l'autre. Après la détection d'une perte, *CUBIC* va essayer de croître le



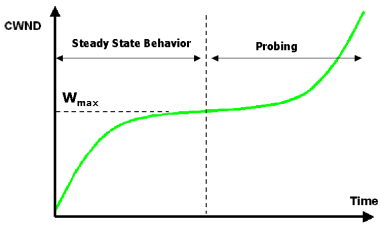
(a) Fonction d'accroissement de la fenêtre de congestion chez *BIC*-TCP. (Source : [NCSUNRL]).



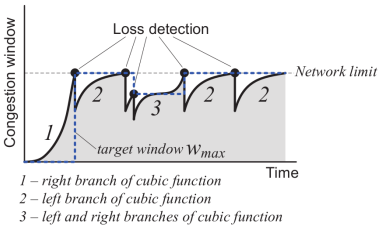
(b) Évolution de la fenêtre de congestion de *BIC*-TCP. (Source : [Afanasyev2010])

FIGURE 1.9 – Fonctionnement de BIC TCP.

plus rapidement possible jusqu'à ω_{Max}. Lorsque ω_{Max} est atteint, la taille de la fenêtre va s'incrémenter lentement. Mais plus la valeur d'ω est éloignée en taille de ω_{Max}, plus la croissance va s'accélérer. L'avantage de *CUBIC* sur *BIC* est le remplacement la fonction de contrôle linéaire par une fonction cubique pour plus d'agressivité. L'algorithme *CUBIC* est décrit par le [RFC8312].



(a) Fonction d'accroissement de la fenêtre de congestion chez *CUBIC*-TCP. (Source : [NCSUNRL]).



(b) Évolution de la fenêtre de congestion de *CUBIC*-TCP. (Source : [Afanasyev2010]).

FIGURE 1.10 – Fonctionnement de CUBIC.

1.1.4 Contrôle de congestion avec implication des routeurs

D'autres approches ont été étudiées pour aider le contrôle de congestion de TCP. Ces approches impliquent les routeurs et ne reposent plus que sur le principe de bout-en-bout propre à TCP.

Explicit Congestion Notification (ECN) vise à renforcer l'indication d'un événement de congestion [RFC3168]. Avec ECN, la congestion est signalée avant que la perte d'un paquet ne se produise. Lors de la réception d'un paquet indiquant une congestion, l'émetteur va alors réduire sa fenêtre de congestion et sa fenêtre d'émission. La réduction de la capacité d'émission de l'émetteur évitera pertes et retransmissions et une réduction des délais de reprise. L'usage de cette option nécessite que l'émetteur, le récepteur et les routeurs du chemin soient capables de gérer les notifications explicites. Avec ECN, l'information de congestion est transmise à l'émetteur. Aucune indication sur le lieu précis de la congestion est indiquée.

eXplicit Control Protocol (XCP) est un protocole de contrôle de congestion utilisant les notifications explicites de débit [Katabi2002]. En cela, il reprend l'idée de *Quick-start*. Cependant il se différencie par le découplage opéré entre la problématique du partage équitable entre les flots, et celle de l'efficacité du transfert. Dans l'architecture de protocoles, *XCP* se situe entre TCP et IP. *XCP* repose sur un en-tête qui va servir aux routeurs

traversés pour indiquer le débit d'émission pour le flot. La valeur d'adaptation de la fenêtre de congestion est calculée à partir des informations contenues dans l'en-tête *XCP*. *XCP* propose un contrôle de congestion qui fonctionne sur un réseau 100% *XCP*. Une seconde limite est l'iniquité avec les autres protocoles de transport. Les performances sont fortement dégradées si différents protocoles de bout en bout sont exécutés dans le même réseau, tels que TCP. *XCP* possède de mauvaises performances si des routeurs IP classiques (non-*XCP*) se trouvent au niveau du goulot d'étranglement.

Afin de résoudre le problème d'interopérabilité, Dans [Lopez2006], l'auteur propose *XCP-interoperable (XCP-i)*, une version *XCP* qui garde les mécanismes de contrôle *XCP* sans ajouter d'état de flux. L'objectif d'*XCP-i* est de déployer *XCP* sur un réseau comprenant des routeurs XCP et non-XCP. Pour cela, *XCP-i* va fonctionner en deux phases. Dans une première phase, il va découvrir les nuages non-*XCP*. Un nuage non-XCP est un ensemble de routeurs non capables de traiter XCP. En comparant les champs *Time-To-Live* (TTL) d'IP et d'*XCP*, le nombre de routeurs non-*XCP* présents dans le réseau peut être déduit. La seconde phase consiste à déterminer les ressources du nuage non-*XCP*. En rajoutant un champ *last_xcp_routeur*, *XCP-i* garde en mémoire l'adresse du dernier routeur *XCP* traversé. À partir d'algorithmes d'estimation de bande passante, la bande passante du nuage non-*XCP* sera estimée entre les deux nœuds *XCP*. La dernière phase pour réaliser une inter-opérabilité complète entre routeurs classiques et routeurs *XCP*, consiste à prendre en considération la bande passante estimée dans les calculs du feedback de *XCP*. Le protocole *XCP-i* va créer un routeur *XCP* virtuel à la place du nuage non-*XCP*. Grâce a ces mécanismes, un réseau hétérogène devient virtuellement homogène pour *XCP*. Les performances de *XCP-i* sont comparables à celle de *XCP* [Lopez2006]. *XCP-i* résout le problème d'inter-opérabilité de *XCP* sur des réseaux non 100% *XCP*.

Ces solutions présentent le désavantage de devoir être déployées également au sein des routeurs. Le principal avantage de ces solutions est une indépendance au délai. Les problématiques liées au délai, que l'on a présentées précédemment, sont alors inopérantes. Dans le cadre de La Réunion, les délais peuvent être importants.

1.1.5 Caractérisation de La Réunion

L'augmentation des débits d'accès s'accompagne de l'augmentation de la capacité des liens d'interconnexion, comme celles des câbles sous-marins. Malgré cette augmentation des débits, le temps de propagation reste inchangé. Dans cette partie, nous déterminons à partir de quel débit un accès Internet à La Réunion peut être sujet aux problèmes rencontrés sur les LFN.

Dans la section 2.1, nous avons vu que La Réunion est raccordée à Internet par deux accès reposant sur des câbles sous-marins, le SAFE et le LION. Le câble SAFE est prolongé par le câble SAT-3/WASC. Le temps de propagation (t_p) sur un câble peut être estimé par la formule mathématique 1.5 dans laquelle d représente la distance et c la vitesse de propagation du signal sur le support.

$$t_p = \frac{d}{c} \tag{1.5}$$

Si nous retenons la route directe entre La Réunion et la France hexagonale qui passe par le plus long des accès constitué par les câbles SAFE et SAT-3/WASC. Sachant que le câble SAFE a une longueur totale de $13\,500$ km pour aller de l'Afrique du Sud à l'Asie. Si on fait l'hypothèse que l'île de La Réunion se situe à une distance équivalente à la moitié du câble SAFE. La longueur du câble pour La Réunion est de $6\,750$ Km. La vitesse de

propagation du signal pour une fibre optique est égale à la vitesse de la lumière (299 792 Km/s). L'application de la formule 1.5 donne t_{p1} avec

$$t_{p1} = 1/2 \times d_{SAFE}/c = 22,52ms \tag{1.6}$$

t_{p1} approxime le temps de propagation entre La Réunion et le point de sortie du câble SAFE, en Afrique du Sud ou en Asie. Pour obtenir le RTT, ce temps est à doubler. On obtient alors la valeur $RTT_1 = 45,04$ ms.

La seconde partie du trajet de l'Afrique du Sud jusqu'en Europe emprunte le câble SAT-3/WASC. D'après [Cablesmap], la longueur du câble est de 14 350 Km. Le temps de propagation entre l'Afrique du Sud et l'Europe noté t_{p2} s'exprime comme :

$$t_{p2} = (d_{SAT-3/WASC})/c = 47,87ms \tag{1.7}$$

Le RTT sur ce câble est de $RTT_2 = 95,74$ ms.
Au total, le RTT incompressible pour joindre l'Europe en passant par les câbles SAFE/SAT-3/WASC consiste à additionner le RTT de chaque câble, à savoir RTT_1 et RTT_2. Le RTT incompressible est donc minimal de $140,78\ ms$. Ce délai comme nous venons de le calculer ne prend en compte que la propagation. Il néglige le temps de transmission du paquet ainsi que les temps d'attente avant la transmission.

L'étude présentée dans[Anelli2012] a mesuré un RTT minimal pour les paquets quittant l'île de La Réunion de 185 ms. Ce résultat a été obtenu par une étude de mesures depuis les locaux de l'Université de La Réunion. La figure 1.11 représente la *Probability Density Function* (PDF) des RTT mesurés. Cette fonction est comparée à celle qui est obtenue depuis la France hexagonale et de Paris en particulier. On constate une forte similitude sur la forme des courbes. La courbe de La Réunion enregistre un décalage dans le temps de 185 ms par rapport à celle de Paris. Ce décalage représente le RTT minimum mesuré pour rejoindre la métropole et accéder à l'Internet.

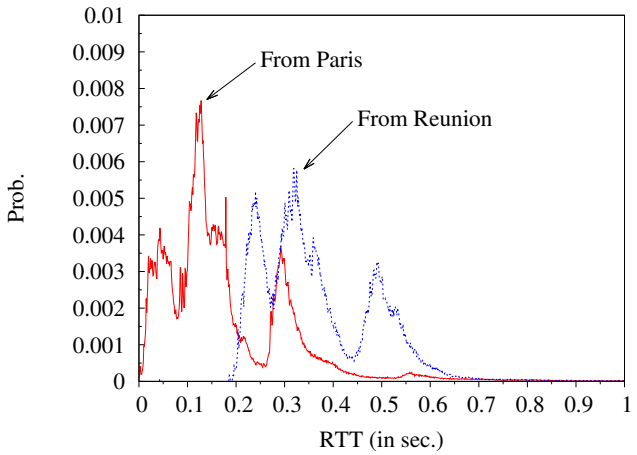


FIGURE 1.11 – Répartition des délais depuis Paris et l'île de La Réunion. (Source : [Anelli2012]).

Si l'on considère la valeur de BDP de 12, 5 Ko indiquée par le [RFC1072] comme la limite basse d'un LFN, et si nous reprenons les différentes TAI présentées dans la section 2.1, nous pouvons calculer le produit délai-bande passante d'un canal de communication entre La Réunion et la métropole. Il est fait l'hypothèse pour ce calcul que le goulot d'étranglement est donné par l'accès à Internet. Le tableau 1.2 présente les résultats obtenus.

TABLE 1.2 – Approximation du produit délai bande passante de la connectivité de La Réunion à l'Internet.

Nom	RTT (en secondes) / Bande passante	Estimé : 0,141	Mesuré : 0,185
Modem	56 Kbit/s	987 o	1,30 Ko
	128 Kbit/s	2,26 Ko	2,96 Ko
	512 Kbit/s	9,02 Ko	11,8 Ko
ADSL	1 Mbit/s	**17,6 Ko**	**23,1 Ko**
	8 Mbit/s	**141 Ko**	**185 Ko**
	20 Mbit/s	**353 Ko**	**463 Ko**
VDSL	50 Mbit/s	**881 Ko**	**1,16 Mo**
Fibre	35 Mbit/s	**617 Ko**	**809 Ko**
	100 Mbit/s	**1,76 Mo**	**2,31 Mo**
	200 Mbit/s	**3,53 Mo**	**4,63 Mo**
	1 Gbit/s	**17,6 Mo**	**23,1 Mo**

Le tableau présente en gras les produits délai-bande passante dépassant la limite des $12,5$ Ko. Ainsi les résultats sont assez éloquents. Dès que l'on arrive sur un accès ADSL, avec un débit minimal d'1 Mbit/s, nous avons un BDP supérieur à la limite fixée par le [RFC1072]. Ainsi, rapidement l'évolution des débits proposés sur l'île et les capacités des câbles sous-marins associés à un délai élevé ont fait de l'Internet réunionnais un réseau qui a les caractéristiques d'un LFN.

Nous avons vu que TCP est un protocole de transport dont la performance est dépendante du RTT et du BDP. Les délais sont une des caractéristiques des LFN. La Réunion est un réseau à forte capacité de stockage due à des délais importants. Il est important de mesurer pour comprendre l'impact de cette caractérisation sur les performances de TCP.

1.2 Métrologie du trafic Internet

Avec l'Internet qui devient de plus en plus gros et de plus en plus complexe, la métrologie est une activité qui vise à mieux comprendre le fonctionnement de l'Internet. Nous allons dans cette partie du manuscrit présenter les techniques de métrologie appliquées à l'Internet.

1.2.1 Définition

Métrologie est un mot composé de deux termes grecs. Le premier *metron* signifie la mesure, tandis que *logos* fait référence à la science. Par définition, la métrologie désigne *la science de la mesure*. Par la suite, le terme métrologie fera uniquement référence à la métrologie appliquée aux réseaux informatiques.
La métrologie signifie donc la mesure des caractéristiques d'un réseau sous de nombreux aspects. Cette science est devenue un outil indispensable pour avoir une compréhension de divers aspects de l'Internet. On peut citer la complexité, la qualité de service et la qualité utilisateur, la performance du réseau, la performance des protocoles, le fonctionnement ou encore la validation des modèles.
La métrologie Internet englobe deux types d'activités. La première est l'étude des paramètres physiques de la qualité de service. La seconde consiste a mettre en évidence les problèmes liés à l'Internet [Larrieu2010].

Dans [Paxson2001], l'auteur présente l'approche *research driven* et l'approche *measurement driven* pour définir les objectifs d'une étude de métrologie. Le choix d'une approche va aider une personne souhaitant faire de la métrologie sur la bonne façon d'aborder l'étude qu'elle veut mettre en place.

L'expression *research driven* peut être traduite par "axée sur la recherche". Elle consiste à définir, en premier lieu, les métriques recherchées avant de mettre en place l'infrastructure et les outils nécessaires, de lancer les campagnes de mesures et d'interpréter les résultats. Une métrique se définit comme une grandeur mesurable et spécifiée de manière rigoureuse. Une bonne métrique doit pouvoir se mesurer de façon reproductible, être utile en pratique pour les utilisateurs et les administrateurs du réseau [RFC2330]. Cette approche est celle généralement utilisée par les opérateurs et les groupes de recherches. Elle est développée par le groupe de travail *IP Performance Metrics* (IPPM) de l'IETF. Ce groupe de travail a produit de nombreux documents pour définir les mesures de performances L'approche *research driven* comporte un défaut principal. En laissant de côté certaines métriques, des aspects du comportement du réseau ne sont pas étudiés. Par exemple, une étude restreinte aux délais ne peut indiquer les raisons de la variation des délais dans le temps.

L'approche *measurement driven* peut se traduire en "la mesure pour la mesure". Cette méthode consiste à mettre en place une infrastructure de mesures afin de récupérer le maximum d'informations, puis effectuer toutes les analyses possibles sur les traces collectées et interpréter les résultats obtenus. Une telle méthode peut s'utiliser lorsque l'on souhaite mettre en avant le comportement général d'un lien. Cette approche permet, à la différence de la précédente, d'analyser à plusieurs reprises une même source de données, en fonction des résultats obtenus.

Le tableau 1.3 résume les deux approches de conduite de projet en métrologie.

TABLE 1.3 – Comparatif entre les approches de métrologie.

Research Driven	*Measurement Driven*
1 - Métriques définies préalablement	1 - Collecte des données
2 - Utilisation d'un outil adapté	2 - Analyse exhaustive

Ces deux approches sont complémentaires l'une de l'autre et s'appliquent dans les deux classes de techniques de mesures : les techniques de mesures actives et les techniques de mesures passives.

1.2.2 Métrologie active

La métrologie active consiste à injecter un trafic spécifique et à mesurer en réception l'effet sur le réseau à étudier. L'hypothèse faite par la métrologie active est que la mesure faite de bout en bout est révélatrice de la performance du service du réseau telle qu'elle peut être perçue par une application. Les paquets émis sont des sondes qui en empruntant la route entre la source et la destination expérimentent la performance du canal de communication. Il convient de limiter le trafic des sondes afin qu'il ne vienne pas perturber le trafic et donc fausser la mesure. Les métriques mesurées par les mesures actives sont généralement des métriques associées à la topologie du réseau ou au trafic comme les routes ou les délais. Dans le cas de la métrologie active, il se peut que l'émetteur soit également le collecteur. La figure 1.12 illustre ce principe.

La métrologie active est opérée à l'aide d'outils spécifiques de génération et de collecte de sondes. Le tableau 1.4 indique les métriques obtenues avec les outils de métrologie présentés par la suite.

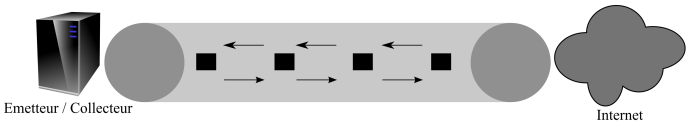


FIGURE 1.12 – Principe de la métrologie active.

TABLE 1.4 – Classement des outils.

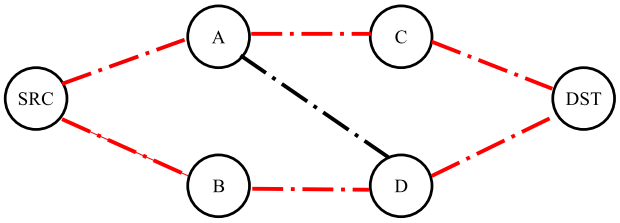
Métriques / Outil	RTT	Routes	Débits
Ping	X		
Traceroute	X	X	
Paris Traceroute	X	X	
Reverse-traceroute	X	X	
TraceIXroute	X	X	
Pathchar			X
Clink			X
Iperf			X

La mesure du RTT est généralement obtenue par l'outil ping *(Packet Internet Groper)*. Cet outil se présente sous la forme d'une commande dans un système de type Unix. Elle sert en premier lieu à vérifier la connectivité à Internet et l'accessibilité d'un nœud. En second lieu avec cette vérification, le RTT et la longueur de la route exprimée en nombre de sauts sont déterminés. Elle utilise le protocole *Internet Control Message Protocol* (ICMP) pour effectuer la mesure. Un message *ICMP Echo request* est émis. Le destinataire renvoie à l'émetteur un message *ICMP Echo reply*. La période qui sépare l'émission de la réception du coté émetteur est mesurée.

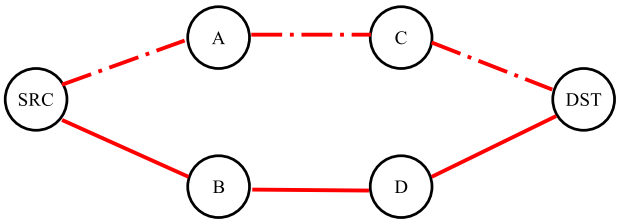
Pour en savoir plus sur la connectivité d'un nœud et notamment sur la route empruntée pour atteindre une destination donnée, l'outil traceroute offre le moyen de cette découverte [Jacobson1989-1]. Cet outil se présente, comme pour ping, sous la forme d'une commande de type Unix. Son principe de fonctionnement est basé sur un envoi successif de messages avec un champ TTL du paquet IP qui va croissant. Le routeur qui reçoit un message dont le TTL du paquet a atteint la valeur zéro envoie un message ICMP *Time Exceeded* pour reporter l'erreur à l'émetteur. Par ce message, il indique en adresse source l'adresse IP de son interface qui a rejeté le paquet. Ainsi, si un paquet ayant un TTL positionné à n est envoyé vers une destination donnée, le routeur situé à n sauts de la source va faire connaître son adresse IP et ceci tant que le chemin vers la destination est supérieur à n sauts [Crovella2006]. Le résultat est l'ensemble des nœuds traversés répondant au protocole ICMP. De nouveaux outils utilisant le principe de traceroute furent développés pour répondre à d'autres problématiques, comme la présence des points d'échange ou encore l'asymétrie des liens.

La réponse affichée par la commande traceroute n'est pas la seule route existante. En exécutant à plusieurs reprises la même commande traceroute, les réponses obtenues peuvent être différentes. A cause de l'équilibrage de charge (*load-balancing*), la sortie d'un routeur ne sera pas toujours la même. L'équilibrage des charges sert à répartir le trafic sur différents liens. Ainsi il est possible que deux paquets provenant de la même source vers la même destination n'empruntent pas la même route. Sur la figure 1.13, les liens physiques entre les différents nœuds sont indiqués en rouge. Les traits en pointillé représentent le chemin emprunté par les messages ICMP envoyés par la source. La figure 1.13a montre le résultat trouvé par traceroute. La route empruntée est $\{SRC,\ A,\ D,\ DST\}$.

Traceroute va envoyer 3 paquets avec un champ TTL égal à 2. Dans le cas de cet exemple, l'ensemble des paquets est dirigé vers B. Ainsi, malgré l'absence de liaison physique directe entre les nœuds A et D, traceroute nous indique la présence d'une route entre ceux deux équipements. L'outil Paris-traceroute vise à traiter ce problème [Augustin2006]. La figure 1.13b montre la route découverte par Paris-traceroute. La route affichée est $\{SRC,\ A,\ C,\ DST\}$. On remarque que la route obtenue existe physiquement. Pour obtenir ce résultat, Paris-traceroute change le numéro d'identification du flux à l'émission des paquets ICMP. Cette modification oblige les routeurs à suivre une seule et unique route. Paris-traceroute autorise également l'affichage des numéros de voies logiques MPLS.



(a) Traceroute.



(b) Paris-traceroute.

FIGURE 1.13 – Illustration du phénomène d'équilibrage des charges.

MultiProtocol Label Switch (MPLS) est un mécanisme de commutation rapide de paquets, fondé sur des adresses de format fixe et sans structure hiérarchique [RFC3031]. Ces adresses sont des numéros de voies logiques appelées des étiquettes ou *labels* (par anglicisme). Dans le cas de l'utilisation de traceroute avec MPLS, il faut que le routeur MPLS puisse envoyer un message ICMP. Le [RFC4950] documente une simple extension à ICMP pour retourner de l'information spécifique à MPLS autrement dit pour qu'un routeur MPLS puisse indiquer des informations spécifiques à MPLS dans le paquet ICMP émis en cas de problème. [Donnet2012] a étudié les possibilités offertes par des routeurs MPLS.

Dans les *explicit tunnels*, la structure interne du tunnel est entièrement visible et chaque nœud dans le *Label Switched Path* (LSP) est marqué comme nœud MPLS. Dans ce type de tunnel, le champ *ttl-propagate* qui est dans l'en-tête MPLS des paquets et le [RFC4950] sont appliqués. Cela signifie que le champ TTL du datagramme IP est décrémenté à chaque routeur rencontré.
Dans les *implicit tunnels*, le LER d'entrée active l'option *ttl-propagate*, mais les LSR n'implémentent pas le [RFC4950]. La décrémentation du TTL est effective mais aucune information de routeur MPLS n'est visible.
Dans les *opaque tunnels*, c'est l'inverse de l'*implicit tunnels*. Les routeurs implémentent le [RFC4950]. Le nœud d'entrée n'active pas l'option *ttl-propagate*. Le TTL est alors décrémenté à la sortie du tunnel MPLS. Le paquet ICMP-reply indique quand même l'existence d'un tunnel MPLS.
Pour les *invisible tunnels*, le LER d'entrée n'active pas l'option *ttl-propagate*. Dans ce cas, le TTL est décrémenté uniquement lors du dernier routeur du tunnel. Le [RFC4950] n'est pas implémenté par le dernier routeur du LSP. Cela implique l'absence d'information

sur le mécanisme MPLS au sein des paquets ICMP. On n'a alors pas d'informations sur l'existence d'un tunnel ICMP sur la route empruntée.

Avec l'acheminement avec MPLS des mauvaises valeurs de TTL peuvent être obtenues à cause du type de tunnel mis en œuvre. Il est donc important que le [RFC4950] soit implémenté dans les routeurs.

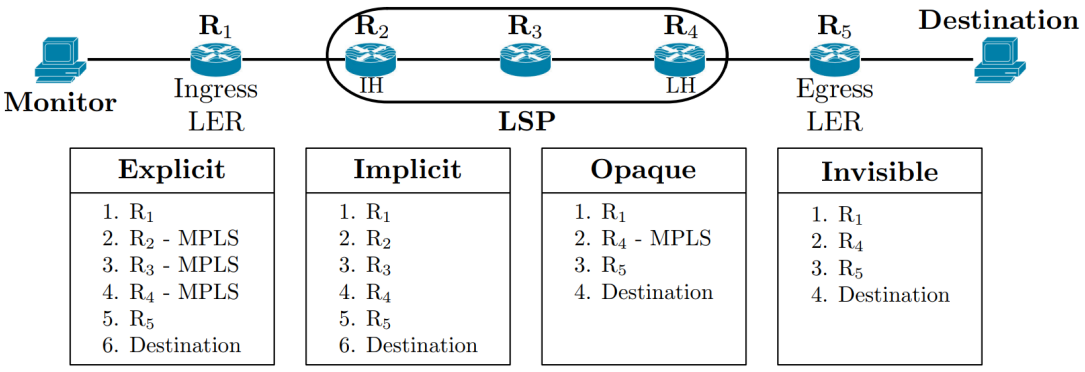


FIGURE 1.14 – Taxonomie des configurations de tunnels MPLS et des comportements de *traceroute* correspondants. (Source : [Donnet2012].)

Paris-traceroute propose l'affichage des informations MPLS lorsque celles-ci sont disponibles [Augustin2007]. La texte ci-dessous illustre les résultats obtenus par Paris-traceroute sur un *Explicit tunnel*. On y voit l'affichage des marques MPLS avec le TTL associé à chaque nœud.

```
traceroute [(41.213.141.35:33456) -> (81.82.166.157:33457)],
protocol icmp, algo hopbyhop, duration 3 s
 1 41.213.141.33 23.266 ms 2.542 ms 3.696 ms
 2 41.213.133.97 6.811 ms 5.613 ms 4.635 ms
 3 10.32.2.161 5.779 ms 6.841 ms 4.073 ms
  MPLS Label 16445 TTL=1 | 212996
 4 10.32.2.37 2.223 ms 2.249 ms 2.264 ms
  MPLS Label 16386 TTL=2 | 212996
 5 41.213.128.50 2.185 ms 2.245 ms 2.097 ms
  MPLS Label 16442 TTL=3 | 212996
 6 10.32.2.193 3.551 ms 9.330 ms 7.775 ms
 7 41.213.133.158 2.337 ms 3.088 ms 2.250 ms
 8 41.213.128.54 195.439 ms 195.555 ms 195.512 ms
 9 213.242.121.233 211.737 ms 211.724 ms 212.013 ms
10 4.69.148.181 234.190 ms 234.271 ms 234.323 ms
11 4.68.72.22 236.854 ms 236.798 ms 237.063 ms
12 213.224.250.110 237.108 ms !T0 236.580 ms !T0 236.570 ms
!T0
13 213.224.250.2 237.213 ms 236.631 ms 236.694 ms
14 213.224.201.252 239.100 ms 239.461 ms 238.680 ms
15 81.82.166.157 250.874 ms 249.608 ms 248.057 ms
```

Avec traIXroute l'objectif est de découvrir les différents points de *peering* (IXP) sur un chemin vers une destination [Nomikos2016]. Pour l'identification des nœuds d'échange, cette version de traceroute combine deux bases de données complémentaires qui sont PeeringDB [PeeringDB] et Packet Clearing House [PCH]. Avec une géolocalisation des adresses retournées, la liste des pays traversés peut être établie.

D'après [Steenbergen2009], « l'outil de dépannage numéro 1 pour vérifier la connectivité d'un nœud reste traceroute » pour les administrateurs réseaux mais « les liens asymétriques sont les fléaux numéro un de l'outil » car « le chemin de retour est entièrement masqué. » Afin de corriger cela, l'outil reverse-traceroute propose d'obtenir une route non pas entre la source et la destination mais entre la destination et la source [Katz2010], pour cela l'outil va utiliser l'enregistrement des adresses IP des routeurs sur le chemin du retour à l'aide des options d'en-tête *Record-Route* et *Timestamp* d'IP,

Pour déterminer le débit pathchar [Jacobson1997] vise à donner le débit saut par saut vers une destination. Aussi il reprend le principe de traceroute en émettant des sondes avec le champ TTL avec une valeur croissante. Lorsqu'il injecte le trafic de sondes vers un nœud du chemin il le fait avec des paquets de taille variable. Ainsi pathchar détermine la bande passante disponible entre chaque nœud rencontré.

L'outil Clink [Downey1999] est similaire à pathchar. La différence se fait au niveau sur le nombre de paquets envoyés. Clink envoie un nombre de paquets plus important que Pathchar. Ainsi les mesures réalisées par Clink auront une meilleure précision.

Iperf [Tirumala2005] est un outil pour mesurer la bande passante et la qualité d'un lien réseau. Ce dernier est délimité par deux machines sur lesquelles est installé Iperf. Une machine tient le rôle de serveur tandis que la seconde machine sera paramétrée comme client.

Pour des mesures plus représentatives, il est nécessaire d'augmenter les points de collectes. Des outils de métrologie active ont été conçus pour être répartis sur plusieurs nœuds. Ces outils se présentent sous la forme de plates-formes de métrologie active déployées à travers le monde. De nos jours, on compte de nombreuses plates-formes de métrologie active. Comme chaque plate-forme a un objectif précis et pour identifier la plate-forme appropriée pour réaliser une étude précise, l'auteur de [Bajpai2015-1] effectue une comparaison des différentes plates-formes selon 5 critères qui sont :

1. l'échelle, la couverture et la durée de vie de la plate-forme ;
2. le matériel physique utilisé pour la sonde ;
3. les métriques disponibles ;
4. l'architecture de mesure de la plate-forme ;
5. l'impact de son utilisation pour la recherche.

De cette comparaison, nous avons gardé 4 plates-formes que sont Atlas RIPE NCC, BISMark, DASU, SamKnows. Ces plates-formes ont été gardées car elles autorisent l'étude des performances des réseaux d'accès. Nous y avons ajouté les plates-formes Archipelago et Planet-Lab. Ces deux plates-formes ne font pas partie du document d'origine mais font l'objet d'une utilisation par de nombreux participants, tel que l'indique le nombre de sondes actives de ces deux plates-formes.

En 2007, le CAIDA a déployé sa propre plate-forme de mesures [Archipelago]. A travers le deployement de nœuds (des sondes dans le vocabulaire de Archipelago) sur l'ensemble de la planète, l'objectif est d'offrir des accès pour effectuer des mesures avec des outils tels que ping et traceroute. Archipelago est composée, à la date du 1^{er} Mars 2017, de 170 sondes réparties dans 59 pays et sur tous les continents.

Dans le courant de l'année 2010, le *Regional Internet Registry* (RIR) européen RIPE NCC a démarré la distribution de sondes pour la création de la plate-forme Atlas [Ripe2010]. Cette plate-forme vise à créer un réseau de sondes pour l'étude de la connectivité de l'Internet. Composée actuellement de près de $10\,000$ sondes réparties à travers le monde, elle est capable d'effectuer des tests de métrologie active autour des commandes ping, DNS, HTTP, NTP, traceroute et Paris-traceroute.

À l'initiative de Georgia Tech, la plate-forme *Broadband Internet Service Benchmark (BISMark)* a vu le jour en 2010. L'objectif est la réalisation d'un état des lieux des performances des accès Internet [Sundaresan2011]. La plate-forme est composée de 405 routeurs instrumentés avec OpenWrt. « Le projet OpenWrt est un système d'exploitation Linux ciblant les appareils embarqués. OpenWrt fournit un système de fichiers entièrement inscriptible avec gestion des modules d'installation de logiciels. Cela libère la sélection et la configuration des applications fournies par le fournisseur et permet de personnaliser l'appareil grâce à l'utilisation de progiciels adaptés à n'importe quelle application » [OpenWrt]. Les sondes sont distribuées dans 34 pays à travers le monde.

DASU est un utilitaire développé en 2010 à l'Université de Northwestern. Le logiciel couple métrologie active et passive avec pour objectif de caractériser les performances des utilisateurs. L'outil fut développé comme une extension d'un logiciel *peer-to-peer*, BitTorrent [Sanchez2013]. Depuis Juillet 2010, plus de 90 000 personnes, réparties à travers 147 pays, utilisent DASU.

En 2003, des chercheurs américains ont déployé une plate-forme de test, Planet-Lab [Chun2003]. En 2008, une extension européenne [PlanetLabEurope] a vu le jour. Planet-Lab dépasse le seul objectif de métrologie, elle vise aussi de tester des nouveaux services de communication en situation réelle. Les nœuds Planet-Lab ont pour *Operating System* (OS) Fedora. Il est possible d'installer n'importe quel logiciel, du moment qu'il est compatible avec cet OS. Avec une certaine liberté, il est possible d'effectuer des tests et des mesures depuis 425 sites répartis sur tous les continents.

La plate-forme SamKnows a vu le jour en 2008 [SamKnows]. SamKnows sert à l'étude des performances des connexions des particuliers et des entreprises. Elle est composée de près de 440 000 sondes. Cette infrastructure est partenaire de 36 *Fournisseurs d'Accès Internet* (FAI) de tous les continents.

Le tableau 1.5 résume les possibilités offertes par les plates-formes. La colonne *Impact sur la recherche* est déterminée à partir du nombre de citations par des articles scientifiques suivis par le site *Google Scholar*.

La plate-forme de mesures Atlas RIPE NCC [Ripe2010] a été utilisée dans le contexte insulaire de Cuba. Dans l'article [Bischof2015], l'auteur cherche à caractériser l'accès Internet cubain. Dans ses résultats, l'auteur a montré une forte asymétrie des routes internationales pour le trafic cubain. D'un point de vue de la topologie physique, cette île possède une connectivité qui peut par certains aspects ressembler à de celle de l'île de La Réunion.

L'île de La Réunion bien que Française est rattachée administrativement au RIR de la zone Afrique (AfriNIC). L'AfriNIC est le dernier RIR créé et les études de métrologie concernant cette zone sont peu nombreuses. Nous pouvons citer [Gupta2014] qui se penche sur l'interconnexion des FAI sur le continent africain. Cette étude montre que les échanges de paquets ne se font pas au sein du continent africain mais en Europe. La raison avancée par l'auteur est un coût d'inter-connexion inférieur en Europe. Ces règles de routage on des conséquences sur les délais, et donc sur les performances sur le service de transport rendu par TCP. Ces résultats ont été confirmés par [Fanou2015]. Cette étude s'intéresse en plus à la stabilité des routes. Les résultats ont montré que les chemins africains restent stables sur une longue durée. Pour les auteurs, l'émergence de nouveaux points d'échanges sur le continent doit aider à la réduction des délais, à conditions que les coûts d'interconnexion soient proches de ceux pratiqués en Europe.

Enfin, l'article [Chavula2017] publié en 2017 présente la latence pour les transferts de fichiers à partir de 53 pays africains différents. Ces mesures s'appuient sur la plate-forme RIPE Atlas [Ripe2010] et Speedchecker [Speechecker]. À partir des mesures réalisées, les

TABLE 1.5 – Tableau des plates-formes de mesures de métrologie active.

Nom	Nombre de sondes déployées	Métriques disponibles	Impact sur la recherche
Archipelago	~200	Longueur du chemin, RTT, DNS, *Autonomous System* (AS)	109
Atlas RIPE NCC	~12 000	RTT, Route, HTTP GET, et requêtes SSL	38
BISMark	~420	RTT, taux de pertes, débit écoulé, temps de chargement d'une page web	304
DASU	~100 000	Informations sur les flux TCP, RTT, routes empruntées, résolution DNS, HTTP GET, débit écoulé	84
PlanetLab	~400		1218
SamKnows	~70 000	RTT, débit écoulé, débit utile, gigue, taux de perte, performance de certains services	154

auteurs avancent que l'Afrique est un continent inégalitaire en terme de latence intra et inter pays. Ils ont conclu que l'existence d'une faible latence entre deux FAI d'un même pays provient d'accord de *peering* au sein d'un IXP hébergé, soit par le pays concerné, soit par un pays voisin.

1.2.3 Métrologie passive

La métrologie passive a pour objectif la mesure des flots de paquets à partir d'un point particulier du réseau appelé le point de collecte. Elle consiste à écouter, capturer et analyser les paquets IP. La figure 1.15 illustre le principe de la métrologie passive. Elle montre que le point de collecte n'est pas forcément localisé du coté émetteur ou récepteur. Les paquets IP transitant par le point de collecte sont capturés et sauvegardés. On appelle alors les fichiers contenant les paquets IP collectés des traces. Les mesures passives peuvent être effectuées à différents niveaux de granularité.

Au niveau microscopique, les mesures passives tendent à étudier les flots au niveau de la connexion de transport. On peut par exemple étudier le nombre de paquets perdus durant une connexion TCP. Au niveau macroscopique, les mesures passives sont effectuées sur des métriques agrégées comme le débit écoulé total ou le nombre total de connexions.

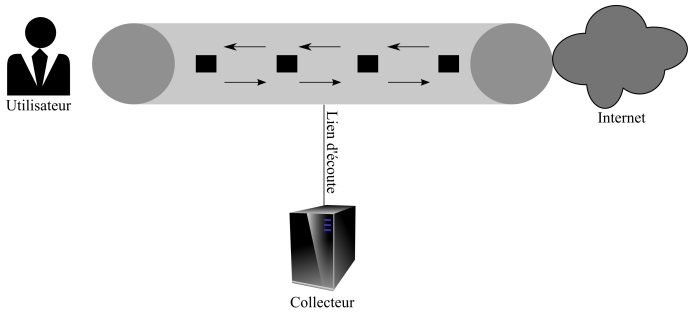


FIGURE 1.15 – Principe de la métrologie passive.

La meilleure façon de réaliser des mesures passives au niveau microscopique est de capturer tous les paquets traversant le point de collecte. Mais comme il est difficile de capturer tous les paquets lorsque le débit du lien est élevé, il faut avoir recours à l'échantillonnage du trafic. Dans ce cas, les mesures ne sont pas faites sur la totalité des paquets traversant le point de collecte, mais sur un sous-ensemble bien spécifique de ces paquets. Le groupe de travail *Packet Sampling* (PSAMP) de l'IETF travaille sur un algorithme d'échantillonnage adapté au trafic Internet [PSAMP].

Une combinaison entre l'analyse des deux granularités est capable de donner une évaluation réelle du trafic. Les informations que l'on peut obtenir par la métrologie passive sont nombreuses. Elles reposent sur l'étude des informations contenues dans le datagramme IP, que ça soit dans l'en-tête du datagramme IP ou dans celle du message du protocole de transport. Les métriques sont également dépendantes des outils utilisés. On peut classer les métriques en deux catégories que sont la supervision et la performance.

La supervision donne des informations sur le fonctionnement du réseau et la caractérisation du trafic. On peut ainsi étudier les différents services et protocole de transport utilisés.
La performance se rapporte à celle du protocole de transport c'est-à-dire son fonctionnement ou sur l'analyse des flots par rapport soit à la composante temporelle ou soit à la composante sémantique. On peut alors comparer le débit d'accès théorique et le débit mesuré. Pour cela, on va étudier le taux de perte, le RTT et la MSS.

La méthode de capture peut reposer sur des équipements matériels dédiés ou par un système logiciel fonctionnant sur un équipement standard. Le logiciel s'appuie majoritairement sur la bibliothèque Libpcap [Jacobson1989-2]. Cette bibliothèque capture les paquets reçus mais elle s'utilise également en lisant des traces de paquets préalablement capturés. Le problème principal des solutions logicielles viennent de la vitesse des liens. Plus le lien a un débit élevé, plus la capture au niveau logiciel devient difficile. Il faut alors se tourner vers des solutions de matériels dédiés. La carte DAG [Graham1997] développée par l'équipe [WAND] de l'Université de Waikato en Nouvelle Zélande en est un parfait exemple. Cette carte de capture est capable de capter les paquets sur des liens de très haut débit. Ce matériel se charge d'extraire les entêtes des paquets, de les estampiller suivant une horloge synchronisée et de les stocker sur un disque dur.

L'analyse des données est réalisée selon deux techniques : temps réels ou *Batch*. Le principe du temps réel est de pouvoir récupérer, extraire et restituer de l'information en temps réel sur des flux continus de données. Le mode *Batch* va englober tous les traitements de données nécessitant un temps de calcul plus conséquent. Le premier procédé se propose d'analyser à la volée ce qui se passe dans le réseau par le branchement d'un équipement d'écoute sur le réseau. On se concentre alors sur la performance du lien. Des outils comme Tstat [Mellia2005] ou Netflow [Claise2004] réalisent ce genre d'analyse. La

seconde technique se décompose en deux phases distinctes que sont la capture et l'analyse. La première étape est de réaliser la capture du trafic, appelée des traces. Des outils comme TCPDump [Jacobson1989-1] ou Wireshark [Chappell2010] peuvent enregistrer des traces sous format *DUMP* ou *PCAP*. La seconde phase consiste à analyser les traces collectées. Les formats de sortie des données analysées sont dépendants des outils. Les informations peuvent être retranscrites au format texte ou graphique. Des outils comme TCPTrace [Ostermann2000] ou TCPStat [Herman2001] peuvent effectuer ce genre d'analyse de données. C'est avec cette technique qu'il est possible d'étudier les performances d'un protocole.

Il n'existe pas de plate-forme d'accès publique réalisant des captures de trafic au niveau international. Malgré cela, des traces collectées sont disponibles sur Internet à des fins de recherche. Dans [Allman2007], les auteurs présentent les règles à respecter avant de publier des traces. Un point est à souligner et concerne les adresses IP des paquets. La non-anonymisation des adresses IP constitue une violation de la vie privée de plus elle présente un risque d'insécurité pour les machines impliquées par les paquets capturés. CAIDA gère un dépôt de partage et propose d'accéder à des traces collectées à travers plusieurs points d'échange américains. Pour y accéder, il faut indiquer la finalité de l'utilisation des traces demandées. D'autres plates-formes dédiées à des projets ont été mises en place à travers le monde.

Le projet IPMon de l'opérateur américain SPRINT consiste à identifier les problèmes d'un réseau déjà déployé afin de pouvoir anticiper son évolution future[IPMon]. Dans l'article [Fraleigh2001], l'auteur présente l'infrastructure de mesure qui est déployée en divers points du réseau de l'opérateur. Les premiers résultats, publiés dans [Fraleigh2003] ont montré une utilisation de plus en plus importante par du trafic multimédia sur le protocole TCP. De plus, les flots TCP présentent des performances élevées, avec des taux de dé-séquencement faibles et un délai minimal proche du temps de propagation.

Le projet METROPOLIS s'est inspiré du projet IPMon. Il s'agit d'un projet français avec des points de mesures sur deux types de réseaux Internet différents : RENATER et le réseau ADSL de France Télécom. « L'objectif de METROPOLIS était de concevoir de nouvelles méthodologies pour la métrologie des réseaux IP » [METROPOLIS]. Dans le cadre de ce projet, un outil de caractérisation et d'analyse des traces fut développé. Ce nouvel outil s'intitule ZOO. Une présentation de l'outil sera réalisée dans la sous-section 3.2.2. Les résultats ont mis une évidence l'usage prédominant du protocole de transport TCP. Les applications de type *peer-to-peer* représentaient plus de 80% du trafic étudié.

La position géographique de La Réunion et son rattachement au RIR AfriNIC attirent notre attention sur les travaux de métrologie passive africains. La carte [AfterFibre] présente les réseaux fibres terrestres et maritimes liés au continent africain. On voit ainsi que les réseaux sont inégalement répartis sur le territoire. La grandeur du continent et les interconnections présentes font du territoire un espace d'étude intéressant. C'est pourquoi de nombreux chercheurs privilégient l'étude de la connectivité et des performances de l'Internet africain.

Dans l'article [Johnson2011], une étude sur une zone rurale connectée par satellite est réalisée. Les résultats ont montré que le trafic est principalement composé de flux web, dont une forte proportion pourrait être mise en cache. Au niveau des délais, le RTT moyen sur la période de mesure varie entre 3 et 10 secondes. Ce délai rend l'utilisation des applications temps-réel difficile. Le dernier résultat notable de cette analyse est la présence de trafic généré par des logiciels malveillants (*malware*). Des attaques pour lister les ports UDP et TCP ouverts ont été remarquées.

En 2015, les auteurs de [Zheleva2015] ont étudié les performances du réseau et le comportement des usagers après une augmentation de la bande passante en Zambie. L'un des

premiers résultats indique une augmentation de plus de 58% de la quantité des données échangées. Au niveau des performances, ils ont pu également remarquer une très légère dégradation du canal de communication avec un taux de retransmission en hausse. Ce pourcentage est passé de $1,12\%$ à $1,16\%$. Le dernier résultat noté porte sur l'augmentation du RTT moyen de plus de 100%, passant de $0,1436$ s à $0,3190$ s. L'augmentation de la bande passante a permis l'accès à de nouveaux services entraînant des changements pour les usagers.

Dans [Fanou2016], l'auteur s'intéresse aux services proposés et compare la localisation des serveurs. Le premier résultat montre l'externalisation continentale de nombreux serveurs. Ceci a pour conséquence d'augmenter les délais et de dégrader la performance du service de communication. Il faut, pour l'auteur, arrêter de raisonner en terme d'infrastructure mais plus en terme de service et mettre l'utilisateur au centre du système. Pour cela, il propose de rapatrier les services sur le territoire et d'augmenter les accords d'échanges entre les opérateurs continentaux.

Enfin dans [Johnson2016], les auteurs s'interrogent sur les faibles performances de TCP en Afrique. La présence de zone reculées, avec des accès satellitaires, poussent les délais vers des valeurs allant au delà des 400 ms. Ces longs délais sont à rapprocher des débits faibles. De plus, une expérimentation sur les performances de TCP en fonction du système d'exploitation a été menée. Les résultats ont mis en évidence que le système Linux avec la version TCP *CUBIC* est moins sensible au long délais. La solution proposée au problème de la différence de connectivité à travers le continent est la création d'une ingénierie réseau (liaison physique, protocole de transport, nouveau service) tenant compte du contexte Africain.

1.2.4 Comparatif entre mesures actives et mesures passives

La métrologie active et la métrologie passive présentent des points communs et des points de divergences. Une fois des objectifs fixés et au moment du choix de la méthode, il est important de connaître les avantages et les inconvénients liés à chaque type de mesure. Le tableau 1.6 récapitule synthétiquement ce qui vient d'être présenté.

TABLE 1.6 – Comparatif entre mesures actives et mesures passives.

	Métrologie Active	Métrologie Passive
Avantages	1 - Pour la mesure directe des paramètres de QoS principalement le délai, le taux de pertes et la gigue.	1 - Non intrusives. 2 - Permettent une mesure directe des paramètres utilisés dans l'ingénierie des réseaux.
Inconvénients	1 - Intrusives : le trafic de mesure peut, dans certains cas, fausser les mesures elles-mêmes. 2 - Le fait que certains administrateurs et entreprises bloquent ou limitent le trafic ICMP, peut fausser les résultats obtenus par les techniques actives car ces dernières font souvent usage de ce protocole.	1 - Elles sont locales (relatives à un lien) et il est difficile de les étendre à la globalité du réseau. 2 - Elles ne permettent pas la mesure directe des paramètres de QoS. 3 - Elles nécessitent des ressources disque et mémoire vive importantes.

1.3 Synthèse

Ce chapitre a rappelé le fonctionnement du contrôle de congestion de TCP. Le contrôle de congestion de TCP vise à maximiser l'utilisation des ressources, et à maximiser le débit utile écoulé de la connexion. Ce contrôle est régi par une boucle fermée caractérisée par un RTT. Plus le délai est élevé, moins TCP est susceptible de réagir dynamiquement aux événements de congestion. Lorsque le produit du RTT et de la capacité du canal de communication est trop important, TCP peine à atteindre les objectifs précédemment présentés. L'augmentation progressive de la bande passante sans diminution des délais a pour effet l'augmentation de la capacité de stockage des liens. Cet accroissement a un effet négatif sur les performances de TCP. Cet effet négatif impacte le démarrage de connexion, les flots courts, la résolution de la congestion et la dynamique du sondage. Pour diminuer l'effet de la capacité de stockage des liens sur les performances de TCP, de nouveaux contrôles de congestion furent développés. Chaque nouvelle version du contrôle de congestion ambitionne de résoudre une à plusieurs problématiques des réseaux à forte capacité de stockage. Le démarrage de connexion et les flots courts ont des solutions communes comme une augmentation de la capacité d'émission de TCP à l'initialisation de la connexion ou la réduction du RTO. Les problématiques de résolution de congestion et de dynamique de sondage ont permis la création de nouvelles versions du contrôle de congestion de TCP. Ces versions de TCP sont des solutions de bout-en-bout. D'autres solutions nécessitent un changement de paradigme et l'interaction avec les routeurs. Ces solutions ont l'avantage d'être réactives mais nécessitent la mise à jour des équipements intermédiaires du réseau.

Le localisation géographique de La Réunion au milieu de l'océan indien place l'île dans une situation où la capacité de stockage du réseau peut être importante. Nous avons ainsi estimé cette capacité à l'aide des débits théoriques des accès et les délais de propagation estimés et mesurés. Les résultats obtenus ont mis en évidence une capacité de stockage autorisant la caractérisation de l'Internet réunionnais comme un réseau à forte capacité de stockage. L'impact de cette capacité de mémorisation n'a pas encore été mesuré. C'est pourquoi nous nous sommes concentrés sur la métrologie Internet.

La métrologie active est une science invasive en injectant des paquets dans le réseau. La métrologie active mesure directement des paramètres de qualité de service comme les délais, les routes, le taux perte et la gigue. Nous avons vu que des outils sont en capacité de mesurer deux métriques simultanément. Certains outils peuvent être distribués et ainsi former des plates-formes de mesure. Ces plates-formes offrent la possibilité aux personnes intéressées du monde entier de générer des données de mesure à travers le monde. Les performances de TCP sont dépendantes du délai. Les délais sont eux-même dépendants des routes physiques et logiques empruntées. Il est donc important d'étudier ces deux paramètres. Connaissant nos besoins, nous utiliserons l'approche *research driven* pour l'étude de métrologie active. L'approche *research driven* est une approche consistant à définir en premier lieu les métriques recherchées avant de mettre en place l'infrastructure et les outils nécessaires à l'étude. Notre étude de métrologie active est présentée dans le chapitre 2.

La métrologie passive permet une mesure directe des paramètres utilisés. Cette classe de métrologie est centrée sur un lien de mesure. Elle utilise l'écoute et la capture des datagrammes IP. La métrologie passive étudie la caractérisation du trafic et la performance des protocoles. Nous avons vu que des outils sont en capacité de réaliser les deux études en parallèle. Ne pouvant réaliser des études de métrologie passive à distance, de nombreux chercheurs ont mis à disposition de la communauté scientifique des données publiques. La littérature scientifique propose un grand nombre de métriques pour l'étude des performances du protocole de transport TCP et de la supervision du trafic. Afin de

ne pas nous concentrer sur une métrique en particulier, nous faisons le choix de ne pas dresser une liste de métriques. Notre étude de métrologie passive, que nous présenterons dans le chapitre 3, utilisera l'approche *measurement driven*. Cette approche consiste à mettre en place une infrastructure de mesures afin de récupérer le maximum d'informations puis d'effectuer toutes les analyses possibles sur les données collectées. Néanmoins la métrologie passive souffre de deux faiblesses essentielles : (1) elle reste locale et il est difficile d'étendre les résultats à la globalité du réseau, (2) au niveau microscopique, les captures aboutissent très rapidement à des volumes de traces colossaux.

Chapitre 2

Caractérisation de la connectivité de La Réunion

Le rapport [Mediametrie2018-2] sur l'accès Internet à La Réunion a montré que 85,6% de la population réunionnaise de plus de 13 ans s'est déjà connectée à Internet. 74,7% de ces personnes sont des usagers réguliers. En comparaison, le rapport [Mediametrie2018-1] montre qu'aux alentours de 68% de la population française métropolitaine se connecte quotidiennement. Ces sondages montrent l'intérêt pris par l'Internet pour la population réunionnaise.

En 2013, une étude de métrologie réalisée par BinarySec vise a effectuer un classement des fournisseurs d'accès Internet de La Réunion. Dans le rapport associé [Vergoz2013], 9 métriques sont présentées. Parmi elles, le débit descendant moyen est mesuré à $9,36\ Mb/s$. En comparaison, le débit descendant moyen en France métropolitaine, mesuré par [Akamai2015], s'élève à $8,2$ Mbit/s. Akamai utilise la plate-forme *Intelligent Platform*^{TM} pour récolter des données, dont le débit réel. La Réunion possédait ainsi un meilleur débit descendant que la France métropolitaine. Le débit moyen français présenté par [Akamai2017] est de $10,75$ Mbit/s. Le débit descendant minimum réunionnais, mesuré par [nPerf2017], est de $18,63$ Mbit/s. Ainsi, l'écart entre les débits français et réunionnais s'est accentué. Malgré un débit plus élevé, La Réunion présente des délais plus élevés que la France.

L'évolution des débits pose la question sur l'évolution des délais depuis la dernière campagne de mesure. La figure 1.11 montre des délais plus importants à La Réunion qu'à Paris. L'objectif de ce chapitre est d'étudier l'évolution des délais depuis 2012. On s'intéresse également à la connectivité de La Réunion, en terme de délai et de routes. L'asymétrie des liens est une chose courante dans l'Internet. Les questions que l'on se pose depuis La Réunion doivent également être posées lorsque l'on essaye de joindre l'île. Dans ce chapitre, nous allons explorer la connectivité de La Réunion. Pour cela nous avons mis en place un protocole de mesures se basant sur notre propre plate-forme de mesures respectant la répartition des destinations. Notre plate-forme a pour objectif l'étude des routes et des délais spécifiques de l'île par rapport à son accès Internet via les câbles sous-marins.

Une seconde question est alors apparue. Est-ce que ces spécificités sont uniquement celles de La Réunion ou alors communes aux îles de la Zone Océan Indien ?

Dans la section 2.1, nous présentons les objectifs de notre étude de métrologie et les contraintes associées. Afin de répondre à ces contraintes, un cahier des charges est présenté dans la section 2.2. Le protocole d'étude est décrit dans la section 2.3. Les résultats obtenus pour La Réunion, suivis de ceux des îles de l'Océan Indien, sont présentés dans la section 2.4.

2.1 Objectifs

En 2012, [Anelli2012] a réalisé une campagne de mesure des délais depuis La Réunion et Paris. Cette campagne de métrologie active, basée sur la commande ping, a pour objectif de démontrer la différence de délai et de débit entre La Réunion et Paris. Le premier objectif de nos travaux consiste à la mise jour des données par une nouvelle étude des délais. Nous ferons par la suite référence à cet objectif par le titre "Evolution".

Le second objectif est l'analyse de la connectivité Internet de La Réunion. Pour arriver à obtenir une analyse précise de la connectivité Internet réunionnaise, une étude sur les routes empruntées par les paquets IP en provenance et à destination de La Réunion sera réalisée. Pour cela, on utilisera un outil de type traceroute. On utilisera les données récoltées pour l'identification des portes de l'Internet réunionnais. La référence utilisée pour cet objectif dans le suite du manuscrit est "Connectivité".

Ayant ciblé les métriques, nous avons fait le choix de la méthode *research-driven*. Cette méthode, présentée dans la section 1.2.1, a l'avantage de se concentrer uniquement sur des métriques décidées préalablement. Dans le cas de notre étude, ce sont les délais et les routes.

2.2 Cahier des charges

Deux paramètres doivent être pris en considération lors de la rédaction du cahier des charges : l'outil de mesure et l'outil d'analyse.

2.2.1 Evolution

Pour répondre à l'objectif, nous allons effectuer une reprise de l'existant. L'outil de mesure sera la commande ping associée à la plate-forme Planet-Lab [PlanetLabEurope]. L'outil d'analyse sera identique à celui utilisé par [Anelli2012].

2.2.2 Connectivité

Identification des besoins

Dans le tableau 1.4, nous avons vu que différents outils sont capables de mesurer les routes et les délais. L'outil retenu devra limiter les erreurs liées aux mécanismes de l'équilibrage de charge et de MPLS. Cet outil devra réaliser des mesures depuis des nœuds répartis sur l'ensemble de l'île. Pour cela, il est nécessaire d'effectuer un choix de plate-forme de métrologie active. Ce choix se fera sur 2 points : la distribution géographique des nœuds de mesure et la couverture des différents fournisseurs d'accès internet.

L'outil d'analyse devra être en capacité d'identifier les portes de l'Internet réunionnais à travers la géolocalisation des adresses IP, d'identifier les marques MPLS présentes dans les données pour une meilleure compréhension des règles de routage, générer une carte des relations entre pays à travers les échanges de paquets envoyés et réaliser des statistiques sur les différents nœuds empruntés.

Mise en œuvre d'une infrastructure de métrologie active

Dans la section précédente, nous avons vu que notre cahier des charges devra respecter 3 principaux critères : outil de mesure, plate-forme de mesure et outil d'analyse.

Paris-traceroute

Nous avons vu dans la partie 1.2.2 que l'étude des routes et des délais peut se faire à l'aide d'un seul outil : traceroute. Or cet outil est sujet à des imprécisions liées à l'équilibrage des charges par exemple. Souhaitant limiter l'impact de ces aléas dans nos données nous faisons le choix de Paris-traceroute. Pour rappel, une présentation de l'outil et de ses mécanismes est faite à la section 1.2.2.

La plate-forme RunPL

Les plates-formes disponibles Similairement, dans la section 1.2.2, nous avons présenté des plates-formes de métrologie active. La plate-forme sélectionnée devra respecter les critères présentés précédemment.

Parmi les plates-formes, seules Atlas et Planet-Lab ont des sondes présentes sur l'île, respectivement 21 et 2. Ces sondes sont réparties de manière inéquitable sur l'île. La région Est de l'île ne compte qu'une sonde quand le minimum est de 6 dans les autres régions. De plus, certains des *Fournisseurs d'Accès Internet* (FAI) n'hébergent pas de sonde de mesure. Le résumé de notre comparaison est indiqué dans le tableau 2.1.

TABLE 2.1 – Répartitions des sondes chez les Fournisseurs d'Accès Internet.

	Archipelago	Atlas	BISMark	DASU	Planet-Lab	SamKnows
Paris-traceroute	**Oui**	**Oui**	**Oui**	Non	**Oui**	Non
Disponibilité sur l'île	Non	**Oui**	Non	Non	**Oui**	Non
Couverture de l'île	Non	**Oui**	Non	Non	Non	Non
Répartition fournisseurs	Non	Non	Non	Non	Non	Non

On constate ainsi qu'aucune des plates-formes présentées ne remplit la totalité des critères de sélection. Nous avons souhaité déployer notre propre infrastructure. Cette nouvelle plate-forme répondra à nos critères en offrant une meilleure couverture de l'île, sur les aspects géographiques, FAI et *Technologies d'Accès à Internet* (TAI). L'échantillon de population est représenté par un ensemble d'étudiants. Notre plate-forme nous autorise également à être maître de l'infrastructure de mesures que l'on souhaite mettre en place. Afin de sélectionner les outils (physiques et logiciels) les plus adaptés à nos objectifs, nous avons décidé des spécificités de notre plate-forme.

Création et déploiement de la plate-forme RunPL La plate-forme que l'on souhaite déployer devra respecter un schéma de connectivité bien précis, représenté par la figure 2.1. La *Sonde de mesure* est le cœur de la plate-forme. La *Destination* correspond à une adresse IP ou un nom de domaine à joindre pour obtenir des informations sur les routes empruntées et les délais associés. Le *Serveur de stockage* est présent pour délester la sonde de mesure. L'*Ordinateur distant* représente l'administrateur de la plate-forme. Ne pouvant se déplacer pour configurer la sonde, un accès distant doit être réalisé. Il est illustré par le train en pointillé sur la figure. Le trait plein entre la sonde et la destination correspond à l'interaction entre la sonde et la destination. Cette interaction représente les mesures que l'on obtiendra sur les performances des liens. Les sondes de mesure devront pouvoir effectuer les mesures sans limitation de destinations. Elles devront, afin de limiter

le stockage, effectuer un délestage des mesures collectées sur un serveur de stockage. Ce serveur de stockage, tout comme la sonde de mesure, devra pouvoir être joint par l'ordinateur distant. Cette communication a un double objectif. Le premier est la récupération des données pour les analyses. Le second est la mise à jour du protocole de mesure si nécessaire. Une interaction sécurisée est établie entre l'ordinateur distant, la sonde et le serveur de stockage. Cette liaison est caractérisée par les pointillés sur la figure 2.1.

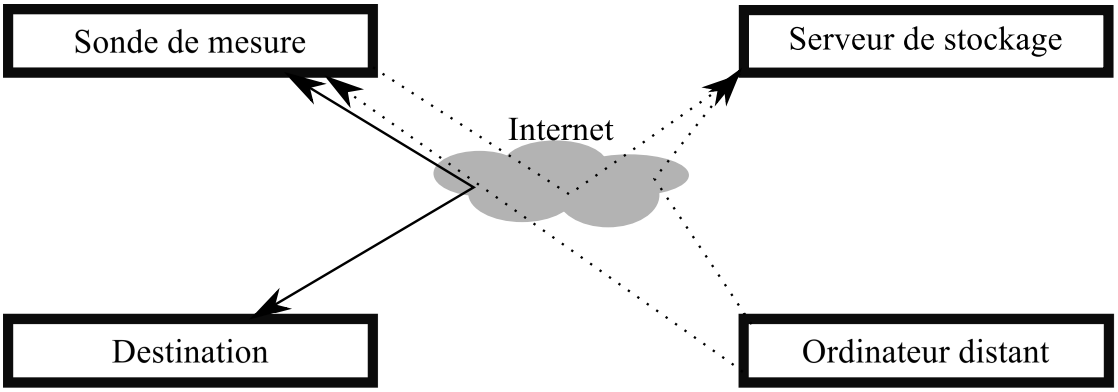


FIGURE 2.1 – Schéma d'interconnexion de la plate-forme.

Les spécificités de notre plate-forme se décomposent en deux grandes parties, que sont la partie matérielle et la partie système.

Matérielle Un cahier des charges spécifique à notre plate-forme de mesure doit être réalisé. La première partie concerne le choix du matériel physique.

La partie matérielle de la plate-forme de mesure est formée de deux composants, la sonde de mesure et le serveur de stockage des données. Le serveur de stockage sera fourni par le *Laboratoire d'Informatique et de Mathématiques* (LIM). Seule la sonde de mesure sera indiquée dans le cahier des charges. Le matériel sélectionné devra respecter les critères précis. Ces critères ont été décidés en étudiant les solutions proposées par les plates-formes précédemment étudiées :

— Peu encombrant : de nombreuses sondes proposées par les différentes plates-formes sont très discrètes. Notre sonde devra également être peu visible. Nous souhaitons que la sonde soit directement connectée sur le routeur de l'usager.

— Peu coûteux : le coût unitaire de chaque kit ne devait pas dépasser 50€ afin que l'on puisse avoir un nombre de nœuds conséquent. Un kit sera composé de la sonde, de son câble alimentation, d'une carte mémoire et d'un câble réseau.

— Peu énergivore : la facture d'électricité étant à la charge de l'usager, nous souhaitions une solution à faible consommation d'énergie.

— Diversité du système d'exploitation (OS) : Le système d'exploitation choisi devra supporter l'installation de Paris-traceroute.

La seconde partie du cahier des charges de notre plate-forme se concentre sur le choix du système d'exploitation.

Pour rappel, sur la figure 2.1, nous avons représenté en pointillé des interactions sécurisées. Ces échanges concernent l'accès distant à la sonde, au serveur de stockage et à la sauvegarde des données de mesures sur le serveur. Le système d'exploitation devra correspondre aux critères de sélection suivants :

— Paris-traceroute. Le système d'exploitation devra intégrer Paris-traceroute dans ses librairies d'installations ou supporter l'installation du code source.

— Licence GNU-GPL. Des modifications du système seront potentiellement nécessaires.

— Accès distant. Le matériel devant être géré à distance. Un accès *Secure SHell* (SSH) devra donc être configuré. Le protocole SSH [RFC4250] fut développé pour permettre l'accès à distance de terminaux.

— Transmission sécurisée. L'accès au différents composants de la plate-forme devra se faire d'une façon sécurisée. La restriction se fera à travers un système d'identification.

Sélection du matériel [Maksimovic2014] réalise une comparaison de différents micro-ordinateurs, tels que Arduino [Arduino], BeagleBone [Beaglebone], Phidgets [Phidgets], Udoo [Udoo] et RaspberryPi [RaspberryPi]. Dans ce comparatif, les critères utilisés sont proches de ceux que l'on a sélectionnés. Le tableau 2.2 résume l'ensemble des critères de sélection du matériel. Il provient directement de l'article [Maksimovic2014].

TABLE 2.2 – Tableau de comparaison des micro-ordinateurs. (source : [Maksimovic2014]).

Critères	Arduino	BeagleBone	Phidegts	Raspberry Pi	Udoo
Encombrement (en mm)	**75*53**	86.3*53.3	81.3*53.3	85.6*53.98	110*85
Coût (en $ par nœud	**30**	45	50-200	**25-35**	99-135
Énergie (en V)	7-12	**5**	6-15	**5**	6-15
Système d'exploitation	/	Linux angstrom	Linux	**Raspbian, Ubuntu, Android, ArchLinux, FreeBSD, Fedora, RISC OS**	Ubuntu, Android, Linux, ArchLinux

Nous avons mis en évidence les valeurs respectant les critères. Nous faisons le choix du Raspberry Pi car il possède le plus de critères respectés.

Sélection du système d'exploitation Le premier critère de sélection est l'installation de Paris-traceroute. D'après [Paris-traceroute], l'outil est disponible sur les systèmes Raspbian, Ubuntu, ArchLinux et FreeBSD.
Concernant les licences, l'ensemble des OS ne sont pas équivalents. Ainsi, seul Raspbian, Ubuntu et ArchLinux proposent une licence *General Public Licence* (GPL). RISC OS est associé à une licence propriétaire. Android, FreeBSD et Fedora sont sous licence de logiciel libre et open source. Les licences de distribution open source vont nous autoriser à ajouter, modifier voire supprimer des parties du code pour qu'il corresponde plus facilement à nos besoins.
De nombreux OS proposent nativement la version cliente du protocole SSH. La version serveur peut être activée lors de l'installation du système d'exploitation. L'accès distant nous permettra également la mise à jour des outils et des OS pour des raisons de sécurité.
La sécurisation des échanges se fera au travers d'un *Virtal Private Network* (VPN). Un

VPN est un système permettant de créer un lien direct entre des ordinateurs distants. [Coonjah2015] réalise une comparaison entre deux outils permettant la création de VPN, OpenSSH et OpenVPN. OpenSSH propose de meilleures performances qu'OpenVPN au niveau de l'utilisation de la bande passante et des temps de transferts de fichiers. Malgré cela, nous avons pris le parti d'utiliser OpenVPN car c'est un outil majoritairement utilisé par les entreprises [Coonjah2015]. Cet utilitaire nous propose la mise en place d'une connexion sécurisée, basée sur l'identification à travers un certificat d'authentification. Le VPN permet de joindre, à travers un adressage privé, les différentes sondes qui seront distribuées sur l'île de La Réunion. D'après le site officiel d'[OpenVPN], l'outil peut s'installer facilement sur les distributions Rapsbian, Ubuntu et Fedora.

Le choix du système d'exploitation va dépendre des critères de sélection. Nous récapitulons les critères présentés précédemment dans le tableau 2.3.

TABLE 2.3 – Récapitulatif de la comparaison des Systèmes d'exploitation sur Raspberry Pi.

Critères	Raspbian	Ubuntu	Android	ArchLinux	FreeBSD	Fedora	RISC OS
Paris-traceroute	**Oui**	**Oui**	Non	**Oui**	**Oui**	Non	Non
Licence	**GPL**	**GPL**	ASL	**GNU Linux**	BSD	Creative Commons	Castle Technologies Ltd Licence
Accès distant (SSH)	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**
OpenVPN	**Oui**	**Oui**	Non	Non	Non	**Oui**	Non

Deux systèmes disponibles pour Raspberry Pi répondent à nos critères, Raspbian et Ubuntu. Nous faisons le choix du système Raspbian. Cet OS est une distribution Linux entièrement revue pour des performances optimales sur la carte Raspberry Pi. Fortement inspirée par la distribution Linux Debian, elle propose les mêmes caractéristiques que la distribution dite de Bureau. Les sondes n'étant pas équipées d'un système d'affichage, nous optons pour l'installation la plus légère possible avec uniquement les paquets nécessaires à notre étude.

L'outil d'analyse : rTraceroute

Dans la section 2.1, nous avons présenté les contraintes liées à la sélection d'un outil d'analyse des données de type traceroute. Pour rappel, ces contraintes sont les suivantes : la géolocalisation des adresses IP, l'identification des liens MPLS, la génération d'une carte des liens logiques et la génération d'un fichier comportant des statistiques sur les différents nœuds rencontrés.

Les outils disponibles Il existe différents outils d'analyse des routes, que l'on peut ranger en trois catégories : les générateurs de données brutes, les plates-formes de mesures et les outils d'analyse graphiques. L'outil que l'on souhaite utiliser entre dans la troisième catégorie. La littérature autour d'outils graphiques pour l'analyse des routes n'est pas aussi complète que l'on pourrait croire.

Gtrace est un outil créé par [Periakaruppan1999]. Cet outil reproduit graphiquement les résultats obtenus par Traceroute. Le logiciel génère ses propres données avant de les

représenter sous forme graphique. La géolocalisation ne se fait pas sur les adresses IP mais sur le nom *Domain Name System* (DNS) des nœuds rencontrés. La localisation d'un nœud n'est validée qu'après croisement des informations entre les abréviations des villes et aéroports, d'informations contenues dans deux bases de données. Une dernière vérification est réalisée à l'aide de la commande nslookup. Actuellement, cet outil n'est plus maintenu. Il n'implémente pas le [RFC4950] permettant l'identification des nœuds MPLS dans les routes.

[Aben2015] présente un outil d'analyse des routes intégré à Atlas RIPE NCC. Cet outil d'analyse se nomme OpenIPMap. Il utilise la base de données de RIPE pour effectuer la géolocalisation des données. Les routes sont ensuite tracées sur une carte interactive. Les mesures générées par Atlas sont directement visibles et peuvent s'intégrer dans OpenIPMap. L'identification des nœuds MPLS ainsi que la partie statistique ne sont pas incluses dans les sorties proposées par OpenIPMap.

Dans [Yang2016], l'auteur présente un outil d'analyse des routes centré sur le continent africain, African Visual Route. Le design de l'outil s'inspire largement du projet OpenIPMap [Aben2015]. L'outil possède un défaut important. Il lit uniquement les fichiers provenant de la plate-forme Atlas.

Le tableau 2.4 présente les possibilités offertes par chaque outil présenté précédemment.

TABLE 2.4 – Fonctions disponibles dans les outils graphiques d'analyse des routes.

	African Visual Route	Gtrace	OpenIPMap
Géolocalisation	**Oui**	**Oui**	**Oui**
Identification des liens MPLS	Non	Non	Non
Cartographie	**Oui**	**Oui**	**Oui**
Statistiques	Non	Non	Non

On peut constater, que par rapport à nos besoins, les outils listés présentent des lacunes. Les critères d'affichage des liens MPLS et la partie statistique sur les nœuds intermédiaires n'ont pu être remplis. Pour ces raisons, nous avons développé un outil d'analyse, rTraceroute.

Développement de rTraceroute

Géolocalisation Dans le cadre de nos travaux, la géolocalisation d'adresse IP considère la position géographique de l'adresse, les informations sur le détenteur de l'adresse et l'*Autonomous System* (AS) associés. Un AS est un ensemble d'équipements et de réseaux sous une même autorité. rTraceroute géolocalise les adresses IP rencontrées à travers une base de données implémentée au sein du LIM. Cette base de données est remplie au fur et à mesure que de nouvelles adresses IP sont remontées par les mesures. L'identification des nouvelles adresses se fait par un script, développé en python sous ma direction, par un étudiant de Licence 3^{eme} année [LanYanFock2015]. Cet outil, nommé **rgeoloc**, utilise les commandes de l'*Application Programming Interface* (API) de RIPE NCC. En interrogeant une base de données d'un RIR, nous espérons limiter les erreurs liées à la géolocalisation. Pour nos besoins, nous limitons les informations liées à la localisation et au FAI. Ces informations sont *Pays*, *Latitude*, *Longitude*, *Nom du FAI*, *Numéro de l'AS*.
Les informations (pays, longitude, latitude) seront utilisées par la suite pour effectuer

des calculs de distance entre deux adresses IP. Le nom du FAI autorise le suivi des accords d'échanges de paquets sur les routes. Le numéro de l'AS nous offre la possibilité de suivre les différents chemins empruntés en termes d'AS différents.

rgeoloc est capable d'extraire les informations de délais et de longueurs de routes d'un fichier traceroute. Il peut également découper un fichier contenant plusieurs données traceroute en fichier unitaire.

La géolocalisation des adresses associées à l'identification des liens MPLS va aider à la compréhension des routes de l'Internet dans le monde.

Identification des liens MPLS Paris-traceroute indique dans ses sorties les liens MPLS rencontrés. [Augustin2007] indique que l'identification des liens se fait par la lecture des informations contenues dans les paquets reçus par l'outil. rTraceroute va identifier les marques MPLS et les représenter en un coloris différent sur les cartes.

Cartographie Lors de la géolocalisation des adresses IP, l'information nécessaire à la cartographie est le pays. Lors de cette identification, deux nouvelles informations sont associées à l'IP. Ce sont les coordonnées du pays pour la carte passée en paramètre. À partir de ces nouvelles coordonnées, rTraceroute va générer une nouvelle carte affichant l'ensemble des liens logiques (entre pays) présents dans les traces analysées.

Statistique rTraceroute génère des statistiques sur chaque nœud rencontré. La clé d'identification d'un nœud est son adresse IP et sa position sur la route analysée. Les statistiques générées sont l'occurrence de la paire d'identification, le délai minimal obtenu pour joindre ce nœud à cette position et le pays rattaché à l'adresse IP.

Notre outil est actuellement disponible sur le site du laboratoire, à l'adresse suivante : http://lim.univ-reunion.fr/rtraceroute [rtraceroute]. Cet outil est distribué sous licence libre pour une large diffusion dans la communauté scientifique.

2.3 Protocole de mesure

La connectivité particulière de l'île par les deux câbles sous-marins provoque un intérêt de l'étude des routes empruntées. L'un des objectifs de nos mesures est d'étudier l'évolution des délais et de la longueur des routes entre 2012 et 2016. Le second objectif est l'étude de la connectivité en terme de routes, de délais et des accès logiques de l'Internet réunionnais.

Notre protocole de mesure se divise en 3 parties. La première partie présente les points communs entre les deux objectifs. La seconde consiste à effectuer une comparaison de l'état actuel avec le travail effectué précédemment par [Anelli2012]. Le troisième point concerne les mesures d'identification des portes de l'accès Internet de La Réunion.

2.3.1 Échantillon de mesure

L'échantillon d'adresses IP que l'on va utiliser dans nos études se doit d'être représentatif et précis. La précision s'obtient par la taille d'un échantillon. La représentativité par le respect de la distribution des adresses IP dans l'Internet.

Il existe 2^{32} adresses IPv4, avec une répartition bien spécifique. D'après les [RFC3232, RFC5735, RFC6761], $592\ 708\ 865$ adresses sont réservées. On peut citer en exemple les adresses de type $192.168.0.0/16$. Ce bloc est réservé aux réseaux privés. Son utilisation prévue est documentée dans le [RFC1918]. Telles que décrites dans ce standard, les adresses

de ce bloc n'apparaissent pas légitimement sur l'Internet public.
Après soustraction, il ne reste que $3\ 702\ 258\ 431$ adresses à répartir dans les différents pays et FAI. Ces IP sont distribuées par préfixes par les RIR, dont RIPE NCC pour l'Europe et AfriNIC pour le continent africain. Afin d'avoir un échantillon précis, nous avons généré aléatoirement $1\ 000\ 000$ d'adresses non réservées. Ces adresses ont été testées par le protocole *ICMP*. Ce test nous assure que les adresses IP sont des adresses que nous pourrons utiliser par la suite. Nous avons ainsi validé $84\ 000$ adresses. Néanmoins, nous n'avons aucune garantie sur la modification des attributions des adresses IP au fil du temps.

Pour que notre jeu de destinations soit représentatif, nous avons géolocalisé les adresses valides. Nous avons regroupé les résultats par continent pour une meilleure lisibilité. Le résultat obtenu est illustré par la figure 2.2a.

Nous pouvons constater une forte disparité entre les différents continents. L'Océanie et l'Afrique ont moins de 1% de présence dans notre jeu. On constate également une forte présence d'adresse de type BOGONS. Ces adresses font parti de blocs encore non alloués par les RIR ou alors réservées par l'*Internet Assigned Numbers Authority* (IANA), mais présentes au sein de l'Internet. On peut citer l'adresse *100.120.16.100* en exemple. Cette adresse est marquée comme réservée par l'IANA par RIPE NCC. Ce nombre d'adresses est en diminution avec l'attribution des blocs restant aux différents FAI. Pour valider ce résultat, nous l'avons comparé à la distribution datant de Mai 2016 du site CountryIP-Blocks [1]. Le regroupement est illustré par la figure 2.2b. On remarque un certain équilibre entre l'Europe et l'Asie et une domination de l'Amérique du Nord.

Notre répartition est différente en de trop nombreux points à celle de CountryIP-Blocks. Les données communiquées par CountryIPBlocks proviennent des RIR. Cette distribution est donc plus proche de la répartition réelle. C'est pourquoi, à partir de notre ensemble d'adresses initales, nous sélectionnerons un sous ensemble en respectant la distribution présentée par la figure 2.2b.

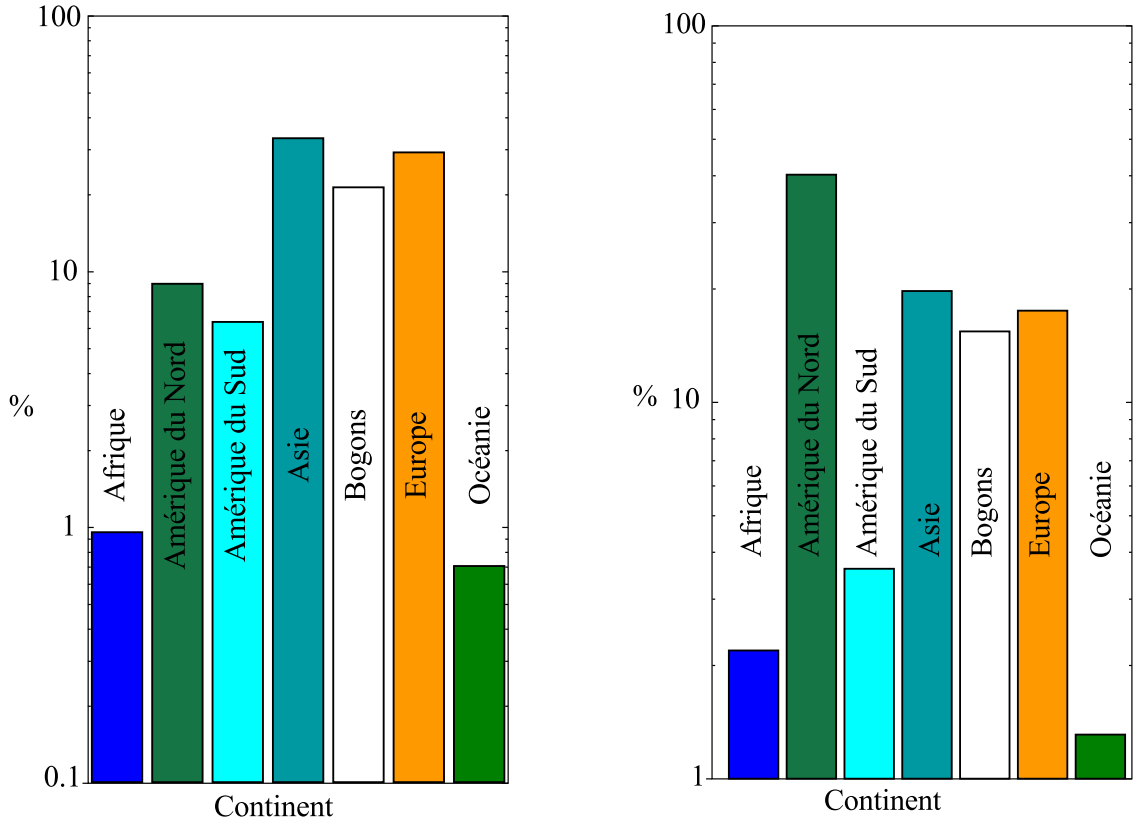
2.3.2 Évolution

En 2012, [Anelli2012] a effectué une campagne de ping depuis Paris et La Réunion. Cette campagne, réalisée sur le FAI RENATER, avait pour objectif la mise en évidence de la différence des délais entre Paris et La Réunion. Afin d'étudier l'évolution des délais et de la longueur des routes depuis l'étude précédente, nous avons réalisé une nouvelle campagne de ping depuis Paris et La Réunion. Cette campagne a mis a contribution les nœuds [PlanetLabEurope] de l'Université de La Réunion et de l'Université Pierre et Marie Curie.

À partir du jeu d'adresses préparé présenté précédemment, nous avons tiré le maximum d'adresses IP possibles tout en respectant la répartition géographique de la figure 2.2b. Nous avons obtenu un jeu de $40\ 000$ adresses. Nous avons fait le choix d'utiliser un échantillon d'adresses différentes par rapport à la première étude. Cette décision provient de notre volonté d'obtenir des données représentatives de l'état actuel de l'Internet, en terme de répartition des adresses. Chaque mesure sera indépendante l'une de l'autre. En effet, pour qu'une mesure se lance, il faut que la précédente soit finie.

L'analyse se déroulera à l'identique de ce qui s'est fait pour l'étude précédente, à l'exception d'une modification. Nous y ajouterons la comparaison de la longueur des routes. Les résultats associés à cette étude seront présentés dans la section 2.4.1.

1. Source : https://www. countryipblocks. net



(a) IP sélectionnée au hasard.

(b) CountryIPBlocks.

FIGURE 2.2 – Distribution géographique des adresses IPv4 publiques.

2.3.3 Connectivité

La seconde étude de métrologie active concerne l'étude de la connectivité de La Réunion. Pour répondre à notre objectif, nous mettons en place deux protocoles de mesure : Un protocole étudiant la connectivité *Depuis La Réunion* et un protocole dans le sens *Vers La Réunion*.

Depuis La Réunion

Notre étude de métrologie se compose de plusieurs phases :

1. la préparation du jeu de destinations ;
2. la réalisation des mesures par les sondes ;
3. la quantification des perturbations de nos mesures sur l'accès des usagers ;
4. la collecte des résultats obtenus par les sondes ;
5. l'analyse des résultats.

Préparation La répartition géographique présentée dans la figure 2.2b ne peut pas s'appliquer à l'intégralité de notre ensemble de départ. Afin de pouvoir garder cette répartition, nous avons réduit notre jeu de destinations à $10\,000$ adresses. Cette réduction est nécessaire afin que l'ensemble de nos mesures puissent être réalisées en un délai de 24 heures. Bien que le nombre d'adresses sélectionnées représente moins de 1% des adresses IP publiques de l'Internet, il est néanmoins suffisant pour que notre jeu reste précis.

Réalisation Chaque sonde étant indépendante, l'automatisation du lancement des mesures dès le démarrage est nécessaire. De fait, une procédure a été implantée au sein de l'OS. Cette procédure va autoriser le démarrage des mesures dès la fin de la phase d'initialisation de l'ensemble des services de Raspbian. La mise en place des mesures est divisée en 2 étapes.

La première consiste, pour chaque sonde, à créer ses propres scénarios de mesures. Un scénario est un fichier contenant deux colonnes : destination et intervalle de temps. La première colonne contient les $10\ 000$ adresses IP de destination. La seconde colonne regroupe des valeurs qui serviront d'écart entre deux mesures. Ces valeurs ont été générées suivant une loi exponentielle de taux 8,64. Ce taux provient de l'équation 2.1 ci-dessous.

$$taux = nombre\ de\ secondes\ par\ jour / nombre\ d'adresses\ IP = 86400/10000 = 8,64 \tag{2.1}$$

Les valeurs obtenues seront identiques sur l'ensemble des sondes de mesures. Chaque scénario sera créé en tirant aléatoirement une adresse IP et un écart. Une fois que l'ensemble des scénarios est écrit et numéroté de 1 à 28, la sonde va programmé dans le temps l'exécution de la seconde étape, grâce à la commande *at*.

La seconde étape consiste à lire le scénario du jour et à joindre la destination par l'outil de mesure. La commande exacte exécutée par chaque test est :

```
Paris-traceroute -m 255 -n -p icmp @ip
```

Dans laquelle les options indiquent :

- *-m 255* : la valeur du champ TTL du paquet est mise à sa valeur maximale (255). Nous faisons le choix d'autoriser l'outil à essayer de joindre la destination jusqu'à épuisement de la valeur maximale autorisée par le protocole pour identifier certains problèmes de routage.
- *-n* : pas de résolution de DNS. Afin d'optimiser les mesures, nous avons éliminé la résolution des noms des routeurs. Seules les adresses IP seront affichées.
- *-p icmp* : le protocole utilisé pour la mesure. [Wenwei2006] effectue une étude comparative entre les protocoles ICMP et TCP pour les mesures de délai. Ils ont montré que, dans certaines conditions, les résultats sont similaires. Quand le ratio α, calculé entre le RTT moyen et le RTT minimal tend à être important (supérieur à 20), TCP est moins stable que son concurrent. C'est pour cette raison que nous avons fait le choix de l'ICMP.
- @ip : adresse IP de destination que la commande va essayer de joindre.

Vérification La sonde va consommer de la bande passante de chaque connexion Internet. L'estimation du débit de la mesure dépend du nombre moyen de paquets émis par mesure et de la durée moyenne d'une mesure. À l'aide d'une période de test, nous avons pu calculer divers paramètres d'une mesure réalisée avec Paris-traceroute. Les informations obtenues concernent la durée d'une mesure et le nombre de paquets échangés. Les résultats obtenus montrent qu'une mesure dure en moyenne 28 secondes et se compose de 54 paquets de 64 octets. Une mesure génère donc un débit d'émission de 987 bits/s à l'entrée de l'interface réseau. Le débit généré effectif (au niveau du support) est de 1265 bits/s. Le débit généré par rapport au débit d'accès d'un accès ADSL est alors négligeable.

D'après le rapport [Vergoz2013], le débit montant le plus faible mesuré est de $128,33Kb/s$. La charge calculée représente près de 1% de la capacité du lien d'accès. Comme il y aura en moyenne 4 mesures simultanées, la capacité consommée correspond donc à 4%. Cette situation correspond au pire cas. Dans la situation courante d'un accès théorique en Mbit/s, nous pouvons avancer que la sonde n'aura aucun impact sensible sur la connectivité du participant.

Collecte Une phase de collecte des données de mesures est réalisée. Le but de cette étape est de libérer de l'espace disque sur la sonde. Chaque jour à minuit, un nouveau scénario est lancé. Une fois que 7 scénarios ont été lus, la sonde va créer une archive. Le nom de l'archive sera composé de la date de création de l'archive, du nom de la sonde et de la TAI. Le nom propose un classement rapide des données, que ça soit par TAI ou par date. L'archive contiendra les mesures des 7 jours précédents. L'archive est envoyée sur le serveur de stockage localisé au sein du laboratoire. Une comparaison de l'empreinte MD5 de l'archive présente sur le serveur et sur la sonde de mesure sera réalisée. Si les deux empreintes sont identiques, alors la suppression de l'archive hébergée sur le Raspberry Pi est réalisée. Le jour d'envoi des données sur le serveur, aucune mesure n'est effectuée afin de ne pas générer de bruit supplémentaire sur le lien. Le lendemain de la copie des données, la sonde va amorcer 7 nouveaux jours de mesures. Un cycle de mesures est composé de 7 jours de mesures consécutifs et d'un jour d'envoi des données vers le serveur de stockage. Ce cycle est répété 4 fois par mois. La figure 2.3 schématise le fonctionnement d'une sonde de mesure sur une durée de 32 jours, soit 4 cycles de mesure et de collecte.

La plate-forme réalise des mesures en continue jusqu'à l'arrêt complet de l'appareil de mesures. Nous n'avons, pour l'instant, pas programmé d'arrêt des mesures. Dans le cadre de l'analyse réalisée dans ce manuscrit, nous avons pris un cycle complet de mesure, soit 32 jours. Nous n'effectuons pas d'analyse comparative temporelle de nos mesures.

Analyse La plate-forme réalise les mesures par cycle de 7 jours. L'analyse des traces récoltées se fait en plusieurs étapes. Le processus d'analyse commence par la découpe du fichier de données en fichiers atomiques. Chaque fichier atomique contiendra uniquement le résultat d'une mesure. Chaque fichier de données récoltées par jour va donc être découper en $10\,000$ fichiers atomiques. Cette découpe est réalisée par l'outil rgeoloc. L'analyse des fichiers atomiques diffère selon l'objectif :

L'extraction des délais s'effectue à l'aide de rgeoloc. Lors de l'extraction, les informations sur les délais sont accompagnées de la longueur du chemin et des adresses IP source et destination.

Nous souhaitons déterminer si les routes Internet provenant de La Réunion sont symétriques ou non. Pour cela une étude des délais et des routes vers La Réunion est effectuée.

Vers La Réunion

Les routes asymétriques sont fréquentes et principalement dues à des politiques de routage et à l'ingénierie de trafic. Des mécanismes comme l'équilibrage de charge (*load-balancing*), *Hot Potato Routing*, ou encore *BGP* (*Border Gate Protocol*) peuvent également générer un phénomène d'asymétrie des liens.
Hot Potato Routing est un phénomène lié au routage sans règlement. Le routeur transfère le paquet aussi vite que possible vers un routeur situé en aval sur la route [Feige1992, Wang2018].

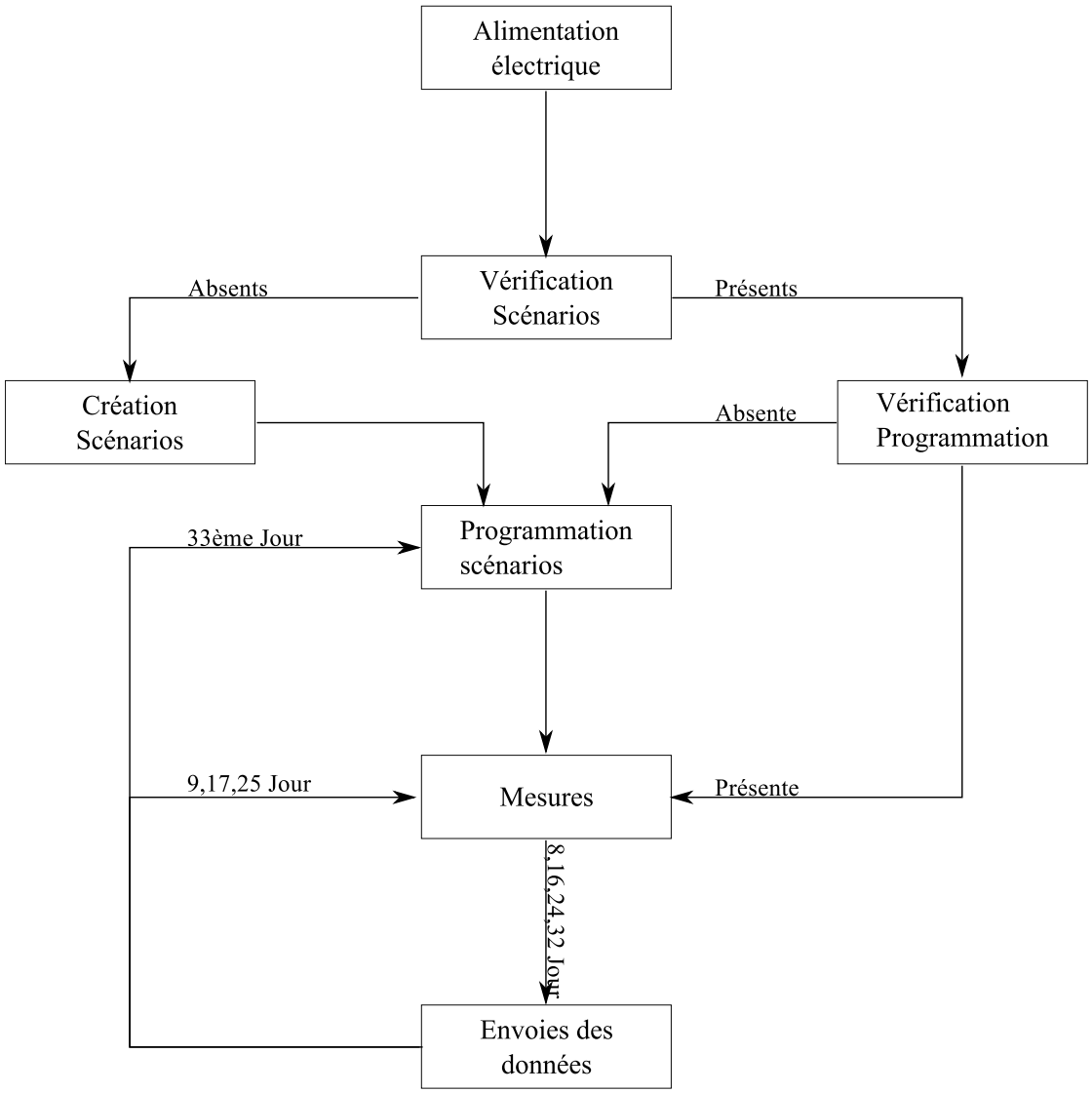


FIGURE 2.3 – Fonctionnement de la sonde.

BGP est protocole de routage inter-AS défini dans le [RFC1105]. En fonction des informations échangées, deux paquets peuvent ne pas suivre la même chemin IP mais suivre un chemin AS identique.

Afin de vérifier la présence des liens asymétriques, nous avons mis en place le protocole suivant, en utilisant la plate-forme Atlas RIPE NCC [Ripe2010]

Préparation Pour notre étude, et en accord avec les *Conditions Générales d'Utilisation (CGU)* d'Atlas, nous avons sélectionné le nombre maximal de sondes autorisées, soit 1 000. Ces sondes serviront de sources pour nos mesures. La sélection des sondes s'est faite selon deux critères.
Le premier est le fait que la sonde soit active. En effet, même si la sonde n'est pas joignable, Atlas continue d'indiquer la sonde dans ses données.
La seconde indication nécessaire à la sélection d'une sonde est son pays d'hébergement. Il est nécessaire de garder la même répartition géographique que les destinations sélectionnées pour l'étude précédente (voir Figure 2.2b).

La sélection des destinations s'est effectuée sur les critères d'identification des FAI et des TAI disponibles sur l'île. Tout comme notre plate-forme de mesure de la section 2.3.3,

il est pour nous important que nos destinations respectent une parité sur ces critères de sélection. Afin de nous assurer que nos destinations soient physiquement hébergées sur l'île, nous avons pris la décision de sélectionner des sondes de mesure de l'étude précédente. L'utilisation d'Atlas étant régi par un système d'utilisation et de création de crédit, nous avons dû limiter le nombre de nos destinations à 10 IP publiques de la plate-forme RunPL. Nous avons pleinement conscience que ce nombre n'est pas forcément représentatif du nombre d'adresse IP disponibles sur l'Île de La Réunion, mais nous sommes restreint par les CGU d'Atlas.

Réalisation Atlas propose deux possibilités de programmation des sondes. La première s'effectue à travers son interface graphique. Le second choix est d'utiliser une API. Comme il est fastidieux de programmer un nombre important de mesures à travers l'interface graphique, nous faisons le choix d'utiliser l'API. Pour effectuer $10\ 000$ mesures par jour, nous avons fait le choix de garder le taux de la loi exponentielle de l'étude précédente, soit $8,64$ secondes. Afin de limiter les phénomènes de synchronisation, le calendrier de mesures a été généré aléatoirement. Nous nous sommes assurés que chaque sonde de mesures allait effectivement joindre l'ensemble des destinations par jour.

Vérification La vérification des perturbations se fait sur la bande passante descendante. En effet, ce sont les sondes de la plate-forme RunPL qui génèrent du trafic en continu. Il ne faut pas que les mesures de la section 2.3.3 soient impactées par l'arrivée des paquets entrants. Le nombre maximal de paquets arrivant jusqu'au routeur de l'hébergeur est de 3. Un paquet possède un poids maximal de 64 octets. Un poids total de 1536 bits est envoyé à la destination. Une mesure étant programmée toutes les 8 secondes, nous utilisons cette valeur comme variable pour calculer le débit. Nous avons donc un débit de 192 bit/s.

D'après le rapport [Vergoz2013], le débit descendant le plus faible mesuré est de $1,58$ Mbit/s. Notre mesure impact représente donc approximativement $0,12\%$ de la capacité du lien. Cet impact est négligeable à un instant donné.

Collecte La plate-forme Atlas stocke automatiquement les résultats liés à ses expérimentations sur son propre serveur. Une fois l'ensemble des mesures réalisées, nous avons récupéré les résultats. Un total de $300\ 000$ fichiers, correspondant aux $300\ 000$ mesures, ont été téléchargés du serveur d'Atlas.

Analyse Cette partie de l'étude est fortement similaire à l'analyse effectuée pour l'étude des routes et délais depuis La Réunion. Une seule partie diffère. En effet, comme indiqué dans la section précédente, chaque fichier collecté représente une mesure. Nous n'avons donc pas la nécessité d'effectuer une phase de découpage de nos données en fichiers atomiques.

Récapitulatif

Afin de pouvoir effectuer une comparaison entre les deux protocoles de mesures sur l'étude des routes et des délais associés, le tableau 2.5 résume les deux protocoles sur le mois de mesure analysé.

Nous constatons une différence notable en terme de sources et de destinations. Cette différence impacte le nombre de fichiers atomiques que l'on a obtenus. Le nombre de fichiers atomiques provient de la multiplication entre le nombre de sources, le nombre de destinations et le nombre de jours de mesures. Cela correspond au nombre maximal de

TABLE 2.5 – Résumé des caractéristiques du jeu de données.

	Depuis	Vers
Sondes de mesures	Raspberry Pi	Atlas RIPE NCC
Nombres de Destinations	$10,000$ IP	10 raspberry-pi
Nombres de sources	27	$1,000$
Nombres de jours de mesures	28	30
Outil de mesure	Paris-traceroute	
Nombres de fichiers atomiques	$7,560,000$	$300,000$
Nombres de fichiers analysés	$1,015,180$	$38,714$

fichiers que l'on peut obtenir. La dernière ligne du tableau indique le nombre de fichiers que l'on a pu analyser après vérification des mesures et nettoyage des fichiers erronés. Ce nettoyage se fait par l'outil d'analyse rTraceroute. Dans la section 2.3.3, nous avons pu analyser $13,43\%$ des données. De la section 2.3.3, $12,91\%$ des données ont été exploités. Nous avons dans les deux cas, un taux de pertes de données important.

2.4 Résultats

Dans la suite de notre manuscrit et pour des raisons pratiques, nous avons réduit le nom des continents à deux lettres. La correspondance entre l'acronyme et le nom complet est indiquée dans le tableau 2.6.

TABLE 2.6 – Correspondance entre acronymes et noms des continents.

Nom	Afrique	Asie	Europe	Amérique du Nord	Océanie	Amérique du Sud
Acronyme	AF	AS	EU	NA	OC	SA

Cette correspondance provient de l'utilisation des deux premières lettres de chaque continent, en version anglophone.

2.4.1 Évolution

La comparaison avec l'existant fut divisée en deux. Dans un premier temps, nous avons comparé les délais. Par la suite, nous avons utilisé une partie des données non encore exploitées pour réaliser une comparaison de la longueur des routes.

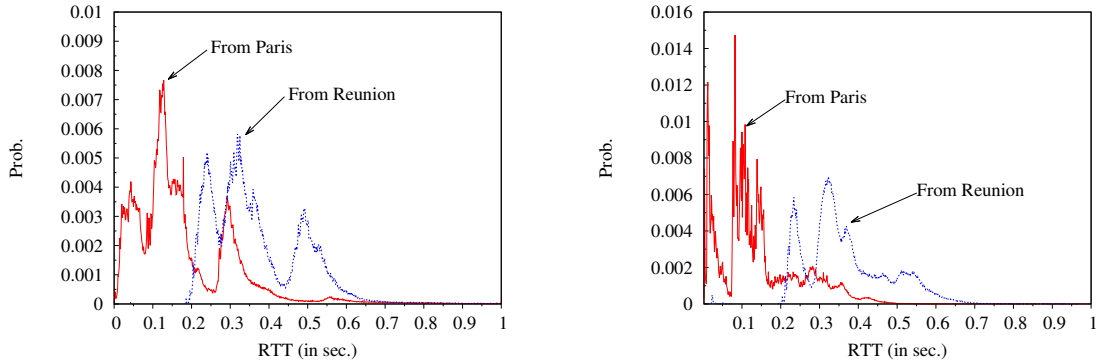
Distribution du RTT

Les mesures obtenues ont permis d'effectuer une comparaison avec les données récoltées en 2012 par [Anelli2012]. Nous avons effectué une campagne de ping en 2016 afin d'étudier l'évolution des délais, depuis Paris et La Réunion. La figure 2.4 illustre l'évolution de la distribution du RTT en 4 ans.

Entre 2012 et 2016, le jeu d'adresses IP de destination fut différent. En 2012, aucune répartition géographique ne fut établie. En 2016, la distribution des adresses est celle présentée dans la partie 2.3.1. Malgré ces différences, nous remarquons que les courbes ont les mêmes tendances en 2012 et en 2016. Des pics sont présents aux environs des valeurs 0.05, 0.1 et 0.3 secondes pour Paris en 2012. Des pics sont identifiés aux valeurs 0.2, 0.35 et 0.5 secondes pour La Réunion en 2012. Les pics sont présents aux alentours des mêmes valeurs sur les deux campagnes de mesure. Nous émettons l'hypothèse que ces

pics correspondent aux 3 continents les plus représentés dans nos échantillons, à savoir l'Amérique du Nord, l'Asie et l'Europe. Nous vérifierons cela par la suite.

Malgré un écart de 4 ans entre les deux campagnes de mesures, on constate une stabilité du délai minimal aux alentours de 0.2 secondes. La stabilité du délai s'est elle accompagnée d'une stabilité de la longueur des routes ?



(a) 2012. (b) 2016.

FIGURE 2.4 – Comparaison des délais entre Paris et La Réunion.

Longueur du chemin

Dans le section précédente, nous avons constaté que le délai minimal pour quitter l'île est resté stable en 4 ans. Nous allons essayer de corroborer cette stabilité du délai par une stabilité de la longueur des routes sur la même période.

La longueur des routes fut obtenue par l'analyse inverse du TTL. Le [RFC1700] préconise une valeur de départ de 64. Or, le site Wikipédia [WikiPing] indique que le TTL initial peut varier. Les valeurs les plus communes sont 64, 128 voire 255 dans certains cas. Nous avons donc, en fonction de la valeur du TTL soustrait une valeur de départ à la valeur indiquée pour obtenir la longueur de la route. Dans les données datant de 2012, les longueurs de certaines routes sont égales à 127. Ne pouvant décider de la valeur de TTL de départ, nous avons fait le choix de ne garder que les résultats dont le TTL affiché par ping est supérieur ou égal à 128. Pour les données de 2016, nous n'avons pas répertorié de valeurs comprises dans l'intervalle $[120, 208]$. De fait, nous avons gardé l'ensemble des valeurs obtenues.

La figure 2.5 illustre l'évolution des routes entre les deux jeux de résultats. En 2012, la longueur des routes évolue entre 10 et 40 nœuds, avec un pic à 24 nœuds. En 2016, les routes ont une longueur qui varie entre 5 et 30 sauts, avec un pic à 17. Un écart de 7 nœuds représenté sur notre figure.

Les délais entre La Réunion et Paris sont restés stables entre 2012 et 2016. Sur la même période, la longueur des routes depuis La Réunion a diminué.

2.4.2 Connectivité de La Réunion

La section 2.4.1 a montré l'évolution des délais et de la longueur des routes entre 2012 et 2016. Malgré ces études, aucune caractérisation de la connectivité de La Réunion n'a été réalisée. Dans cette section, nous allons effectuer cette caractérisation en termes de délais et des routes empruntées.

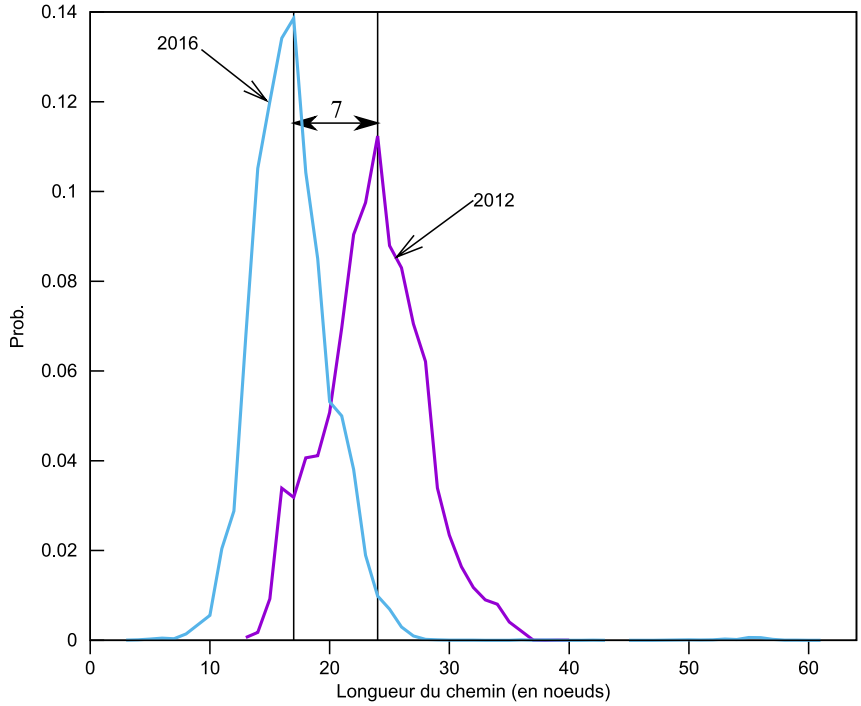


FIGURE 2.5 – Évolution de la longueur des routes entre 2012 et 2016.

Généralités

Nous avons en plus, des informations sur les délais et la longueur des routes, des informations sur les adresses IP rencontrées tout au long des mesures. Ainsi, nous avons décidé de répartir notre analyse sur 4 principales métriques, que sont :

— La longueur du chemin est déterminée par le nombre de nœuds rencontré par Paris-traceroute.

— Le délai analysé est le RTT. Il est associé à la destination jointe.

— La localisation des adresses IP avant (resp. après) le passage par les câbles sous-marins quand nos données arrivent (resp. quittent) à La Réunion.

— La distance géographique correspond à la distance réelle (en Km) entre la source et la destination. Pour cela, on utilise l'équation (2.2). Ils s'agit de l'équation de calcul de distance entre deux points sur une sphère.

$$\begin{aligned} d = arccos[&cos(x) \times cos(y) \times cos(m) \times cos(n) + \\ &+ cos(x) \times sin(y) \times cos(m) \times sin(n) + \\ &+ sin(x) \times sin(m)] \times 6371,1\ [km] \end{aligned} \tag{2.2}$$

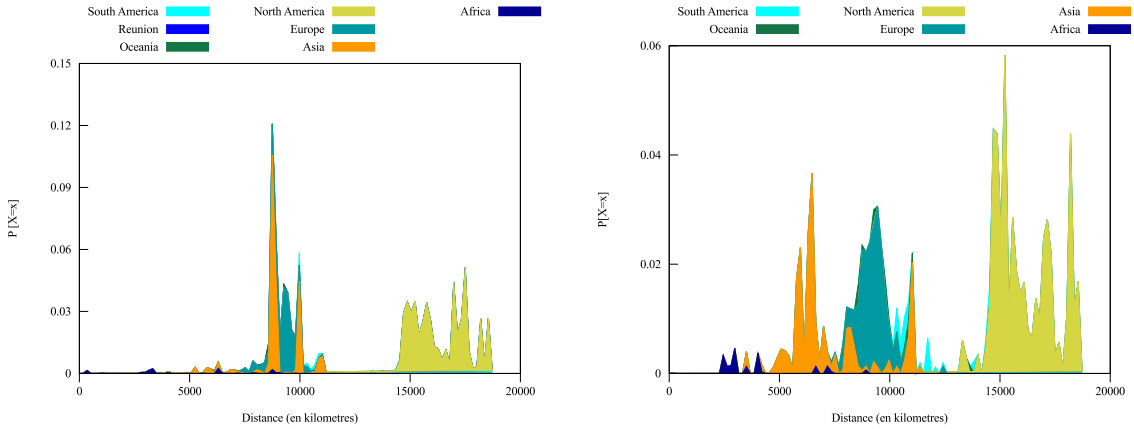
où

— (x,y), (m,n) sont respectivement la latitude et la longitude de la source et de la destination (en radians)

— 6371,1 km est la référence en radius de la Terre

Les coordonnées géographiques des adresses IP ont été obtenues par notre outil de géolocalisation. Nous avons ainsi pu calculer la distance géographique entre deux adresses IP. Si nous prenons l'exemple de la répartition géographique des adresses IP des sondes atlas et des destinations sélectionnées, nous obtenons la figure 2.6. Les deux courbes sont similaires en terme de répartition des distances. La différence des valeurs de l'axe des

ordonnées provient du nombre plus important d'échantillons pour la figure 2.6a. Sur cette figure, il est difficile de visualiser la distance des adresses relatives au continent océanique. La faible épaisseur de la probabilité des adresses océaniques est également présente sur la figure 2.6b. On constate sur cette figure, une présence plus importante d'adresses IP africaines et asiatiques.



(a) Depuis. (b) Vers.

FIGURE 2.6 – Distribution de la distance géographique par continent.

La répartition des adresses IP dans le monde et leur distance géographique ont-elles un impact sur la distribution des délais ? C'est à cette question que nous allons essayer de répondre dans la section suivante.

Distribution du RTT par continent

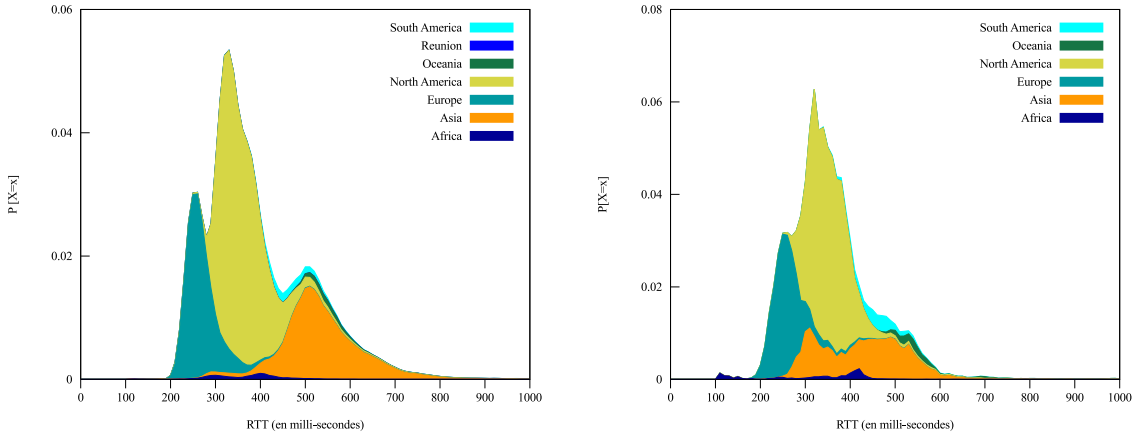
La figure 2.7 représente la distribution des délais obtenus par nos mesures, incluant la répartition par continent. Nous avons utilisé un regroupement des délais par écart de 10 ms. On constate rapidement que les deux figures n'ont pas la même tendance. Dans la section 2.4.1, nous avions émis l'hypothèse que les pics présents sur les courbes des délais étaient associés aux continents les plus présents dans la géolocalisation des adresses IP.

La comparaison que l'on peut effectuer avec les données de l'existant est celle de l'étude "Depuis". Ainsi, on remarque que la figure garde la même forme, avec la présence des 3 pics. Sur la figure 2.7a, nous pouvons identifier ces pics. Ces pics représentent l'Europe, l'Amérique du Nord et l'Asie. On constate que le délai minimal est stable avec une valeur proche des 200 ms.

Dans l'expérimentation "Vers" La Réunion, nous constatons la présence de, non pas 3 mais de 2 pics. Le pic relatif au continent asiatique a disparu. De plus, les délais associés à ce continent sont moins concentrés. Pour les autres continents, la distribution des délais est relativement identique à l'expérimentation précédente. Nous pouvons remarquer la présence de délais africains vers La Réunion aux alentours des 100 ms. Les délais depuis l'Europe sont sensiblement équivalents à ceux de l'étude "Depuis" avec des délais compris entre 180 et 190 ms.

À la lecture des résultats, nous pouvons confirmer que l'hypothèse avancée précédemment est juste.

Nous avons connaissance d'une relation entre la distance et le temps mis pour parcourir cette distance. Ayant constaté l'évolution des délais, nous allons maintenant étudier l'évolution de la distance parcourue.



(a) Depuis. (b) Vers.

FIGURE 2.7 – Distribution du RTT par continent.

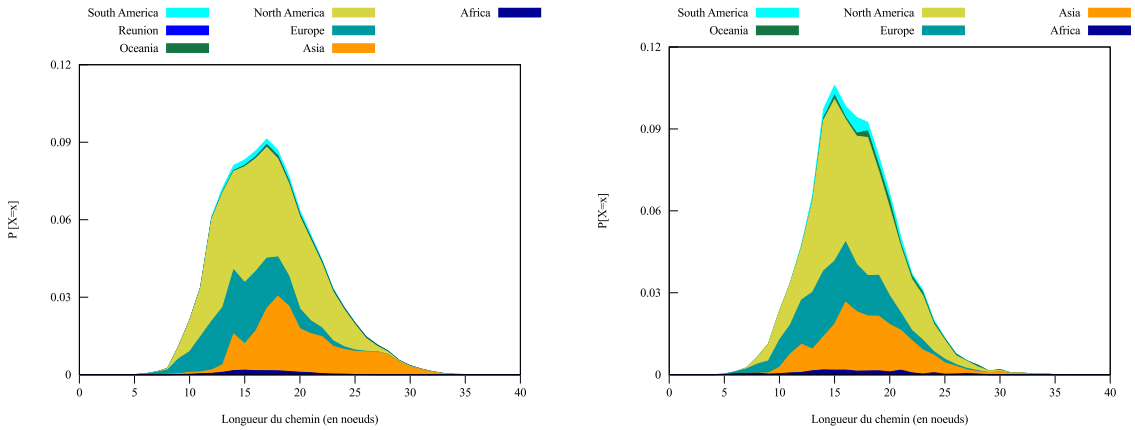
Longueur du chemin par continent

Nous avons pu, dans la section 2.4.1, constater une diminution des routes entre 2012 et 2016. Les figures 2.8 indiquent la répartition de la longueur des routes obtenues en fonction des continents. La première constatation est la forte similitude entre les deux courbes.

Sur la figure 2.8a, on remarque la présence d'un pic pour une longueur de 18 nœuds. Cela indique que peu importe le continent de destination, la probabilité d'avoir une route d'une longueur de 18 sauts est importante.

Dans le sens "Vers", le pic est quasiment identique selon le continent de départ. La valeur générale se situe à une valeur de 15 nœuds pour l'Amérique du Nord, l'Océanie et l'Amérique du Sud et à une valeur de 16 sauts pour les autres continents.

Avec un écart de 2 à 3 sauts selon le sens, on peut donc considérer que la longueur du chemin reste identique pour l'Internet réunionnais.



(a) Depuis. (b) Vers.

FIGURE 2.8 – Distribution de la longueur des routes par continent.

Longueur du chemin et distance géographique

Le premier résultat analysé concerne la distance logique par rapport à la distance physique. Dans l'article [Leguay2004], l'auteur a calculé la moyenne des chemins dans

l'Internet à partir d'un jeu incluant plus de $7\ 000\ 000$ de données. La valeur obtenue est de $15,57$ sauts.

Dans nos résultats, la valeur moyenne calculée est de $17,11$ équipements traversés avant de joindre la destination. Cette valeur regroupe l'ensemble de nos données sans aucune distinction de la localisation de la source d'émission. En étudiant uniquement les données *Depuis*, les routes ont une longueur moyenne de $17,37$ sauts. Si on analyse la longueur des routes des données entrant sur l'île, on obtient une moyenne de $16,85$ équipements. On observe déjà une première asymétrie des routes selon que l'on quitte ou que l'on joint l'île de La Réunion.

Les figures 2.9a et 2.9b illustrent les résultats obtenus. Chaque figure est divisée en deux. On a inséré en bas de chaque figure la PDF de la longueur du chemin en fonction de la distance entre sources et destinations. Tandis qu'en haut, les aires dessinées par les ellipses contiennent 95% des échantillons rattachés à chaque continent. Les barres d'erreurs représentent quant à elles la moyenne et l'écart-type de la longueur du chemin associés à chaque continent.

Nous remarquons que depuis La Réunion la majorité des distance sont situées dans trois grandes régions. Le premier regroupement se situe entre $8\ 000$ et $12\ 000$ km. Ce bloc inclus l'Asie, l'Océanie, l'Europe et l'Amérique du sud. Le second bloc comporte que l'Amérique du Nord et se situe au delà des $14\ 000$ km. Reste le cas africain. Ce continent est très proche de La Réunion. Les destinations et sources africaines sont toutes inférieures à $10\ 000$ km.

L'analyse générale des résultats obtenus montre que le nombre de sauts n'est pas dépendant de la distance géographique. Sur la figure 2.9a, on constate des chemins aussi longs sur la boucle locale que pour joindre certaines destinations lointaines. On a également représenté sur les figures, $PL(d) = \alpha \times d + \beta$ qui est la fonction linéaire de la longueur du chemin comme fonction de la distance géographique. Le tableau 2.7 regroupe les équations obtenues, selon l'expérimentation.

TABLE 2.7 – Formule de corrélation de la longueur du chemin en fonction de la distance géographique.

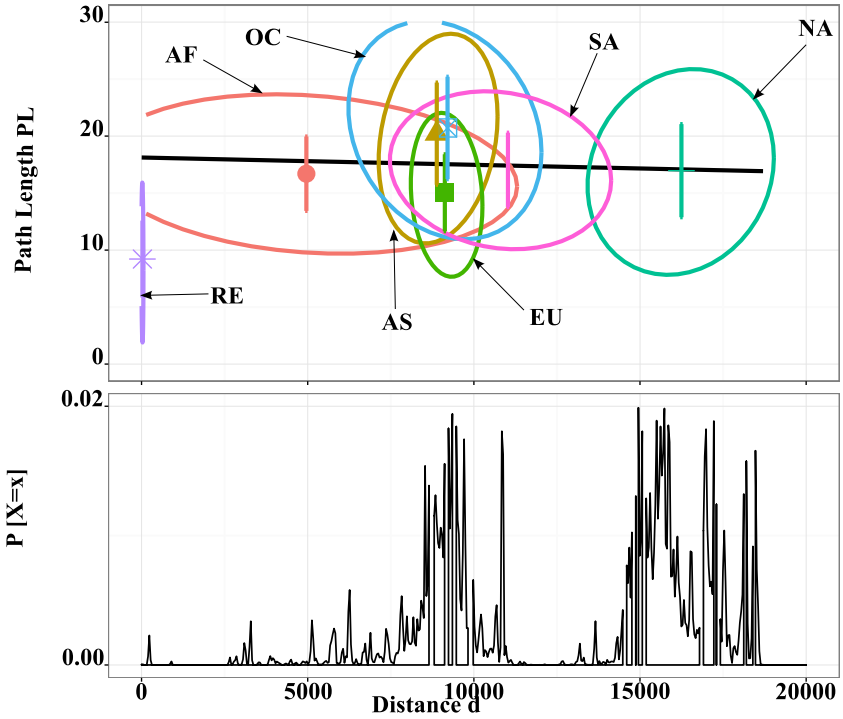
Expérimentation	Équation PL(d)
Depuis La Réunion	$1,58 * 10^{-5} \times D + 16,65$
Vers La Réunion	$7,50 * 10^{-5} \times D + 18,32$

La valeur obtenue pour α, qui est le coefficient directeur de la droite, possède un multiplicateur égal à 10^{-5}. Cette valeur indique le nombre de sauts supplémentaires pour chaque kilomètre. Les valeurs de α, proches de zéro, indiquent clairement que la distance géographique n'impacte pas la longueur du chemin, quelle que soit l'expérimentation.

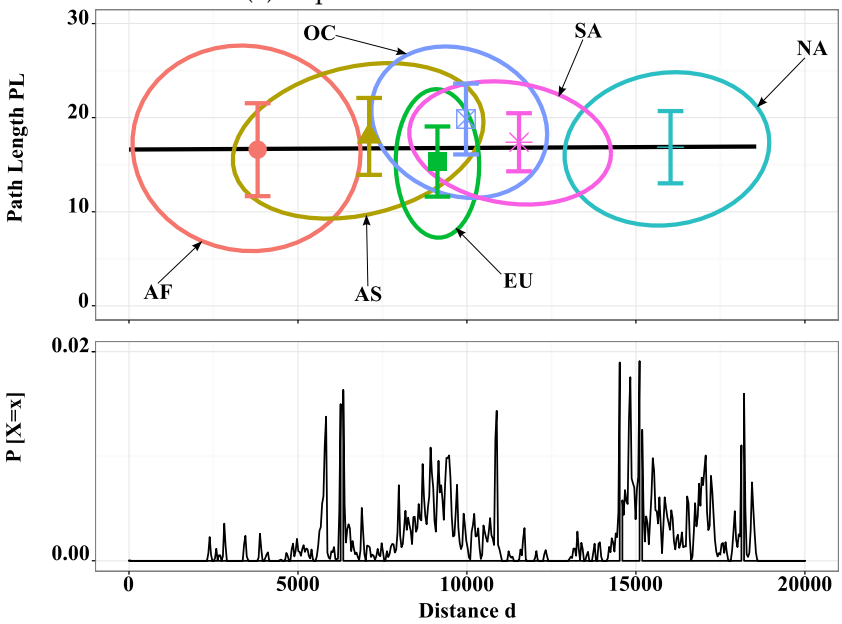
Impact de la longueur du chemin sur le RTT

Les figures 2.10a et 2.10b représentent la distribution du RTT comme fonction du nombre de sauts, ainsi que la médiane et les PDF. Est également présente, en bas de chacune des figures, la probabilité de densité de la longueur du chemin.

Les figures montrent une croissance du délai avec l'augmentation du nombre de nœuds, jusqu'à une certaine limite. Sur la figure 2.10a, représentant l'étude *Depuis*, nous remarquons des délais importants, dépassant les 3 secondes. Cette valeur des 3 secondes peut être atteinte dès que l'on dépasse le 9^{eme} saut. À l'inverse, sur l'étude *Vers*, illustrée par la figure 2.10b, nous constatons une certaine stabilité du délai. Les valeurs restent



(a) Depuis l'île de La Réunion.



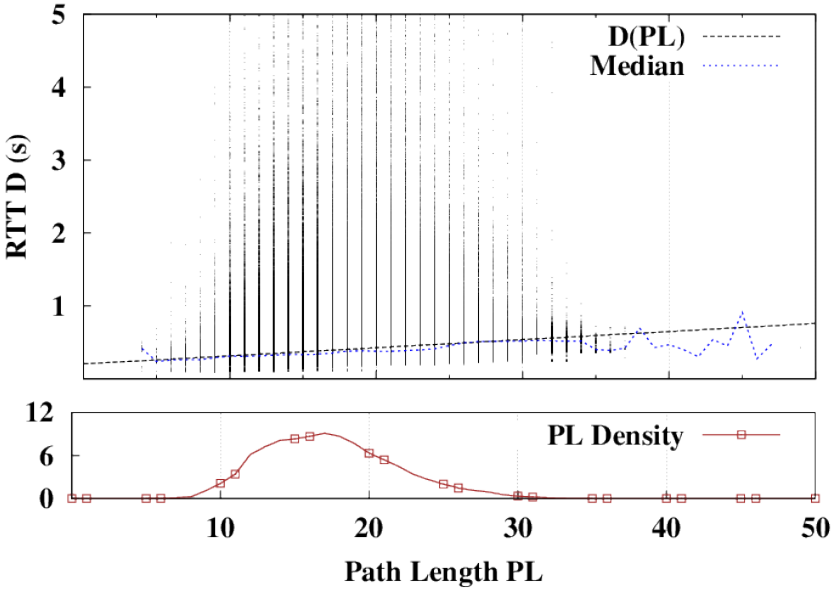
(b) À destination de La Réunion.

FIGURE 2.9 – Relation entre la longueur de la route et la distance géographique.

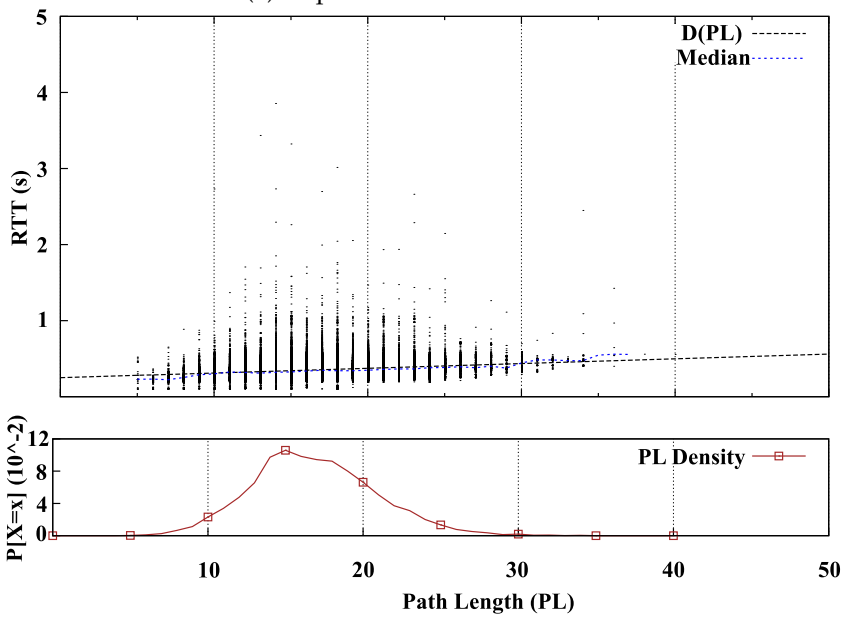
majoritairement inférieures à 2 secondes. L'étude de la médiane nous indique des routes plus courtes lorsque l'on essaye de joindre La Réunion. Il y a une forte variation de la médiane à la fin de la figure, due au nombre d'échantillons pour chaque valeur de la longueur des routes. Afin d'identifier le délai associé à chaque nouveau nœud, la fonction linéaire $D(d) = \alpha \times d + \beta$ du délai comme fonction de la longueur du chemin est également représentée.

Le tableau 2.8 indique les équations obtenues lors de l'analyse des données.

La variable d'ajustement β ne sera pas analysée, bien qu'elle représente un délai minimal. Nous avons vu dans la partie précédente que ce délai était équivalent peu importe



(a) Depuis l'île de La Réunion.



(b) À destination de La Réunion.

FIGURE 2.10 – Relation entre la longueur de la route et les délais.

TABLE 2.8 – Formule de corrélation du délai en fonction de la longueur du chemin.

Expérimentation	Équation D(PL)
Depuis La Réunion	$11,11 \times PL + 204,92$
Vers La Réunion	$6,22 \times PL + 249,66$

l'expérimentation. La pente de la droite, représentée par le coefficient α, indique la valeur associée à chaque nouvel équipement. Cette valeur diffère fortement selon l'expérimentation mise en place. Ainsi, le temps accordé à chaque équipement est beaucoup plus long lorsque nos données quittent La Réunion que dans le sens inverse, avec un coefficient proche du double. Cela signifie que pour chaque saut supplémentaire, un délai additionnel de $6,22\ ms$ (resp. $11,11\ ms$) doit être pris en compte, lorsque l'on joint (resp.

quitte) La Réunion. On passe quasiment du simple au double.

Nous avons précédemment analysé les *Cumulative Density Function* (CDF) des longueurs des routes logiques par continent. Nous avions constaté pour certains continents, une forte similitude entre les différentes courbes. Cette observation est de nouveau présente ici. Les deux PDF sur la longueur des chemins empruntés sont similaires. Néanmoins, le fait d'avoir un plus grand nombre d'échantillons sur l'expérimentation *Depuis* a permis un lissage de la courbe.

Corrélation entre délai et distance géographique

Dans [Krajsa2011], les auteurs se sont intéressés à l'impact de la distance sur le RTT. Les résultats ont été obtenus a partir d'une étude de métrologie active réalisée dans des pays à forte connectivité, en terme de liaisons sous-marines. Les auteurs ont déterminé une fonction linéaire représentée par l'équation suivante :

$$y = 0,0128 \times x \tag{2.3}$$

Cette équation prédit le délai en fonction d'une distance géographique donnée. Nous allons étudier la pertinence de ce modèle dans le cas de l'île de La Réunion. On se réfère à ce modèle par la notation *Expected Internet RTT for a given geographical Distance (EIRD)*.

La figure 2.11 est composéee de trois parties. En haut, nous avons représenté les distances couvertes par chaque continent. La figure 2.11a (resp. fig. 2.11b) graphe la fonction *Expected RTT (ER)* pour le cas *Depuis* (resp. *Vers*) et le modèle EIRD. Le modèle ER(d) vient de la représentation sous forme linéaire de l'impact de la distance géographique sur les délais obtenus. Nous avons également représenté les 5^{eme}, 10^{eme}, 25^{eme}, 75^{eme}, 90^{eme} et 95^{eme} percentiles. Les points présents à l'intérieur des barres d'erreurs indiquent le 50^{eme} percentile. Au bas de chaque figure, la PDF de la distance géographique est représentée.

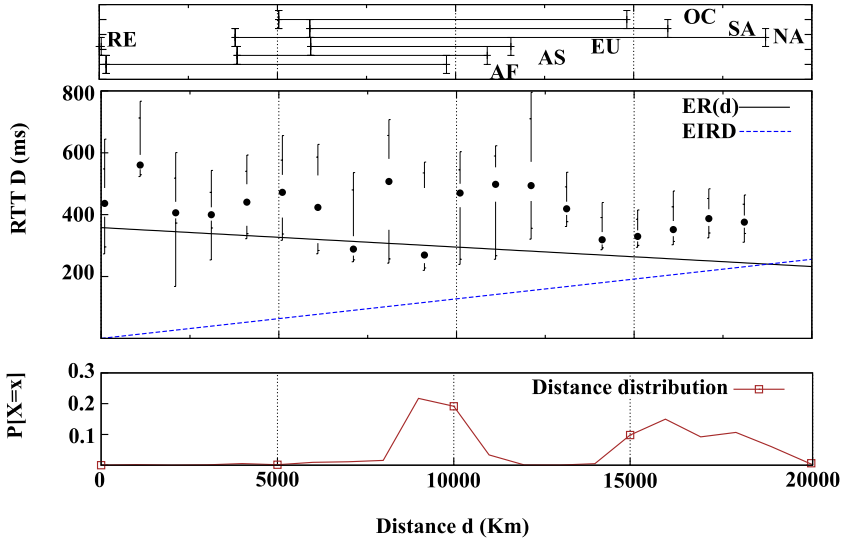
L'étude de la répartition de nos destinations (resp. sources) pour notre étude montre que les distances vont d'une valeur inférieure à 10 km jusqu'à près de $20\ 000$ km. Nous constatons un regroupement des continents entre $5\ 000$ et $10\ 000$ km pour l'étude *Depuis*. Le regroupement se fait à une distance plus grande (comprise en $7\ 500$ et $14\ 000$ km) pour *Vers*. Ces valeurs sont remarquées dans la PDF de chaque étude. Malgré la présence seule du continent Nord Américain après $15\ 000$ km, la densité de probabilité d'avoir une destination prise dans cet ensemble est importante.

Les figures montrent une complète opposition entre le modèle EIRD et nos résultats. Afin d'effectuer une meilleure comparaison, nous avons traduit nos résultats sous la forme $ER(d) = \alpha \times d + \beta$, fonction linéaire du délai en fonction de la distance géographique. Une représentation graphique de $ER(d)$ est indiquée sur les figures. Les équations obtenues sont indiquées dans le tableau 2.9.

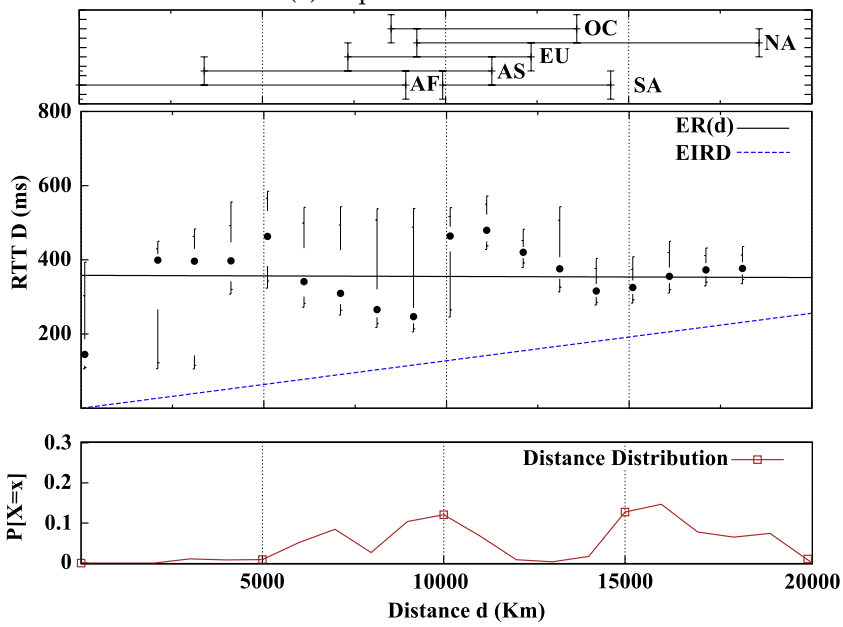
TABLE 2.9 – Formule d'estimation du délai en fonction de la distance géographique.

Expérimentation	Équation d(t)	R^2
EIRD	$y = 0,0128 \times t$	$0,9794$
ER(d) (Depuis La Réunion)	$y = -62,92 * 10^{-4} \times t + 477,6$	$16,80 * 10^{-3}$
ER(d) (Vers La Réunion)	$y = -29,4 * 10^{-5} \times t + 358,1$	$14,81 * 10^{-5}$

Les coefficients de détermination (R^2) entre les fonctions linéaires et nos données indiquent que nous n'avons pas pu trouver de modèle de prédiction suffisamment précis, contrairement au modèle EIRD. Nous constatons également que les pentes de nos modèles ER(d) sont toutes deux négatives. Cela signifie que le délai sera plus court pour



(a) Depuis La Réunion.



(b) Vers La Réunion.

FIGURE 2.11 – Relation entre les délais et la distance géographique.

joindre une distance éloignée physiquement, dès que l'on emprunte les câbles sous-marins. La présence du GIX *Reunix* sur l'île permet d'avoir des délais courts du moment que l'on reste sur la boucle locale *Gazelle* (cf. section 2.1). Par exemple, le délai pour joindre un pays européen est plus court que le délai pour joindre les pays de la ZOI. Ce résultat est contraire à l'analyse *EIRD*. Il peut s'expliquer en partie par le fait l'étude présenté dans [Krajsa2011] est réalisée dans des lieux où la connectivité (en terme de liaisons sous-marines) est importante.

La partie d'analyse des routes empruntées va nous aider à valider ou infirmer l'hypothèse suivante : *Les coefficients α obtenus sur nos équations* ER(d) *proviennent du routage.*

Analyse des routes

Dans la section 2.2, nous avons montré l'existence de liens physiques reliant l'ensemble des îles de la ZOI. Nous cherchons à caractériser l'efficacité des routes empruntées

d'un point de vue géographique. La figure 2.12 représente les différents points d'entrées et de sorties logiques de l'Internet réunionnais que nous avons extraits de nos données.

Des données obtenues de l'étude *Depuis*, nous avons extrait le pays du premier nœud basé à l'extérieur de l'île. Cette information nous permet d'étudier les sorties logiques de l'Internet réunionnais. Le résultat obtenu est indiqué par la figure 2.12a. La taille du lien est proportionnelle au nombre d'échantillons passant par ce pays. Nous dénombrons 4 sorties, dont 3 en Europe. Malgré l'absence de lien direct avec l'Amérique du Nord depuis La Réunion, nous avons identifié une sortie dans la moitié ouest des États-Unis. Les sorties physiques directes de La Réunion, qui sont basées en Afrique, Asie et sur les îles de la ZOI, ne sont pas utilisées. La majorité du routage de nos données, avec près de 97%, s'effectue en France.

Dans la figure 2.12b, nous indiquons le dernier équipement localisé en dehors de La Réunion pour une destination finale localisée sur l'île. Ce sont les entrées logiques de l'Internet réunionnais que nous avons pu obtenir des données provenant de l'étude *Vers*. Le nombre d'entrées est double par rapport au nombre de sorties et plus réparti en terme de continent. Quatre continents sont directement reliés à notre île, l'Afrique, l'Asie, l'Europe et l'Amérique du Sud. Le continent européen est largement représenté dans nos données avec $99,51\%$ transitant sur ce territoire. La France hexagonale capte $99,33\%$ des données, soit la quasi-totalité de nos données. Nous avons tout de même pu identifier des liaisons minimales avec l'Afrique du Sud, l'Inde, le Sri Lanka et le Paraguay. Ce dernier est le seul à ne pas être directement relié à l'île par un câble sous-marin.

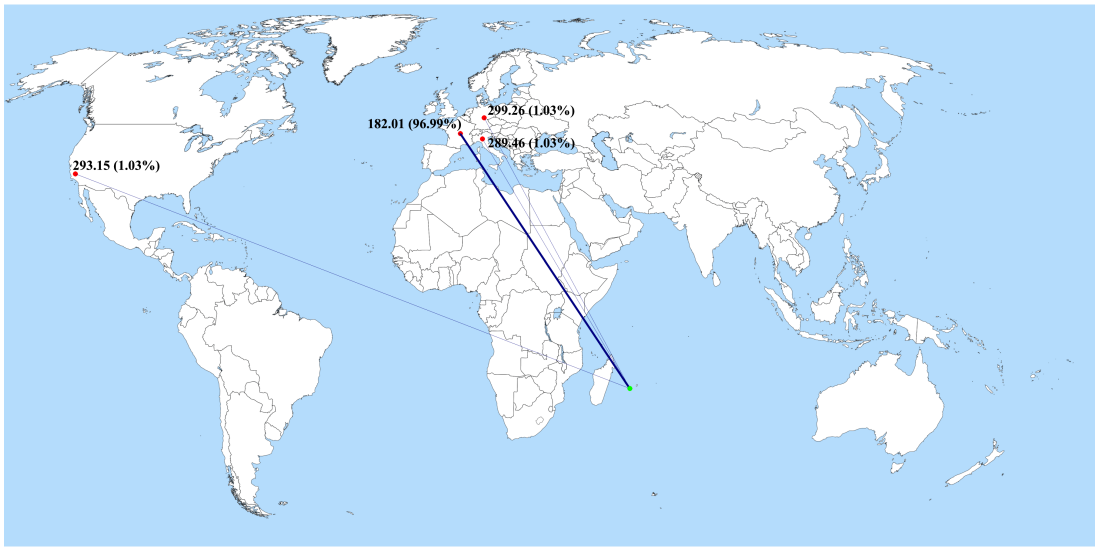
Le tableau 2.10 résume les informations contenues dans les figures 2.12a et 2.12b. Les lignes sont rangées par taux d'utilisation décroissant.

TABLE 2.10 – Tableau récapitulatif des points d'entrées/sorties de l'Internet réunionnais.

Depuis La Réunion	Vers La Réunion
	France (99,33%) 183,30 ms
	Afrique du Sud $(0,45\%)$ $66,42$ ms
France (96,99%) 181,01 ms	Belgique $(0,1\%)$ $197,48$ ms
Allemagne $(1,03\%)$ $299,26$ ms	Italie $(0,04\%)$ $202,59$ ms
État-Unis $(1,03\%)$ $293,15$ ms	Slovénie $(0,04\%)$ $205,50$ms
Italie $(1,03\%)$ $289,46$ ms	Inde $(0,01\%)$ $161,45$ ms
	Paraguay $(0,01\%)$ $454,36$ ms
	Sri Lanka $(0,01\%)$ $207,88$ ms

La présence de liens directs entre La Réunion et des pays beaucoup plus éloignés, tels que les États-Unis ou le Paraguay, sans câbles physiques directs, est symptomatique de l'absence d'informations ou d'erreurs de géolocalisation. Nous pouvons présenter et expliquer quelques points présents dans nos résultats.

1. Les erreurs de géolocalisation. Les erreurs de géolocalisation sont principalement dues à une mauvaise utilisation des blocs d'adresses IP par les opérateurs. Ils préfèrent utiliser des adresses qui leur ont déjà été attribuées que d'effectuer une demande d'adresse IP auprès d'un RIR. Un exemple est l'adresse IP '194.167.142.21'. Cette adresse est attribuée à l'opérateur français RENATER. Comme RENATER possède la nationalité française, le pays de localisation de l'adresse est 'FRANCE'. Or, il s'avère que cette adresse est utilisée comme adresse publique de l'Université de La Réunion. Elle est donc localisée sur l'île. Un raisonnement similaire peut s'effectuer sur les autres régions d'outre-mer possédant des relations avec l'opérateur RENATER. Les filiales d'opérateur métropolitain comme Orange peuvent également utiliser ce système sur l'ensemble de leur réseau. Pour résoudre ce problème,



(a) Sorties.

(b) Entrées.

FIGURE 2.12 – Entrées / Sorties logiques de l'Internet réunionnais.

nous avons effectué une analyse du délai. Si le délai associé à certaines adresses IP correspond au délai théorique associé au continent, nous avons considéré que la géolocalisation est correcte. Dans les cas contraires, nous n'avons pas la possibilité d'être sûrs à 100% de la bonne localisation.

2. Les accords de *peering* se font dans un pays avant que le paquet n'emprunte le câble sous-marin. L'exemple illustré par la figure 2.13 montre que les échanges entre deux adresses IP s'effectuent au sein d'un IXP. Ces échanges peuvent se faire entre deux pays distants au sein d'un troisième pays. Dans notre exemple, l'échange entre La Réunion et les USA se fait en France.
3. L'encapsulation des données au sein du système MPLS génère également des incohérences au sein de nos analyses. L'exemple que l'on peut indiquer est l'analyse de la mesure numérotée 4178740[2] chez Atlas RIPE NCC. Cette trace est composée de 5 sauts entre le Paraguay et La Réunion, avec un lien direct. Or il n'existe aucun câble physique entre ces deux points du monde. Une encapsulation au niveau *In-*

2. https://atlas.ripe.net/measurements/4178740/

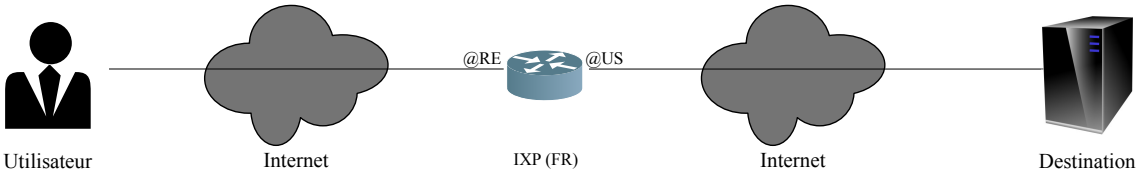


FIGURE 2.13 – Exemple de *peering* entre deux pays à travers un point d'échange basé dans un pays tiers.

visible des données n'indique pas le parcours précis des données, tel que l'indique l'auteur de l'article [Donnet2012].

Ces explications ne sont pas les seules, mais potentiellement les plus fréquemment rencontrées. Dans notre cas, les points 2 et 3 semblent être les raisons prédominantes. Les marques du système MPLS sont dues à la division de la capacité des câbles pour les différents opérateurs et à la connexion en différents points pour régénérer le signal.

Des résultats de nos études, nous déplorons l'absence de *peering* régional. Cette anomalie est la principale cause de la tendance des courbes obtenues dans le tableau 2.9. En étudiant les différents IXP, nous constatons l'absence d'opérateurs communs entre les 3 îles, comme l'illustre la figure 2.14. Ces informations proviennent directement des sites internet officiels des IXP [MIXP2017, MGIX2017, REUNIX2017]. On peut néanmoins noter la présence des filiales de l'opérateur Orange à Madagascar et à La Réunion. Il s'agit, dans le cas d'Orange Madagascar, de l'exploitation du nom sans être dirigée par l'entreprise Orange. De cette figure, on peut déduire que les échanges d'informations et de données se font dans une région éloignée de la ZOI et à un niveau plus élevé. On peut supposer que ce sont des Tiers-1 qui se chargent du *peering* de cette zone. Afin de valider cette hypothèse, nous avons déployé des sondes de mesures de RunPL sur les îles voisines.

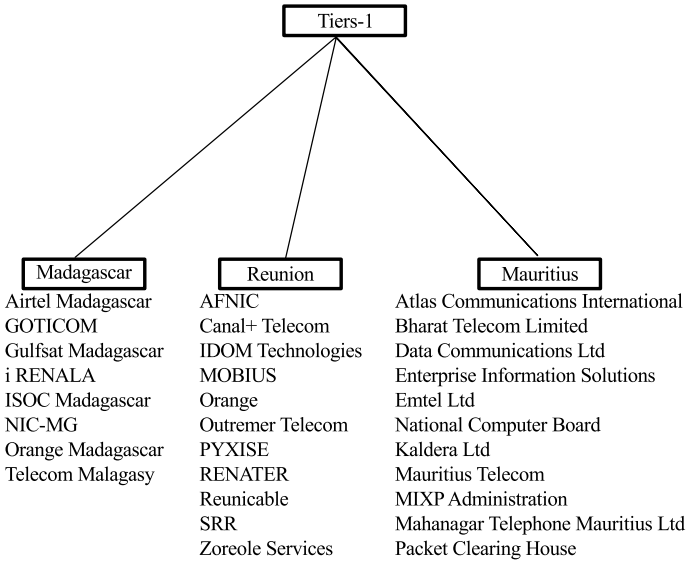


FIGURE 2.14 – FAI présents dans chacun des 3 IXP de la Zone Océan Indien.

2.4.3 Connectivité des îles de la Zone Océan Indien

Nous avons vu dans la section 2.2 que les îles de la ZOI partagent des routes physiques en commun. Nous avons constaté dans la section 2.4.2 que La Réunion possède

une connectivité Internet particulière. Nous sommes donc en droit de nous demander si cette connectivité est commune à l'ensemble des îles de la ZOI ou non. Nous avons pu déployer un minimum de deux sondes par pays étudié. Le protocole de mesure et d'analyse mis en place est en tout point identique à celui utilisé pour l'étude de la connectivité de La Réunion. Ainsi, nous avons utilisé les mêmes métriques pour valider la comparaison.

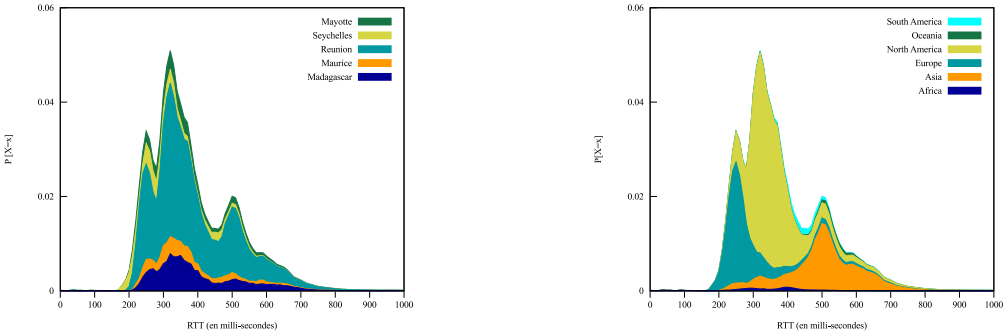
Distribution du RTT par pays étudié

La figure 2.15 illustre la répartition des délais des îles de la ZOI selon le pays d'origine des mesures (2.15a) et du continent de destination (2.15b). Comme pour La Réunion, nous remarquons la présence des trois pics.

D'après la figure 2.15b, ces pics ont la même signification que dans la situation précédente, c'est-à-dire la présence des délais pour joindre l'Europe, l'Amérique du Nord et l'Asie.

Sur la figure 2.15a, on remarque également des valeurs minimales et maximales différentes selon le pays. Ainsi, les Seychelles ont les délais les plus courts de la ZOI. À l'inverse, c'est La Réunion qui possède le plus de délais au delà des 800 ms.

Le comportement des délais étant communs à l'ensemble de la ZOI, nous allons maintenant étudier la longueur des routes pour chaque île étudiée.



(a) En fonction de l'île source.

(b) En fonction du continent de destination.

FIGURE 2.15 – Distribution des délais des îles de la ZOI.

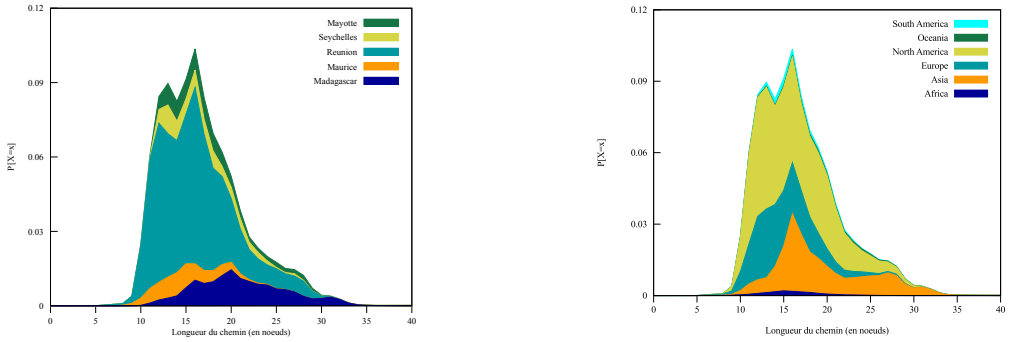
Longueur des routes par pays étudié

La figure 2.16 représente la densité de probabilité de la longueur des routes. En confondant les destinations, nous pouvons étudier la répartition de la distance en fonction de l'île source (2.16a). Nous avons appliqué le même raisonnement en mélangeant les îles sources pour se concentrer sur la destination (2.16b). Les figures étudiées n'ont pas la même forme que celles uniquement dédiées à La Réunion. En effet, la courbe 2.16 possède 2 pics.

Sur la figure 2.16a, on remarque que cette différence est fortement accentuée par la présence des données réunionnaises.

Sur la figure 2.16b, on voit une différence de comportement en fonction du contient joint. Ainsi, l'Afrique, l'Asie et l'Europe ont la présence d'un seul pic. Cela signifie que ces continents seront majoritairement joints par des routes comprises entre 10 en 20 sauts. Pour les Amériques et l'Océanie, il y a deux pics. Cela sous-entend la présence de deux "grandes" routes, avec l'une plus courte que l'autre. La plus petite est composée de 13 sauts. La seconde route est quant à elle d'une longueur de 16 sauts.

Cette différence peut s'expliquer par la présence de routes empruntées différentes en fonction des pays de destinations. Pour corroborer cela, nous allons poursuivre l'étude en fonction des métriques présentées dans la section 2.4.2.



(a) En fonction de l'île source.

(b) En fonction du continent de destination.

FIGURE 2.16 – Longueur des routes empruntées.

Longueur du chemin et distance géographique

Dans cette section, on va étudier la relation entre la longueur du chemin et la distance géographique. On a vu à travers le résultat précédent que le choix du continent avait un impact sur la longueur du chemin. Pour plus de lisibilité, nous avons représenté les résultats sous la forme d'équations linéaires, représentés par l'équation 2.4.

$$PL(d) = \alpha \times d + \beta \tag{2.4}$$

Les équations obtenues sont indiquées dans le tableau 2.11 et représentées graphiquement par la figure 2.17.

TABLE 2.11 – Formule de corrélation de la longueur du chemin en fonction de la distance géographique.

île de départ	Équation PL(d)
Madagascar	$y = -0,000303631 \times d + 26,1771$
Maurice	$y = -0,000183807 \times d + 18,4231$
Réunion	$y = -9,18819 * 10^{-5} \times d + 17,1201$
Seychelles	$y = -0,000183362 \times d + 18,9892$
Mayotte	$y = -7,15288 * 10^{-5} \times d + 18,4781$

Nous pouvons séparer nos résultats en 3 groupes. D'un côté, les départements français avec La Réunion et Mayotte. Dans un second groupe, l'île Maurice et les Seychelles. Et dans un troisième groupe, Madagascar. Les résultats de La Réunion et de Mayotte sont similaires. La pente α est quasi-nulle et l'écart sur le coefficient β est de 1 saut. Ce résultat est similaire à celui obtenu précédemment. Maurice et les Seychelles ont également des coefficients proches. Les pentes sont légèrement négatives. Cela implique une petite dépendance du nombre de sauts en fonction de la distance géographique. Le cas le plus intéressant est Madagascar. Nous allons nous intéresser plus en détail à son comportement.

Madagascar possède les coefficients α et β les plus élevés. Cela signifie que le pays possède une route minimale plus longue que les autres îles. Son coefficient α négatif

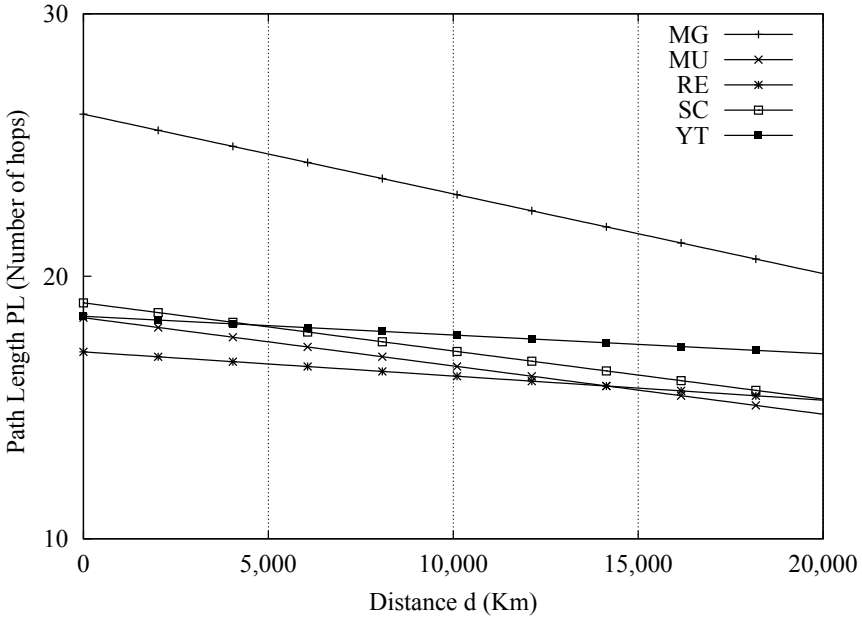


FIGURE 2.17 – Relation entre la longueur de la route et la distance géographique.

est presque deux fois plus élevé que pour Maurice et les Seychelles. L'impact de la distance sur le nombre de sauts est donc plus fort. La figure 2.18 a été réalisée selon le même schéma que les figures 2.8. La représentation de la PDF de la distance des destinations par rapport aux sondes déployées à Madagascar montre deux grands groupes. Le premier situé entre $5\,000$ et $10\,000$ kilomètres. Ce groupe regroupe Asie, Europe, Océanie et Amérique du Sud. Le second groupe, évoluant aux alentours des $15\,000$ kilomètres, englobe la totalité des adresses IP géolocalisées en Amérique du Nord. Le nombre d'adresses provenant du continent africain est compris entre 0 et $10\,000$. La pente négative suggère donc que les routes vers les continents éloignés sont plus courtes que les routes vers des destinations proches géographiquement. Néanmoins, la lecture des cercles montre des routes globalement aussi longues quel que soit le continent.

Impact de la longueur du chemin sur le RTT

Tout comme la section précédente, nous avons représenté les résultats sous forme d'équations linéaires. Le tableau 2.12 regroupe les équations obtenues, tandis que la figure 2.19 les représente graphiquement.

TABLE 2.12 – Formule de corrélation de la longueur du chemin en fonction de la distance géographique.

île de départ	Équation D(PL)
Madagascar	$y = 13,5709 \times t + 119,717$
Maurice	$y = 14,296 \times t + 171,69$
Réunion	$y = 14,2259 \times t + 166,84$
Seychelles	$y = 17,3953 \times t + 35,3596$
Mayotte	$y = 16,3138 \times t + 90,9087$

Comme on pouvait s'y attendre, le délai s'accroît avec le nombre de sauts. Les coefficients α obtenus sont proches les uns des autres. La différence se fait plus sur la valeur d'ajustement β. Cette valeur correspond au délai minimal. Les Seychelles ont la pente

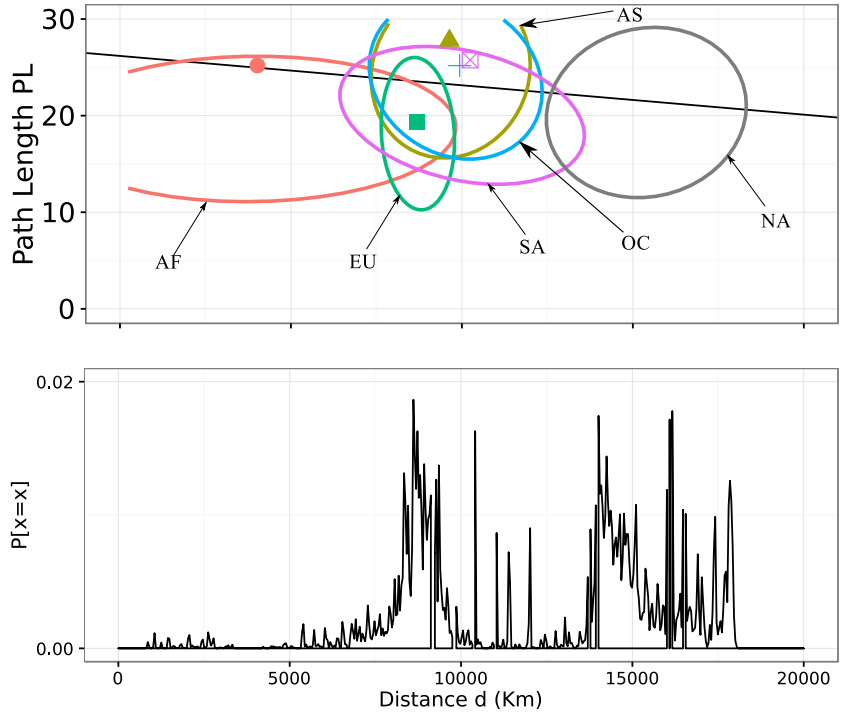


FIGURE 2.18 – Relation entre la longueur de la route et la distance géographique pour Madagascar.

la plus élevée et la valeur d'ajustement la plus basse. Cela signifie que malgré un délai minimal faible, le temps mis par un paquet dans chaque routeur est plus important que pour les autres îles. Mayotte est sensiblement dans le même cas. Pour Maurice et La Réunion, les pentes sont proches et la valeur de β également. Ces deux îles auraient donc un comportement similaire.

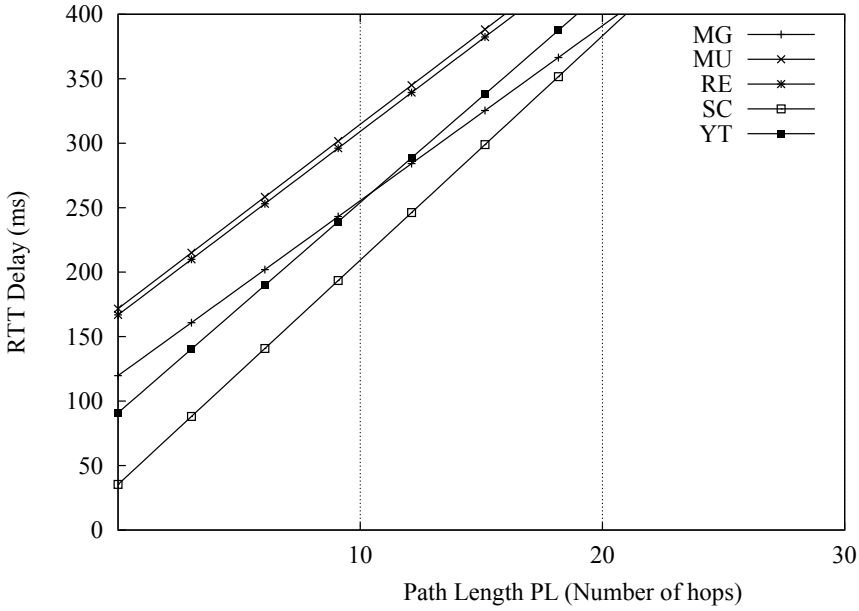


FIGURE 2.19 – Relation entre la longueur de la route et les délais.

Corrélation entre délai et distance géographique

Nous avions vu que pour La Réunion, il y avait une incohérence sur la relation entre le délai et la distance géographique. En effet, nous avions comme résultat le fait que le délai décroissait avec la distance. Ce schéma se reproduit également pour les autres îles de la ZOI, tel qu'illustré par la figure 2.20. Les équations associées à chaque pays sont présentées dans le tableau 2.13.

TABLE 2.13 – Formule de corrélation de la distance géographique et du RTT.

île de départ	Équation PL(t)
Madagascar	$y = -0,0053913 \times t + 476,626$
Maurice	$y = -0,00418997 \times t + 438,177$
Réunion	$y = -0,00370839 \times t + 440,249$
Seychelles	$y = -0,00344991 \times t + 368,501$
Mayotte	$y = -0,0015904 \times t + 397,1$

On constate des pentes fortement différentes en fonction des pays. Ainsi Mayotte a une pente beaucoup plus douce que les autres îles. Malgré un β proche, on voit que l'écart des délais entre La Réunion et Maurice s'accroît avec la distance. La pente de Madagascar est très importante. Ça indique une forte décroissance du délai avec la distance. Ainsi le délai pour joindre l'île Maurice sera beaucoup plus important que pour joindre les pays d'Amérique du Nord.

L'une des conséquences de ces résultats est la présence d'un délai plus élevé pour joindre les îles de la ZOI que pour joindre des destinations plus lointaines. Et cela malgré des routes toutes aussi longues. Cela montre une contradiction à travers nos résultats. Pour comprendre cela, il est nécessaire d'étudier les portes de sorties de l'Internet des îles de la ZOI.

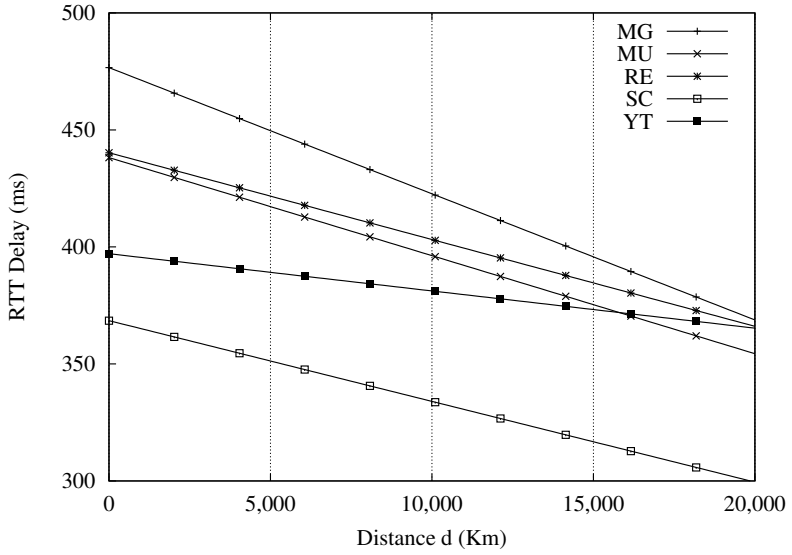


FIGURE 2.20 – Relation entre les délais et la distance géographique.

Analyse des portes de sortie

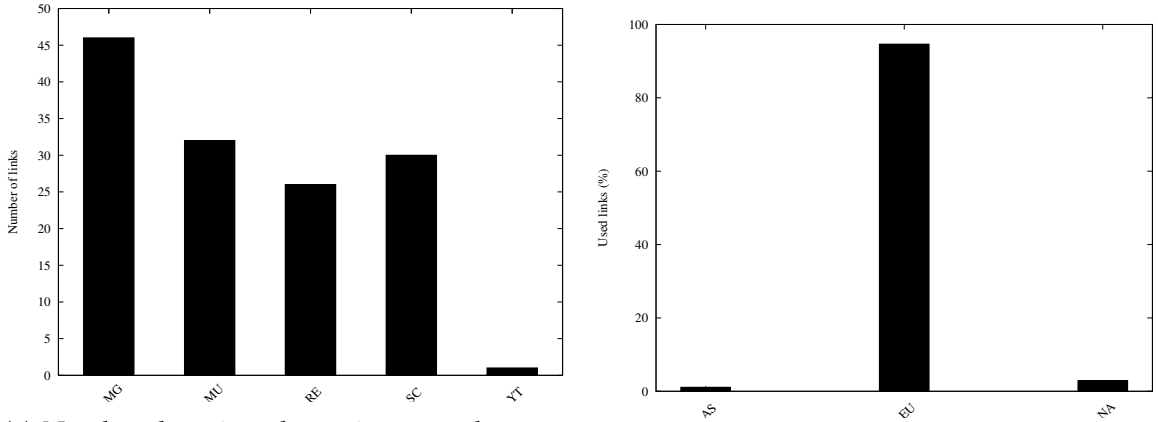
Chaque île de la ZOI possède ses propres routes, avec ses propres règles et ses propres sorties. À la fin de la section 2.4.2, nous avons émis l'hypothèse suivante : *les échanges de*

paquets entre les FAI des îles de la ZOI ne se font pas au sein de la ZOI.

La figure 2.21 indique le nombre de sorties que l'on a pu relever durant nos mesures (2.21a) et le pourcentage de leur répartition géographique (2.21b).

En analysant la figure 2.21b, on constate que la majorité des pays de sortie est située en Europe, avec 94,63%. On remarque l'absence de sortie au niveau Africain et d'interconnexion directe entre les îles de la ZOI.

Sur la figure 2.21a, on remarque qu'à l'exception de Mayotte, chaque pays a plus de 20 sorties différentes. Pour La Réunion c'est un résultat fortement différent de celui obtenu dans la section 2.4.2. Cela peut s'expliquer par les mêmes raisons que lors de l'étude précédente, pour rappel les raisons invoquées sont potentiellement des erreurs de géolocalisation, des accords de peering direct dans un pays tiers ou encore de l'encapsulation MPLS.



(a) Nombre de points de sorties pour chaque île de la ZOI.

(b) En fonction du continent.

FIGURE 2.21 – Répartition des sorties de l'Internet des îles de la ZOI.

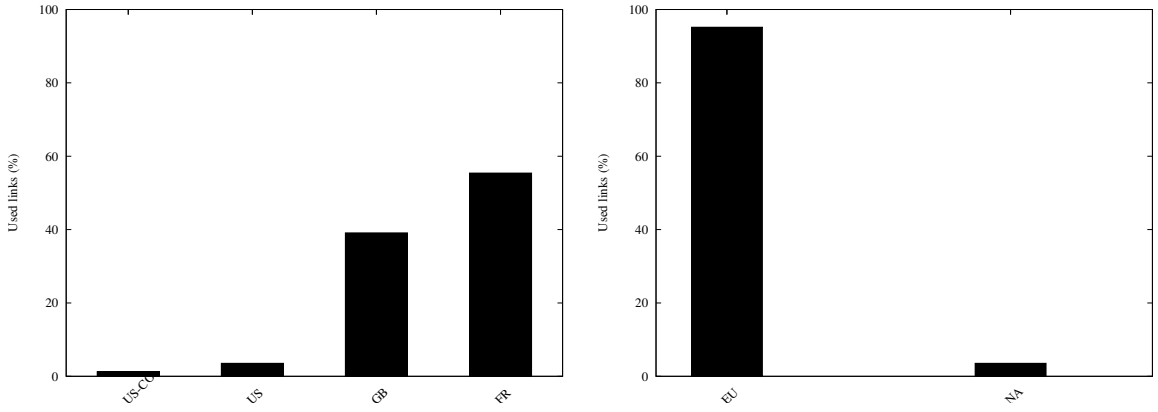
La figure 2.22 montre la répartition des sorties en pourcentage selon les pays (fig 2.22a) et les continents (2.22b) pour La Réunion. En comparaison avec les résultats obtenus précédemment, on constate une forte diminution du pourcentage de sorties géolocalisées en France hexagonale (FR). Nous sommes passés de 96.99% à une valeur de 55.408%. Néanmoins, le pourcentage par continent reste extrêmement élevé avec 95.1636 de sorties localisées en Europe.

À travers l'analyse des points de sorties de l'Internet des îles de la ZOI, nous validons l'hypothèse présentée selon laquelle les accords d'échanges entre opérateurs des îles de la ZOI se font à travers un Tiers-1.

2.4.4 Synthèse des résultats

L'étude des routes et des délais menée durant nos travaux de thèse a été divisée en trois grandes parties. La première consistait à comparer l'état actuel avec une étude réalisée quatre ans auparavant. La seconde phase de métrologie active a mis en avant une analyse plus fine de la connectivité Internet de La Réunion avec l'étude des routes. La dernière partie avait pour objectif de comparer la connectivité Internet de La Réunion avec les autres îles de la ZOI.

La campagne de ping menée à l'Université de La Réunion, au sein du LIM, a montré une réduction de la longueur des routes depuis La Réunion. En dépit de la réduction des routes, nous avons constaté une stabilité des délais, aux alentours des 200 ms.



(a) par pays. (b) par continent.

FIGURE 2.22 – Répartition des sorties de l'Internet pour La Réunion.

Notre seconde étude faite à partir de données de type traceroute, menée depuis différents points de mesures répartis sur l'île, a montré des résultats intéressants. Le premier résultat est la corrélation des délais et de la localisation des destinations jointes depuis l'île de La réunion. Nous avions constaté des pics sur la PDF des délais. Ces pics correspondaient bien à la répartition des continents dans notre jeu de destinations. La longueur des routes est, quant à elle, moins impactée par cette répartition des destinations. Nous avons tout de même trouvé une forte symétrie aux courbes, peu importe le sens de l'étude. À partir de ces données, nous avons étudié les relations suivantes : $\{Longueur\ du\ chemin,\ Distance\ geographique\}$, $\{Longueur\ du\ chemin,\ RTT\}$ et $\{RTT,\ Distance\ geographique\}$. La première concordance a montré que la longueur du chemin n'est pas dépendante de la distance géographique. La seconde corrélation a montré une première asymétrie des liens. En effet, le temps associé à chaque nœud du trajet est très différent selon que l'on quitte ou que l'on essaye de joindre La Réunion. Le dernier rapport a mis en évidence une particularité de l'accès Internet de La Réunion. À l'inverse de tout sens commun, les délais provenant et à destination de La Réunion vont en décroissant en fonction de la distance géographique. L'analyse des routes, et plus particulièrement les points d'entrées et de sorties logiques de l'Internet réunionnais a permis d'expliquer ce comportement.

Notre dernière étude utilise le même protocole et la même plate-forme que l'étude précédente. Nous avons réussi à distribuer des sondes sur les îles de la ZOI. À travers cette étude, nous avons pu constater un comportement proche pour l'ensemble des îles étudiées. Ainsi, nous avons pu trouver des spécificités de l'Internet de la ZOI : La distance géographique a un impact sur la longueur de la route, le délai associé à chaque nœud de la route est similaire. Mais surtout, le délai pour toute destination basée à l'extérieur d'une île est plus long pour les distances géographiques courtes. Ce comportement s'explique par une inter-connexion des FAI régionaux à travers des Tiers-1 situés majoritairement en Europe.

2.5 Conclusion

Dans ce chapitre, nous avons étudié la connectivité de La Réunion en terme de délais et de routes empruntées.

Lors de la première section, nous avons vu que La Réunion ne propose pas d'infrastructure permettant la mise en place de notre étude. La première étape fut le déploiement de raspberry-pi sur l'ensemble de l'île. Ces sondes connectées à l'ensemble des FAI

et TAI utilisent l'outil Paris-traceroute pour réaliser des mesures de délais et de routes. Cet outil est moins sensible au phénomène d'équilibrage de charges que le traceroute traditionnel.

Une fois notre plate-forme déployée, nous avons réalisé des mesures durant plusieurs mois. Ces mesures actives étudient la connectivité depuis et vers La Réunion. Cette volonté d'effectuer les mesures dans les deux sens provient de la forte présence de routes asymétriques dans l'Internet.

Nos données ont montré que La Réunion est confrontée à ce phénomène. Nous avons effectué une analyse selon 4 paramètres : le délai, la distance géographique, la longueur du chemin et les routes empruntées. La littérature ne proposant pas d'outil respectant nos critères de sélection, nous avons développé notre propre outil d'analyse : rTraceroute. Nous avons souhaité partager notre outil d'analyse à travers une publication. Dans l'attente d'une publication scientifique, un site internet dédié à l'outil est disponible [rtraceroute].

Le premier résultat concerne la longueur des routes. Les routes réunionnaises sont plus longues que la moyenne mondiale. On constate également une différence selon le sens de communication. En étudiant l'impact de la distance kilométrique sur la longueur, on voit qu'aucune corrélation n'existe entre les deux paramètres. Les routes Internet de la boucle locale sont aussi longues que les routes reliant des points situés à plus de $15\,000$ km.
Lorsqu'un paquet traverse un nœud, un délai associé au traitement, à l'émission et à la propagation des données vers le saut suivant peut être calculé. Cette valeur diffère énormément selon que l'on quitte ou que l'on joint La Réunion. On a un coefficient de $1,79$ entre les deux valeurs. Cela corrobore l'asymétrie des liens, mais aucunement un comportement spécifique à la connectivité réunionnaise.
L'un des résultats les plus intéressants concerne la relation entre la distance géographique et les délais associés. Contrairement à ce que l'on pouvait attendre, la connectivité réunionnaise décroît les délais avec l'incrémentation de la distance, lorsque le trafic emprunte les câbles sous-marins.
Dans l'analyse des routes, nous avons constaté que l'inter-connexion régionale se fait, non pas au sein de la ZOI mais, dans une zone éloignée. La Réunion possède 3 sorties physiques que sont l'Asie, l'Afrique et l'Europe. Pour autant, seule la France hexagonale semble être intéressante pour les FAI locaux. Plus de 97% de nos données sortent à travers ce pays, localisé à plus de $10\,000$ km.

Nous avons confirmé le fait que l'inter-connexion se fait dans une zone éloignée à travers l'étude de la connectivité de la ZOI. Cette étude a démontré un comportement similaire entre La Réunion et les îles de la zone. La seule différence notable provient du nombre de portes de sorties pour les îles. Néanmoins, elles sont, à une très forte majorité, géolocalisées en Europe.

Le délai minimal mesuré pour La Réunion et la configuration actuelle de la connectivité Internet réunionnaise peuvent avoir des conséquences sur les performances des protocoles de transport comme TCP. Pour vérifier cela, une étude de métrologie passive a été réalisée. Cette étude est présentée dans le chapitre 3.

Les contributions de ce chapitre ont fait l'objet d'une publication scientifique lors de la conférence *Asian INTernet Engineering Conference (AINTEC)* en 2016 [Noordally2016]. Cette publication a été axée sur les résultats réunionnais. Une seconde contribution dédiée à la connectivité des îles de la ZOI a été publiée lors de la conférence *Global Information Infrastructure and Networking Symposium (GIIS)* en 2017 [Nicolay2017-2].

Chapitre 3

Métrologie sur le service de transport à La Réunion

TCP est un protocole de transport dont la performance est dépendante du RTT et du taux de perte des segments. Plus exactement, ces deux paramètres entrent en compte pour déterminer le délai pris par la fenêtre de congestion pour qu'elle atteigne une taille qui couvre le produit délai-bande passante du canal virtuel qui relie la source à la destination. Aussi TCP voit ses performances réduites lorsque ce produit augmente et change de facteur d'échelle. Les résultats obtenus par l'étude de la connectivité de l'île de La Réunion ont montré un RTT minimal de 180 ms pour le trafic quittant l'île de La Réunion (cf. tableau 2.10). Avec les technologies d'accès à haut débit, il devient techniquement possible que des connexions TCP depuis ou vers La Réunion souffrent des symptômes que l'on retrouve avec l'utilisation d'un LFN.

Dans ce chapitre nous allons étudier quel peut être l'impact de la capacité de stockage des canaux de communication depuis et vers l'île La Réunion sur les performances de TCP. Pour cela, nous allons nous appuyer sur de la métrologie passive afin de pouvoir faire des observations sur la performance de TCP. Dans ce chapitre, nous présentons la méthode que nous avons appliquée afin d'estimer par la métrologie le service que nous obtenons à La Réunion. L'objectif ici n'est pas d'obtenir des résultats représentatifs de l'Internet applicables à La Réunion dans sa globalité mais de mener une première expérience pour valider la méthode et les outils que nous pourrions ensuite appliquer auprès des différents opérateurs locaux.

Ce chapitre se compose de quatre sections. La première section 3.1 fixe les objectifs de l'étude de métrologie. Elle présente les métriques à déterminer pour pouvoir atteindre ces objectifs. La partie 3.2 présente la méthode de mise en œuvre de la plate-forme de métrologie. Le protocole de mesure mis en place pour la réalisation d'une étude est présenté dans la section 3.3. Enfin cette section est suivie par la partie 3.4 qui présente les résultats que l'on peut obtenir et l'interprétation qui peut en être faite.

3.1 Objectifs

L'étude des délais aller-retour (RTT) et des routes Internet de l'île de La Réunion que nous avons présentée dans le chapitre précédent a mis en évidence une connectivité spécifique. L'accès à l'Internet passe principalement par la métropole avec un RTT minimal de 180 ms. Ce RTT multiplié par un débit d'accès de 1 Mbit/s, débit théorique minimal proposé dans les différentes offres par les FAI, donne une quantité de données émises par anticipation de $22,5$ Ko. Ce calcul prend comme hypothèse que le goulot d'étranglement est le lien d'accès de l'hôte. Ce produit délai bande passante représente la taille

de la fenêtre d'émission à partir de laquelle une transmission continue de l'émetteur devient possible. Avec une valeur de $22,5$ Ko, cela place le canal de communication de La Réunion dans la catégorie des réseaux à forte capacité de stockage (LFN). Dans la section 2.1, nous avons vu que La Réunion est pleinement intégrée au plan très haut débit de l'état français. Ce plan a pour objectif de déployer une infrastructure de distribution en fibre optique (*Fiber To The Home* (FTTH)) sur l'ensemble du territoire français. Cela aura pour conséquence, si les délais ne sont pas en diminution, d'augmenter la capacité de stockage du canal de communication.

3.1.1 Les objectifs de l'étude

Le lien d'accès de La Réunion conduit à considérer l'Internet avec les caractéristiques d'un réseau à forte capacité de stockage. Ceci est dû à un délai minimal élevé. Avec ce délai des dégradations potentielles des performances de TCP sont envisageables. La mise en place d'une étude de métrologie passive à l'échelle régionale n'a pas encore été réalisée. Les opérateurs ont une connaissance partielle de la situation de l'île. Afin d'obtenir une vision globale de l'usage de l'Internet sur l'île de La Réunion, il nous faut répondre aux différentes questions suivantes :

— Quel est l'impact de l'augmentation de la capacité de stockage sur les performances du protocole TCP ?

— Est-ce que l'augmentation des débits théoriques est récupérée dans les débits mesurés par TCP ?

Dans la section 1.2.3, nous avons présenté l'article [Zheleva2015]. Pour rappel, dans cette publication les auteurs ont mis en avant un changement d'utilisation des services Internet après une augmentation de la bande passante. Nous allons également répondre à des questions orientées vers la supervision du trafic. Ces questions sont les suivantes :

— Quels sont les protocoles de transport utilisés ?

— Quels sont les services les plus fréquents ?

— Quelle est la distribution géographique des services joints ?

Les réponses à ces questions impliqueront l'apparition d'autres questions.

3.1.2 Les métriques de l'étude

Le tableau 3.1 indique les métriques que l'on va étudier. Chaque métrique étudiée sera mise en relation avec une des questions posées précédemment.

Métriques de supervision

La supervision du trafic consiste à analyser le flux général de paquets qui transite au sein d'un équipement comme un routeur ou un commutateur. On parle d'étude macroscopique, telle qu'indiquée dans le rapport [Owezarski2003-1]. Les informations analysées par la supervision sont généralement les informations analysées par un administrateur Réseau ou encore un FAI. En réponse aux questions sur la supervision, nous avons sélectionné dans un premier temps l'**identification des protocoles de transport**. Le champ *protocole* de l'en-tête IP indique le protocole de niveau suivant utilisé dans la partie des données du datagramme Internet [RFC760]. Les valeurs des différents protocoles sont spécifiées en référence [RFC3232, IANA-port].

TABLE 3.1 – Les métriques de métrologie passive.

Métriques			En-tête	Champs
Supervision du trafic	Caractérisation des destinations		IP	Adresses sources et destinations Protocole
	Protocole de transport employé			
	Service utilisé		TCP	Numéro de port
Performance protocolaire	Performance de TCP	Événement de congestion		ECN/NS + CWR, Numéro de séquence
		RTT		Timestamp
		Pertes		Numéro de séquence
		dé-séquencements		
		Retransmissions		
	Débits binaires	Écoulé		Timestamp, Numéro de séquence, fenêtre
		Descendant		
		Montant		
		Utile		
	Caractérisation des flots	Débit		
		Durée		Timestamp
		Longueur		Nombre de paquets échangés

Nous avons vu précédemment que les services évoluent dans le temps et selon les débits [Zheleva2015]. L'analyse du champ *numéro de port* de l'en-tête TCP aide à l'identification du **Service utilisé**. Chaque numéro de port est associé à un service précis défini dans le [RFC776].

En règle générale, le trafic Internet est divisé en trois catégories en fonction de la destination par rapport à la source. C'est le groupe de travail 802 de l'IETF qui est en charge des caractérisations.

— *Local Area Network* (LAN) : « Un réseau de données destiné à desservir une zone de quelques kilomètres carrés ou moins. Parce que le réseau est connu pour ne couvrir qu'une petite zone, des optimisations peuvent être faites dans les protocoles de signal de réseau qui permettent des débits de données jusqu'à 100 Mbit/s. » [RFC1983].

— *Metropolitan Area Network* (MAN) : « Un réseau de données destiné à desservir une zone proche de celle d'une grande ville. Ces réseaux sont mis en œuvre par des techniques innovantes, comme le passage de câbles à fibres optiques dans les tunnels du métro. » [RFC1983]

— *Wide Area Network* (WAN) : « Un réseau, généralement construit avec des lignes séries, qui couvrent une large zone géographique. » [RFC1983]

La répartition des adresses IP de destination va permettre d'identifier le pays où se situe l'information. Cette information peut permettre de connaître la pertinence du lieu d'hébergement de l'information par rapport au service et à l'application utilisée. Nous utilisons pour cela la base de données associée à l'outil rTraceroute, outil d'analyse graphique des traces présenté dans la section 2.2.2. Dans le cas où une adresse IP n'est pas

répertoriée dans notre base de données, l'information sera extraite de la base de données de RIPE NCC, avec l'outil rgeoloc [LanYanFock2015].

Métriques de performance

Le groupe de travail IPPM de l'IETF a défini dans différents documents des métriques de bases, comme la mesure de connectivité [RFC2678], le délai unidirectionnel [RFC2679], le taux de perte unidirectionnel [RFC2680]. Ces deux dernières métriques sont également définies dans le sens aller-retour avec le [RFC2681].

Nous avons comme objectif la comparaison du débit théorique et le débit mesuré. Le calcul du débit mesuré par TCP se fait à travers 3 métriques : le RTT, la taille de la fenêtre d'émission et la probabilité de perte de paquets. Le **RTT** est le délai entre la mise du premier bit de la question sur le câble et la réception du dernier bit de la réponse [RFC2681]. Il est calculé par la différence de temps entre l'émission du paquet et la réception de l'ACK correspondant. Si le RTT est trop important, TCP peut considérer un paquet comme perdu.

Une **perte** est définie comme « l'émission d'un paquet par la source mais non reçu par la destination » [RFC2680]. Si le paquet est perdu, alors TCP va réduire la fenêtre d'émission.

La fenêtre d'émission est calculée à partir du champ *Fenêtre* des segments TCP. Ce champ est défini dans le [RFC6528] comme le nombre d'octets de données commençant par celui indiqué dans le champ d'accusé de réception que l'expéditeur de ce segment est prêt à accepter.

À l'aide de la formule, indiquée par l'équation 3.1, il est possible de calculer le débit mesuré par TCP.

$$Debit = \frac{\frac{Fenetre}{RTT}}{\sqrt{Probabilite\ perte}} \tag{3.1}$$

Les débits mesurés pourront être classés selon qu'ils soient montants, descendants, confondus ou utiles. Cette différenciation s'explique par le fait que la comparaison avec le débit théorique est montant et descendant. Le débit écoulé (*throughput*) correspond « au nombre de paquets ou de bits par seconde » [RFC6201]. Le débit utile (*goodput*) correspond « au nombre de paquets ou de bits utiles (non retransmis) par seconde. »[RFC5166]

L'étude des performances du protocole TCP passe dans un premier temps par l'étude des pertes et des retransmissions.

Une **retransmission** est définie par le [RFC6298] comme étant le « segment le plus ancien qui n'a pas été acquitté par le récepteur TCP. » Pour obtenir le nombre de retransmissions, on regarde les numéros de séquences des segments TCP. Si dans un flot IP, un numéro de séquence apparaît plusieurs fois, alors cela implique la retransmission du paquet. Les retransmissions seront séparées selon la raison de la retransmission (*fast retransmit*) ou retransmissions abusives (*spurious retransmit*).
Le [RFC5681] explique le phénomène pouvant provoquer une retransmission par le mécanisme de *fast retransmit*. La retransmission d'un paquet due au mécanisme de *fast retransmit* est calculée en fonction du nombre d'acquittements dupliqués et de la différence temporelle entre le paquet de données observées et le précédent acquittement.
Les paquets *spurious retransmit* sont des paquets subissant des fausses retransmissions. Si le numéro de séquence du paquet attendu est inférieur ou égal au numéro d'acquittement du précédent ACK, alors le paquet observé est un paquet retransmis abusivement.

Lorsque le paquet est ré-émis, il va se produire du dé-séquencement. Le **dé-séquencement** se définit dans le [RFC6248] : « L'arrivée ordonnée est une propriété que l'on trouve dans les paquets qui transitent par leur chemin, où le numéro de séquence des paquets augmente avec chaque nouvelle arrivée et il n'y a pas de régression. La détection du réordonnancement à destination est basée sur l'ordre d'arrivée des paquets par rapport à une valeur de référence non inversée. »

Les paquets retransmis peuvent également servir à l'identification des **événements de congestion**. Pour identifier ces événements, deux techniques peuvent être mises en place.
La première consiste a étudier la présence des drapeaux ECN et *Congestion Window Reduce* (CWR) dans les en-têtes des paquets TCP [RFC8311].
La seconde technique se propose d'étudier les variations de la fenêtre d'émission de TCP. Cette étude doit être couplée avec l'analyse des phénomènes de pertes et de retransmission autour de cet événement.

Dans la section 1.1.2, nous avons constaté que la capacité de stockage d'un lien est problématique pour les flots courts. Afin de poursuivre l'étude de l'impact de la capacité de stockage des liens de l'Internet réunionnais, nous allons caractériser les flux. La **caractérisation d'un flot** peut se faire selon la durée (temps écoulé entre le premier et le dernier paquet), la taille (nombre de paquets échangés) et le ratio entre la durée et la taille. D'après les travaux réalisés par [Lan2006], un flot se caractérise par la définition suivante : « *a flow is an unidirectional series of IP packets with same source and destination addresses, port numbers and protocol numbers.* » Ce qui peut se traduire par la définition suivante : « un flot est une série de paquets IP avec le même tuple suivant (adresse IP source, port source, adresse IP destination, port destination, protocole IP) ». Dans ce cas précis, une connexion TCP de par son coté bi-directionnel est constituée de deux flots.

3.2 Mise en oeuvre d'une plate-forme de métrologie

La mise en place d'une étude de métrologie passive au sein du territoire réunionnais soulève trois contraintes.

La première est la **mise en place d'un accord de partenariat** avec un ou plusieurs FAI. L'objectif de ce partenariat est la mise en place d'un système d'écoute et de capture de données au sein de leur infrastructure, tout en garantissant une confidentialité maximale à leur clients et à l'entreprise.

Une seconde contrainte est la sélection d'un **outil de mesure**. Cet outil sera capable, non seulement d'écouter les données circulant sur une interface mais également de capturer les données sous diverses extensions.

La dernière contrainte est liée à la sélection d'un **outil d'analyse**. Cet outil sera capable d'apporter un support de réponses aux questions posées précédemment. Il devra répondre à des critères que l'on détaillera par la suite.

Le trafic étant variable d'un instant t à l'instant t+1, nous allons mettre en place un système de capture de données. Ce système permettra l'analyse a posteriori des métriques. En fonction des résultats, d'autres métriques pourront être extraites des données. De plus, la capture nous autorise, après quelques démarches administratives, de partager les traces auprès de la communauté scientifique.

3.2.1 Pour la capture du trafic

Nous avons vu dans le chapitre 1 que les outils nécessaires à la réalisation d'études de métrologie passive sont nombreux. Notre analyse sera la plus large possible en terme de

métriques. Nous devrons, en fonction des résultats obtenus, étudier d'autres métriques que celles choisies en premier lieu. Pour ces raisons, nous faisons le choix de réaliser des captures du trafic. Dans la section 1.2.3, nous avons présenté les outils disponibles pour la capture de trafic. Nous allons dans un premier temps utiliser une solution logicielle. Dans le cas où les débits sur les liens seraient trop élevés, nous basculerons alors vers une solution matérielle.

3.2.2 Pour analyser les traces

De nombreux outils d'analyse de traces existent dans la littérature. Afin d'en choisir un, nous allons détailler des critères de sélection. Nous présenterons quelques outils d'analyse existants en mettant en avant leurs réponses aux critères présentés. Nous finirons par la présentation d'un outil d'analyse de traces développé au sein du LIM.

Définition des critères

L'outil d'analyse pour la plate-forme de métrologie passive devra répondre aux critères de sélection suivants :

1. **Protection de la vie privée** des utilisateurs. Pour respecter ce critère, une fonction d'anonymisation des traces doit être appliquée. La loi Informatique et Liberté de 1978 réglemente le traitement des données personnelles [LIL1978]. Une trace est une écoute d'un trafic initié par un utilisateur. Les données transportées n'ont pas à être lues. En plus des données ce sont aussi les adresses IP qui ne doivent pas apparaitre en clair.
2. **traiter une volumétrie importante**. Le volume des traces étant variable, il est nécessaire que l'outil soit capable de traiter des traces de grande taille. Potentiellement ce sont des fichiers de traces de plusieurs dizaines de Go (Giga-octets) qui peuvent être amenés à être traités.
3. **proposer des métriques adaptées**. Pour réaliser une analyse approfondie, il faut que la liste des métriques proposées par l'outil d'analyse soit la plus large possible. À ce titre, nous avons présenté dans le tableau 3.1, une base de métriques a analyser.

Les outils d'analyse disponibles

Il existe de nombreux outils d'analyse de données de métrologie passive. Nous proposons une classification selon les possibilités offertes par chaque outil. CAIDA propose, sur son site internet, une partie dédiée aux différents outils de métrologie passive [CAIDA-Tools].

BRO est un outil pour la détection d'intrus sur le réseau en temps-réel à partir de métrologie passive. Il est présenté pour la première fois dans l'article [Paxson1999]. À partir d'un système de script, il accepte en entrée des fichiers de taille importante. Le principal défaut de Bro par rapport à nos critères de sélection est le non-respect de la vie privée.

CoralReef [Moore2001] est une suite logicielle développée par CAIDA en 1999. Cet outil réalise des analyses de données, que ça soit en temps réel ou sur des traces. Le critère de respect de la vie privée, tel que nous l'avons défini précédemment, n'est pas respecté. L'outil est plus adapté à l'étude des caractéristique du trafic qu'au performance de TCP. Ainsi les métriques liées à l'étude des performances ne sont pas incluses dans le code de l'outil.

Netflow est un outil propriétaire. Il nécessite l'utilisation d'un matériel de la marque CISCO, plus la licence du logiciel. L'outil réalise principalement la supervision du trafic

transitant sur le matériel. Le respect de la vie privée est ici respecté mais les métriques de performance protocolaire ne sont pas inclues.

TCPStat [Herman2001] rapporte certaines statistiques du trafic transitant à travers une interface réseau. C'est un outil qui peut travailler sur un flot en temps réel ou en analysant un fichier de trace. Cet outil ne permet pas l'anonymisation des adresses IP. Peu de métriques sont ainsi renseignées. On pourrait obtenir les débits et la volumétrie des paquets IPv4 échangés.

TCPTrace [Ostermann2000] est un logiciel qui permet le traitement de traces d'écoute. Outil très complet, il a déjà fait ses preuves sur d'autres projets de métrologie passive. Le critère de respect de la vie privée, tel que nous l'avons défini précédemment, n'est pas rempli. La métrique de caractérisation des destinations et la répartition géographique ne sont pas incluses dans les métriques proposées par l'outil.

Tstat [Mellia2003-1] est un outil qui peut réaliser la collecte et l'analyse du trafic. Cette analyse se fait sur différents niveaux, passant des paquets à la couche applicative. Cette analyse réalise une anonymisation des adresses IP. Les métriques de caractérisations des destinations et de répartitions géographiques ne sont pas intégrées dans l'outil.

Wireshark [Orebaugh2006] est un outil graphique d'analyse réseau très répandu. Cet outil permet de filtrer et d'analyser des données entrantes et sortantes d'un point en temps réel ou sur des traces collectées. Il autorise également la capture et la lecture de traces. L'outil présente des lacunes sur les trois critères présentés.

ZOO est un outil développé dans le cadre du projet Metropolis. Créé par le *Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS)*, le logiciel essaie de trouver un moyen de mesurer la qualité du service, de trouver des paramètres pour définir le processus de trafic et d'aider à émettre un modèle adapté pour le trafic" [Owezarski2004]. Au niveau des métriques présentées, ce sont principalement des statistiques et des informations de supervision qui sont disponibles. L'anonymisation des adresses IP n'est pas incluse dans les caractéristiques de l'outil.

Le tableau 3.1 sert de base pour la réponse aux critères dédiés des métriques. Netflow possède un catalogue de métriques restreint à la supervision du trafic. TCPTrace et Tstat sont des outils qui auraient pu correspondre à nos besoins mais les métriques de caractérisation des destinations et la répartition géographiques sont absentes. N'ayant pu faire un choix sur un outil pouvant répondre à la totalité des critères, nous nous orientons vers le développement d'un analyseur de traces.

Développement de Xanalyse

L'analyse des traces de métrologie passive peut s'effectuer avec de nombreux outils. Dans la section précédente, nous avons présenté les critères de différenciation de ces outils. Tstat et TCPTrace sont des outils très complets. Ces deux outils auraient pu nous convenir. Néanmoins, le temps de traitement des fichiers de volumétrie importante est beaucoup trop important. Dû à cela, nous avons pris le parti de développer un nouvel outil d'analyse de traces : Xanalyse.

Le premier critère concerne le respect de la vie privée. Une approche simple pour anonymiser une adresse IP est de la faire correspondre avec une adresse IP aléatoire. Une telle méthode rend la trace inutilisable dans des situations utilisant la logique des adressages IP. L'anonymisation d'adresse est performante si elle préserve le même préfixe. Autrement dit, si deux adresses IP partagent k-bits de préfixes, leurs équivalences anonymisées conserveront ces k-bits de préfixes en commun. La méthode *crypto-pan*, décrite dans l'article [Xu2002], sert de base à la fonction d'anonymisation mise en œuvre. L'anonymisation s'appliquera que lors de l'affichage des résultats. Nous avons besoin de

l'adresse pour deux métriques de supervision que sont la répartition du trafic et la géolocalisation. Concernant le champ *Données* des paquets TCP, il n'est pas utilisé. L'étude ne recommande que les en-têtes.

Sur l'aspect du traitement d'une volumétrie importante, Xanalyse fut développé avec la volonté de maximiser l'utilisation des ressources de la machine hôte. Pour cela, nous avons eu l'idée d'utiliser la programmation parallèle (*thread*). La parallélisation permet l'exécution de plusieurs instructions simultanément.

Le calcul des métriques fut directement réalisé en considérant leurs définitions dans les différents RFC, tel que nous l'avons décrit dans la section 3.1.2 . Une partie statistique fut également intégrée à notre outil. Des calculs de moyenne, de variance et d'écart-type furent intégrés. Ces calculs se font à la toute fin du programme. Durant le développement, nous avons corroboré l'ensemble de nos résultats avec les résultats de TCPTrace. Cette comparaison a été mise en place pour vérifier l'exactitude de nos résultats. Le développement de l'outil fut réalisé, sous ma direction, dans le cadre d'un stage de fin d'étude de Master 2 [Ravoavahy2017].

Pour finir, nous avons réalisé une validation par comparaison entre Xanalyse et TCPTrace. Le tableau 3.2 montre le bilan de cette comparaison.

TABLE 3.2 – Comparaison de performances.

	TCPTrace	Xanalyse
Temps d'analyse sur une trace de 20 Go	10 jours	7 jours
Temps d'analyse sur une trace de 1 Go	1 Heure	3 Min

Xanalyse se révèle être un outil beaucoup plus rapide que TCPTrace, avec des résultats identiques sur le calcul des métriques. Cet outil est actuellement disponible sur le site du laboratoire à l'adresse suivante : http://lim.univ-reunion.fr/xanalyse.

3.3 Protocole de mesure

Le protocole de mesure présente les différentes phases que l'on souhaite mettre en place durant l'étude. Elles sont ainsi au nombre de cinq : les contraintes réglementaires, la vérification des perturbations, la capture du trafic, la collecte et l'analyse. Ce protocole fut rédigé en prenant en considération les conseils indiqués dans [John2010]. Dans cet article, les auteurs délivrent différents conseils et indications basés sur l'expérience de plusieurs acteurs de métrologie passive.

Notre protocole a été mis en place dans le but de rassurer l'ensemble des acteurs. Ce protocole fut testé dans le cadre d'une étude de métrologie passive du LIM.

Contraintes réglementaires Avant toute étude de métrologie Internet passive au sein de l'Université de La Réunion, il faut obtenir l'autorisation du président de l'établissement. Le président consultera le *Correspondant Informatique et Libertés* (CIL) et le *Responsable Sécurité et Systèmes d'Information* (RSSI) de l'université. Ces personnes définiront, en fonction des objectifs de l'étude, les limites de notre étude, en accord avec les lois françaises. Les limites imposées par la présidence de l'Université, indiquées par le CIL et le RSSI, furent celles autour de la vie privée. À ce titre, nous n'avions pas le droit d'étudier le trafic en temps réel, n'y d'étudier le champ *Données* des paquets TCP. Nous avions également l'obligation d'anonymiser l'ensemble des adresses IP privées rencontrées. La dernière obligation fut la restriction de nos écoutes au LIM. Ces obligations furent respectées dans le développement de l'outil d'analyse.

Afin de ne capturer que le trafic du Laboratoire, nous avons travaillé en collaboration avec la *Direction des Services Informatiques* (DSI) de l'Université. Ce partenariat a pour objectif d'isoler le trafic du LIM dans un *Virtual Local Area Network* (VLAN) spécifique. Un VLAN est « un mécanisme par lequel les hôtes qui résident dans la même infrastructure physique commutée, mais des domaines de diffusion virtuelle séparés, sont adressés à partir du même sous-réseau IPv4 et partagent une adresse IP de passerelle par défaut commune, supprimant ainsi l'exigence d'un sous-réseau IP dédié pour chaque réseau local virtuel (*Local Area Network* (LAN) ou MAN). » [RFC3069] Les VLAN séparent les usagers selon leur autorisations et les types de connexion. Par exemple, un enseignant-chercheur a plus de droits qu'un étudiant. Une personne connectée par connexion filaire a des droits différents d'une personne connectée par à un réseau sans fil. Le RSSI de l'Université ne souhaitant pas obliger les membres du LIM à participer à cette étude, une campagne de prévention fut organisée. Les personnes ayant explicitement émis le souhait de ne pas participer à notre étude seraient de facto connectées à un autre VLAN par la DSI. Au sein du laboratoire, tout le personnel a accepté de participer à notre étude.

Vérification des perturbations La figure 3.1 illustre l'inter-connectivité mise en place pour l'écoute du LIM.
Chaque ordinateur du laboratoire génère un trafic Internet qui passe par le VLAN du laboratoire. Par le système de port-mirroring, le routeur va créer une copie des paquets transitant par le port du VLAN laboratoire. Le paquet copié sera alors redirigé vers la sonde de capture. La sonde de capture aura deux interfaces réseaux. La première (Eth0) sera dédiée à la capture des paquets provenant de la technique de port-mirroring. La seconde carte réseau (Eth1) servira pour l'accès distant à la sonde de capture.
L'ordinateur d'accès possède une clé privée permettant l'accès à distance à la sonde de capture. Cette porte d'entrée sécurisée permet une gestion à distance de la sonde. Les traces collectées seront transférées sur un serveur de stockage dédié au sein du LIM. Le transfert se fera à l'aide de la commande SCP et l'accès sécurisé présenté précédemment. L'accès distant et le transfert des traces font partie intégrante du trafic généré par les membres du laboratoire. Les perturbations peuvent survenir à deux niveaux : au routeur et à la sonde. Au niveau de la sonde d'écoute, le débit affecté en entrée-sortie du VLAN du laboratoire est égal à $1\,000$ Mbit/s. Ce débit est devenu fréquent sur les cartes réseaux vendues sur les ordinateurs grand public. Les caractéristiques de la carte réseau dédiée à la capture accepte un débit maximum égal au débit du VLAN du LIM. On considère alors que le taux de pertes occasionné par la carte de capture peut être négligeable.
Au niveau du routeur, la fonction port-mirroring copie l'intégralité des segments IP entrant sur un port. Le paquet original est redirigé vers l'adresse de destination incluse dans le champ destination de l'en-tête IP. Le paquet forgé au sein du routeur est dirigé vers un port déclaré lors de la programmation de l'équipement. La fonction de port-mirroring fait partie des techniques développées dans le but d'étudier le comportement d'un réseau. [Zhang2007] a étudié les dérives liés à la fonction port-mirroring. Cette fonction nécessite la mise en mémoire tampon des paquets provenant du lien étudié jusqu'à ce qu'ils puissent être transmis sur le lien miroir. Cette mise en mémoire tampon joue sur la synchronisation des paquets entre le lien étudié et le lien miroir. Lors de la transmission des paquets sur le lien miroir, est-ce que la transmission s'est faite dans l'ordre d'arrivée sur le port étudié ? Il y a donc une question d'ordonnancement des paquets à étudier. La mémoire tampon du routeur n'est pas infinie. Il existe donc des cas où la mémoire est remplie, occasionnant à ce moment là des pertes. Les résultats de [Zhang2007] ont mis en avant une différence de synchronisation entre les paquets du lien étudié et les paquets du lien miroir. La différence de synchronisation implique également des erreurs dans le ré-ordonnancement des paquets. Ces erreurs auront pour conséquences des erreurs dans

l'analyse des performances de TCP. Pour résoudre ces problèmes, les auteurs préconisent l'usage d'une carte physique spécifique à l'étude passive, comme les cartes DAG.

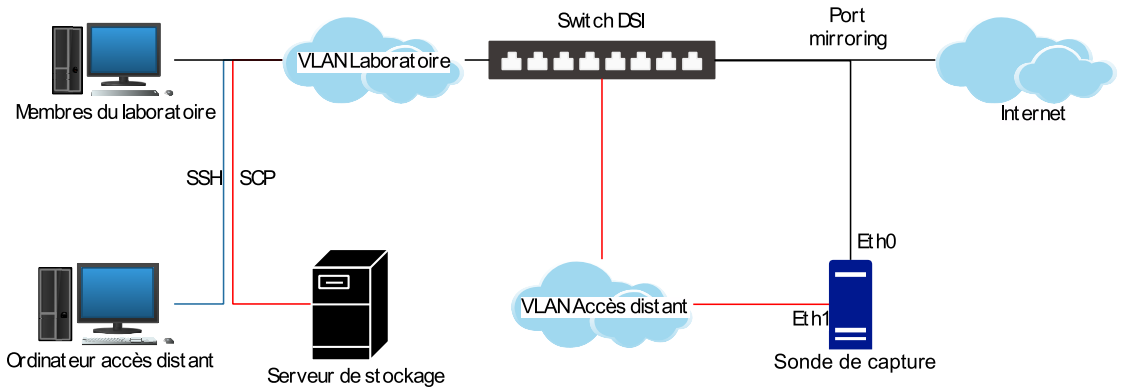


FIGURE 3.1 – Schéma de distribution de la plate-forme de mesure.

Capture du trafic La mise en place des mesures se fait dès la mise sous tension de la sonde et la fin du chargement du système d'exploitation. La capture des données aura une durée comprise entre 1 et 23 heures. Elle s'effectue à l'aide de la commande :

```
tcpdump -i eth0 -w trace-$timestamp.trace &
```

Dans laquelle les options indiquent :

— *-i eth0* : indique l'interface de capture. Nous avons prévu une seconde interface réseau pour l'accès distant sécurisé.

— *-w trace-$timestamp.trace* : cette option désigne le fichier d'écriture. Les fichiers sont nommés par le *timestamp* de début.

Une fois la capture finie, la sonde va décider du temps avant la prochaine écoute. Cette durée n'excédera pas 24 heures. L'objectif est d'avoir des mesures quotidiennes mais programmées de manière aléatoire, sur la durée d'écoute et sur l'écart entre deux mesures.

Le paragraphe de vérifications des perturbations a démontré qu'il est difficile de mettre en place une capture de la totalité des paquets. Une solution de capture est l'échantillonnage. Dans notre cas, nous avons réalisé un échantillonnage indépendant du contenu [RFC5475]. Cet échantillonnage est réalisé sans prendre en considération le contenu du paquet. Ayant une volonté d'obtenir un grand nombre de données, nous avons mis en place une durée de capture maximale de 23 heures et un écart entre deux captures de 24 heures.

Collecte Une phase de collecte des traces est régulièrement réalisée. L'objectif est de libérer de l'espace disque au niveau de la sonde de capture. Lorsque la sonde a fini de réaliser sa capture, elle va envoyer le fichier de capture vers un serveur de stockage, au sein du LIM. Nous avons vu que le fichier de capture est nommé selon une nomenclature spécifique. Pour rappel, cette nomenclature comporte la date (au format *timestamp*) du début de l'écoute. La dénomination du fichier autorise un classement des traces par date de capture. Ce classement peut permettre une étude temporelle du trafic.

L'envoi du fichier se fait à travers l'interface *eth1*. La technique utilisée pour le transfert est la commande SCP. L'utilisation de l'empreinte *MD5* du fichier nous assure que le transfert des données s'est réalisé correctement. En cas de différence entre les empreintes,

le transfert s'effectue à nouveau. L'objectif est de vérifier l'intégrité des données transférés.

Le schéma 3.2 schématise le fonctionnement de notre sonde de mesure. Nous considérons que la fonction de port-mirroring est déjà programmée sur le routeur DSI.

Dès que la sonde est alimentée électriquement et que l'OS est chargé, la sonde va vérifier qu'une capture est programmée. Si aucune capture de trace n'est programmée, la sonde va en planifier une dans les prochaines 24 heures. Si la sonde a connaissance d'une programmation, elle va alors réaliser la capture. La sonde va enregistrer le trafic sur une durée allant entre 1 et 23 heures. Lorsque la capture est finie, la sonde va alors programmer le prochain enregistrement. La sonde va également envoyer la trace vers le serveur de stockage.

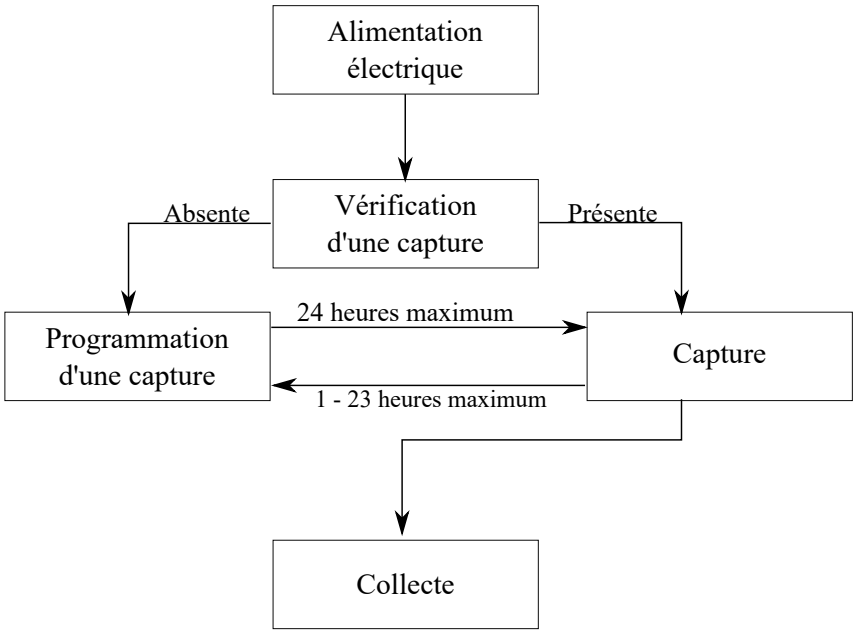


FIGURE 3.2 – Schéma de fonctionnement de la plateforme de mesure.

Analyse L'analyse des données obtenues se fait en deux étapes. La première consiste à utiliser l'outil Xanalyse pour obtenir les résultats bruts. La seconde étape est l'extraction des données pour les représenter sous forme graphique.

3.4 Résultats

Notre étude se cantonne à mesurer les performances du trafic au sein du LIM. Le LIM fait partie intégrante de l'Université de La Réunion et à ce titre, les usages de l'Internet au sein de l'établissement sont réglementés. Ainsi l'étude des métriques de supervision pourraient ne pas correspondre à un usage plus libéral de l'Internet. Pour rappel, les métriques étudiées sont indiquées dans le tableau 3.1.

Nous avons fait le choix de séparer notre étude en deux. La partie *supervision* donne un aperçu de l'usage du réseau Internet au sein du LIM. Nous essaierons dans la mesure du possible de faire des extrapolations avec l'usage de l'Internet à La Réunion. La section *performance* est celle qui est la plus intéressante. C'est elle qui va nous indiquer les dégradations occasionnées par les longs délais pour La Réunion.

3.4.1 Supervision du trafic

Le tableau 3.3 montre la distribution des 4 protocoles de transport rencontrés.

TABLE 3.3 – Distribution des protocoles encapsulés dans IP.

Protocole	ICMP	IGMP	TCP	UDP
Pourcentage	5,72	0,01	92,49	1,78

La présence du protocole ICMP à plus de 5% s'explique par la présence des sondes de mesures de *RunPL*. Pour rappel, l'objectif de cette plate-forme est d'étudier la connectivité de La Réunion et des îles de la Zone Océan Indien à travers de la métrologie active. Nous avons dans le chapitre 2 présenté des résultats liés à ces études. L'usage du protocole ICMP est fréquent au sein de l'Internet. Une étude du trafic réunionnais mettrait également l'usage de ce protocole.

Le protocole *Internet Group Management Protocol* (IGMP), défini dans le [RFC3376], est un protocole utilisé par les systèmes IPv4 (hôtes et routeurs) pour signaler leur appartenance à un groupe de multidiffusion IP à tout routeur multicast voisin. Son usage est restreint au sein d'un réseau privé.

Le protocole *User Datagram Protocol* (UDP) a une présence inférieure à 2%. Son rôle est la transmission de données simples sans fiabilité. Son usage est généralement limité au service DNS. Récemment, l'entreprise Google a développé l'option *QUIC*. *QUIC* permet au navigateur *Google Chrome* d'effectuer des requêtes *HyperText Transfer Protocol* (HTTP)/*HyperText Transfer Protocol Secured* (HTTPS) sur le protocole UDP. [Carlucci2015] a étudié les performances de ce système. Les résultats obtenus ont montré un meilleur *goodput* que TCP-CUBIC, malgré un taux de perte plus important. L'usage de *QUIC* est limité au navigateur *Google Chrome*, navigateur le plus répandu à La Réunion d'après [GSCounter]. Néanmoins, cette option est désactivée par défaut.

Les résultats de TCP sont en accord avec l'étude réalisée par [EQUINIX]. Avec un pourcentage de $92,49\%$, TCP est majoritaire. Les services proposés par TCP sont plus nombreux que ceux offerts par les autres protocoles de transport.

Le tableau 3.4 indique les services utilisés. Les services ont été rangés par pourcentage relevé.

TABLE 3.4 – Répartition des services utilisés par TCP.

Service	SSH	DNS	Mail	Non identifiés	Autres	HTTPS	HTTP
Percent	0,02	1,63	4,91	7,21	9,45	32,97	43,79

La présence du service *Secure SHell* (SSH) s'explique par les accès distants à différents outils propres au laboratoire. On peut citer les nœuds Planet-Lab [PlanetLab] à travers le monde, les sondes de la plate-forme *RunPL*, l'accès à la sonde de capture pour cette étude, l'accès à des serveurs distants, etc.

1,63% des paquets échangés dans nos traces sont des requêtes de DNS. Ces paquets permettent de convertir un nom de domaine en adresse IP. L'utilisation du DNS avec le protocole TCP a été restreint aux transferts de zone et aux réponses dont la taille est trop importante pour UDP [RFC5936, RFC6691, RFC7766].

Le service intitulé *Mail* regroupe les services identifiés par les ports numérotés 25, 110, 143, 465, 995 et 993. Ces ports correspondent respectivement à *Simple Mail Transfert Protocol* (SMTP), *Post Office Protocol* (POP), *Internet Message Access Protocol* (IMAP) et leurs versions sécurisées *SMTPs, POPs, IMAPs*. L'utilisation de ces ports est faite par les agents

de messagerie comme Windows Live Mail, Mozilla Thunderbird ou Mail. L'échange de courriel représente $4,91\%$ des paquets échangés. Ce pourcentage est faussé par l'utilisation des interfaces web des messageries. Par exemple, on peut utiliser la page web du service de message Gmail de Google pour envoyer directement des mails. Le service utilisé est alors un service web HTTP ou HTTPS.

Le service nommé *Non identifiés* est une connexion dont le numéro de port n'est pas rattaché à un service en particulier. Ce sont généralement des numéros supérieurs à $1\,000$.

La partie *Autres* regroupe plusieurs services. Ces services sont assez divers. On peut ainsi y retrouver l'utilisation du port numéroté 139 correspondant à *netbios-ssn*. Ce service de NetBIOS autorise l'échange de message en mode connecté. On peut également citer l'usage du service *Hyper Text Caching Protocol (HTCP)* [RFC2756]. Ce service est utilisé pour partager et découvrir les contenus des caches (antémémoires) HTTP entre serveurs mandataires.

Nous avons décidé de garder la séparation entre les services HTTP et HTTPS. HTTPS est l'usage de HTTP avec un chiffrement. Ce chiffrement permet au visiteur de vérifier l'identité du site web grâce à un certificat. Ces services sont pré-dominants au sein du LIM.

L'usage de ces services peut être dégradé si l'on quitte La Réunion. Le tableau 3.5 indique la répartition du trafic selon le type d'adresse de destination.

TABLE 3.5 – Distribution du trafic.

Trafic	LAN	MAN	WAN
Pourcentage	21,65	0	78,35

La répartition s'est faite selon la géolocalisation des adresses IP. Le trafic LAN correspond à des échanges entre adresses privées. Le trafic identifié MAN correspond à des échanges entre adresses géolocalisées à La Réunion. On constate ainsi qu'aucune information cherchée par les utilisateurs n'est géolocalisée à La Réunion. Le trafic *Wide Area Network* (WAN) représente le trafic transitant par les câbles sous-marins. Ce découpage est rendu possible par l'inter-connexion des opérateurs au sein du GIX *Reunix*. Ce découpage ne serait pas le même si on étudiait la totalité du trafic de La Réunion. Ainsi, on constate qu'il n'y a aucun service dont la destination finale serait La Réunion.

Le tableau 3.7 indique la répartition des destinations de type *WAN*. Le tableau 3.6 rappelle la correspondance entre l'acronyme et le nom complet de chaque continent.

TABLE 3.6 – Correspondance entre acronymes et nom des continents.

Nom	Afrique	Asie	Europe	Amérique du Nord	Océanie	Amérique du Sud
Acronyme	AF	AS	EU	NA	OC	SA

TABLE 3.7 – Distribution géographique des destinations WAN.

Continent	AF	AS	EU	NA	OC	SA
Pourcentage	0,19	1,68	48,50	48,67	0,64	0,32

On constate que la répartition des continents est fortement inégale. L'Europe et l'Amérique du Nord concentrent plus de 97% des destinations réunies. L'étude réalisée par [Fanou2016] a montré une incohérence dans l'accès aux contenus. Les résultats ont ainsi prouvé que malgré la présence d'une infrastructure web développée sur le continent africain, la majorité du contenu était stocké sur les continents européen et nord-américain.

Dans le cadre de La Réunion, les règles de routage vues dans le chapitre précédent sont en cohérence avec la répartition des continents.

3.4.2 Performance de TCP

Un flot peut être caractérisé selon sa longueur (nombre de paquets ou octets échangés), sa durée (durée des échanges entre le premier et le dernier paquet capturé) et son ratio. Chaque caractérisation est associée à dénomination selon que le flux est court ou long. Il existe plusieurs définitions de limites de chaque caractérisation. Dans le tableau 3.8, nous indiquons le nom associé à chaque flux selon sa caractérisation ainsi que des exemples de limites.

Pour rappel, nous avons défini un flot comme « une série de paquets IP avec le même tuple suivant "adresse IP source, port source, adresse IP destination, port destination, protocole IP" ». Dans notre étude, nous considérerons un flot TCP sans tenir compte des mécanismes d'établissement et de fermeture de connexion. Ainsi, un flot pourra contenir uniquement des paquets de données et d'acquittement.

TABLE 3.8 – Tableau de dénomination des flux selon [Lan2006].

Taille des flux / Métrique	Courts	Longs	limites
Longueur	Souris	Éléphant	10 paquets [Sallantin2014], 1% de l'utilisation du lien [Estan2001], $100\ Ko$ [Lan2006]
Durée	Libellule	Tortue	2 secondes [Brownlee2002], 15 minutes [Lan2006].
Débit	Guépard	Escargot	100 Ko/s [Lan2006]

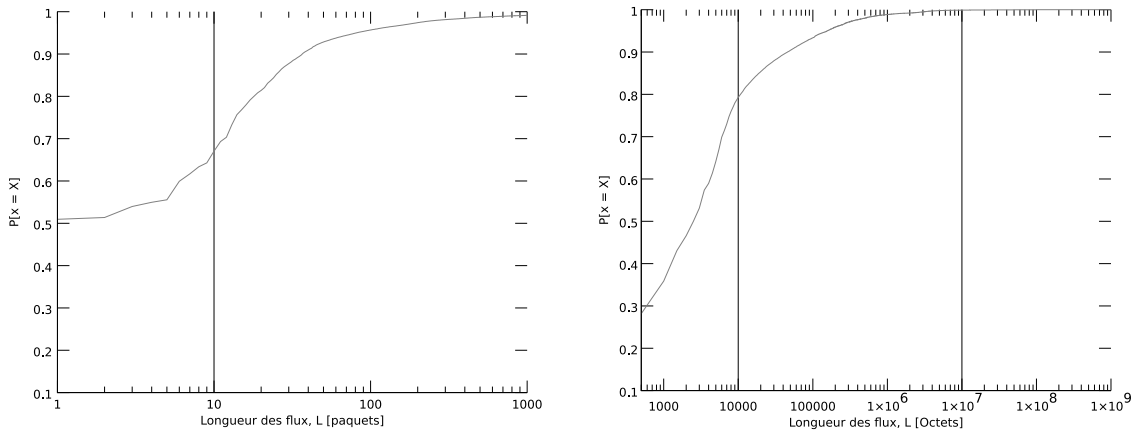
Les limites varient selon les études. Pour notre étude, les limites seront choisies en fonction des résultats. Nous comparerons nos limites avec celles indiquées dans le tableau ci-dessus. Dans notre présentation, la caractérisation des flux confond flux montant et flux descendant. D'après la *loi de Pareto*, environ 80% des effets sont le produit de 20% des causes. Dans l'Internet, 80% du trafic est réalisé par seulement 20% de flux éléphants [Paxson1995]. Nous regarderons si cette loi est respectée par les limites proposées.

Dans la figure 3.3, nous avons représenté les CDF de la longueur des flux, selon les paquets (3.3a) et le nombre d'octets (3.3b). Les traits verticaux représentent les limites indiquées dans le tableau 3.8. Sur la figure 3.3a, le trait vertical représente la limite des 10 paquets de [Sallantin2014]. Sur la figure 3.3b, le trait vertical d'une valeur de $10\ 000$ octets représente la limite indiquée par [Lan2006]. Le trait de droite représente les 1% de la capacité du lien d'accès, soit 10^7 octets (100 Ko).

Sur la figure 3.3a, plus de 50% des flux sont des flux mono-paquet. Les flux inférieurs à la limite proposée par [Sallantin2014] de $10\ paquets$ ont une probabilité de $0,67$. Notre trafic est donc constitué d'une majorité de flots courts sur les paquets. La séparation de 80% du trafic se fait à partir de 18 paquets.

L'axe des abscisses de la figure 3.3b démarre à 500 octets avec une probabilité de $0,28$. La valeur de départ de l'axe des abscisses représente le pas utilisé pour le calcul de la CDF. Le premier axe vertical, représenté à $10\ 000$ octets sépare $79,27\%$ des flux sont des flux courts. La limite proposée par [Estan2001] est représentée à 10^7 octets. Cette séparation indique que 99% des flux sont des flux courts. Aucune des deux limites proposées

ne permet une étude fine de la séparation des flux. La limite proposée par [Lan2006] approche la répartition de *Pareto*.



(a) Paquets.

(b) Octets.

FIGURE 3.3 – Longueur des flux.

La durée d'un flot TCP correspond au délai qui sépare la capture du premier et du dernier paquets du flot. La figure 3.4 représente la PDF pour la durée des flots, en secondes. Le pas utilisé pour effectuer le tracé est de 1 seconde. Ce pas s'explique par la valeur minimale que peut prendre le RTO comme défini dans le [RFC6298]. La ligne verticale représente la limite de [Brownlee2002], égale à 2 secondes.

La durée maximale enregistrée pour un flot est de $61\ 192$ secondes, soit plus de 10 heures d'échange. Au delà des 60 secondes, la probabilité d'avoir un flot supérieur à cette durée est égale à $0,081$. Nous considérons cette probabilité négligeable. Plus de 59% de nos flux sont inférieurs à la limite représentée par l'expiration du RTO (1 seconde). La limite des deux secondes indique que 64% des flux échangés sont des flux courts. Pour atteindre la répartition indiquée par la *loi de Pareto*, la séparation devrait atteindre les 10 secondes.

Les figures 3.5, représentent la répartition du débit utile moyen de chaque flux, selon le nombre de paquets par seconde (3.5a) et le nombre d'octets par seconde (3.5b). La ligne verticale sur la figure 3.5a représente la limite séparant les flux courts et les flux longs. D'une valeur de 10 paquets/seconde, elle est déduite de la limite de 10 paquets de la longueur des flux présentés précédemment. La limite de 100 Ko de [Lan2006] suit le même raisonnement. Ils sont partis de la limite de la longueur des flux pour choisir la limite de caractérisation des flux sur les débits.

La figure 3.5a démarre avec des débits peu élevés mais nombreux. Ainsi, les flux inférieurs à la limite des 10 paquets/seconde représentent plus de 90% des flux rencontrés. On peut donc en déduire que le trafic analysé a très forte majorité de flux à très bas débit.

La figure 3.5b est calculée avec le même pas que pour la longueur des flux, soit 500 octets. En analysant la figure, on remarque ainsi que les flux inférieurs ou égaux à 500 octets ont une probabilité d'exister proche de 0.9. La limite présentée par [Lan2006] autorise une caractérisation de 99% de nos flux en tant que flux courts.

Tout comme l'indiquaient [Paxson1995, Ciullo2009], le trafic est constitué en majorité de flots courts. Dans les trois caractérisations effectuées (longueur, durée, débit), le trafic étudié est constitué à plus 50%, voire 90% comme pour les débits, de flots courts.

TCP est un protocole s'appuyant sur les délais et le système d'acquittement pour adapter ses émissions. On a vu dans le chapitre 2 que l'île de La Réunion possède un

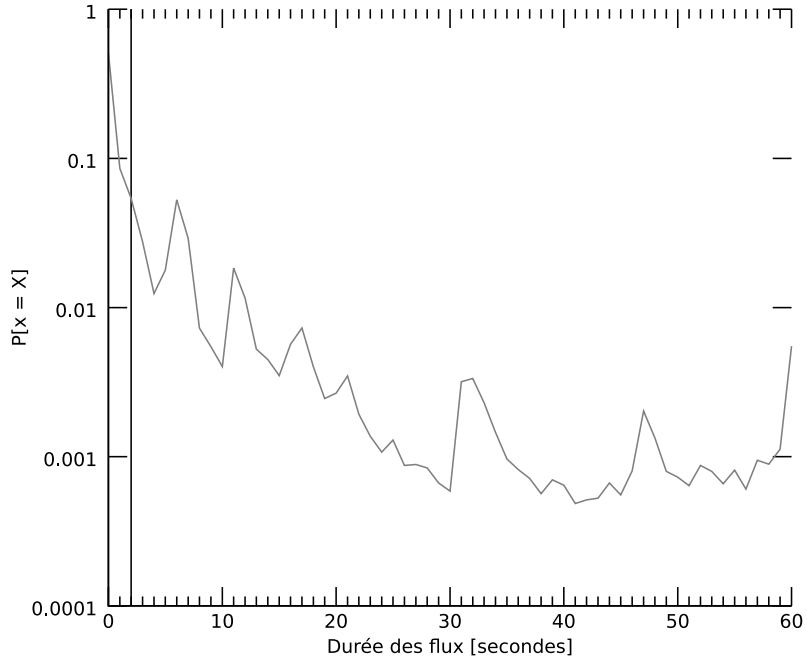
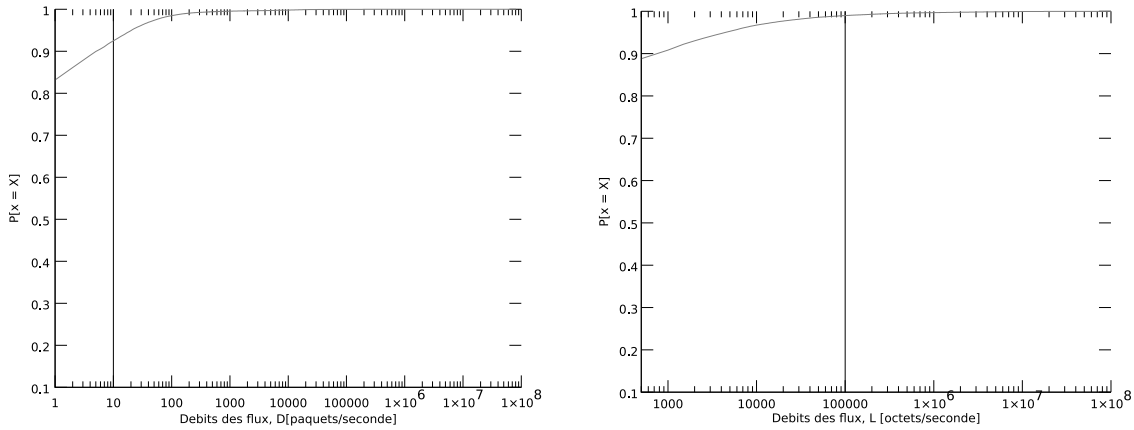


FIGURE 3.4 – Flux TCP - Densité de la durée de communication.



(a) Paquets/seconde.

(b) Octets/seconde.

FIGURE 3.5 – Débits des flux.

comportement particulier vis-à-vis de ce paramètre. Nous faisons l'hypothèse qu'une des conséquences de ce fonctionnement est que La Réunion possède une forte sensibilité aux événements de congestions. Nous avons deux outils permettant de confirmer ce postulat.

1. Le premier est l'identification des différentes options présentes dans l'en-tête TCP, plus particulièrement les options *ECN Echo* (ECE), *Explicit Congestion Notification* (ECN)/*Nonce Sum* (NS) et CWR. Le passage du bit de ces options à 1 indique une gestion des événements de congestion.
2. La seconde possibilité est de repérer les réductions de la fenêtre de TCP et les types de retransmissions qui ont lieu aux alentours de cette diminution.

Avec la première méthode, nous n'avons trouvé aucun paquet avec une option de gestion de la congestion (ECN) à 1. Cela indique que les événements de congestion ne peuvent être identifiés par la lecture des drapeaux. Les auteurs de [Trammell2015] ont montré que le nombre de serveurs répondant à la négociation de l'option ECE à travers le monde a augmenté ces dernières années. L'absence de paquets débutant la négociation,

donc provenant des utilisateurs du réseau du laboratoire, peut s'expliquer par 3 hypothèses.
La première est l'obsolescence des ordinateurs du Laboratoire d'Informatique et de Mathématiques. En effet, il faut un système d'exploitation récent pour que la version de TCP puisse marquer les paquets avec l'option. Cette hypothèse est vite abandonnée sachant que plusieurs participants à notre étude possèdent des ordinateurs achetés à partir de l'année 2014.
La seconde hypothèse est la suppression de l'option par un équipement réseau traversé à l'Université de La Réunion. Cette piste fut abandonnée après un test de mesures. Ce test consistait à envoyer des paquets avec l'option ECN à 1 et à regarder leurs options à leur arrivée au point de capture. Les résultats obtenus ont montré que l'option était inchangée.
La dernière possibilité est que le système d'exploitation ne marque pas l'ensemble des paquets avec le drapeau de négociation. Certains routeurs ou pare-feux incompatibles peuvent bloquer le trafic entre deux hôtes implémentant ECN [Bauer2011]. C'est pour cette raison qu'elle est désactivée implicitement sur la plupart des systèmes d'exploitation contemporains. Nous avons confirmé cette hypothèse à travers une demande d'utilisation de la commande *sysctl* et des options de TCP des systèmes d'exploitation Debian, Ubuntu et Mac OS X. Les résultats ont ainsi montré que les systèmes d'exploitation étudiés n'activaient pas cette option de TCP.

Dans tous les cas, l'absence des options ECE, ECN/NS et CWR est néfaste pour les performances de TCP. Les travaux réalisés par [Mellia2003-2] ont montré que les performances de TCP sont accrues lorsque les paquets sont marqués avec ces options. Sans elles, les événements de congestion sont plus difficiles à identifier.

La seconde façon d'identifier les événements de congestion est plus compliquée à mettre en place. Il s'agit d'identifier les réductions de fenêtre et d'étudier des pertes et/ou des retransmissions de paquets. Elle provoque des incertitudes. Sur un total de $42\,386\,540$ paquets, nous avons identifié $21\,022\,400$ paquets indiquant une diminution de fenêtre. Soit près d'un paquet sur deux.

Le tableau 3.9 indique les pourcentages des paquets retransmis et/ou perdus.

TABLE 3.9 – Répartition des paquets.

	fast retransmit	*spurious retransmit*	Paquets perdus	Non retransmis et non perdus
Pourcentage	$5,2 \times 10^{-3}$	$7,8 \times 10^{-3}$	14×10^{-3}	$99,97$

On constate que le pourcentage des paquets retransmis ou perdus sont ridicules, avec moins de 1% des paquets échangés. Ces pourcentages sont en deçà des valeurs que TCP peut produire dans certaines zones. Aux État-Unis, [Gettys2011] a étudié le taux de perte sur un lien montant à 2 Mbit/s lors d'un transfert de fichiers d'un poids de 20 Go. Le taux de perte est très élevé avec 33% de moyenne. En comparaison avec ces études réalisées, l'île de La Réunion possède des performances de TCP que l'on pourrait qualifier de normales.

3.4.3 Synthèse des résultats

L'analyse mise en place a pour objectif de tester en conditions réelles notre plateforme de mesure et la chaîne d'analyse.

L'étude du trafic du LIM a été découpée en deux parties. La première concerne la supervision du trafic et traite de la composition. La seconde partie se concentre sur les

performances du protocole de transport TCP, sur le trafic à destination de l'extérieur de l'île de La Réunion.
L'étude des données collectées a mis en avant la prédominance d'un trafic empruntant les câbles sous-marins, à destination de l'Europe et de l'Amérique du Nord. Ces deux destinations hébergent de nombreux serveurs de données scientifiques.
L'interrogation de ces serveurs se fait à partir du protocole TCP en utilisant les services HTTP ou HTTPS. Le protocole TCP est majoritaire dans les protocoles rencontrés, tout comme les services présentés.

Sur l'étude des performance du protocole TCP, nous avons effectué une caractérisation des flots, en terme de longueur (paquets échangés), de durée et de vitesse. La majorité de nos flots sont des flots courts contenant peu de données.

3.5 Conclusion

Dans ce chapitre, nous avons présenté la méthode mise en place pour la réalisation d'une étude de métrologie passive sur l'île de La Réunion.

La Réunion est une île dont la connectivité en terme de délais et de routes est particulière, telle que le chapitre 2 présente. L'augmentation progressive des débits d'accès a pour conséquence l'augmentation de la capacité de stockage des liens. On considère qu'un lien possède une forte capacité de stockage quand le produit délai bande passante (BDP) associé à ce lien dépasse la limite de $12,5\ Ko$. Pour La Réunion, la capacité de stockage minimale calculée est de $22,5\ ko$. Cette capacité de stockage entraîne des dégradations sur les performances du protocole TCP. Nous avons souhaité étudier l'impact de la capacité de stockage des liens sur les performances du protocole TCP à La Réunion. L'augmentation de la capacité des liens entraîne également un changement des usages. Nous souhaitons également étudier les différents services utilisés dans l'Internet à La Réunion.

Le cahier des charges fut présenté dans la section 3.1. Le cahier mis en place présente les métriques de l'étude. Ces métriques ont été sélectionnées afin de répondre aux objectifs présentés ci-dessus. Elles couvriront un aspect supervision du trafic pour l'étude des services et la répartition géographique. L'aspect des performances du protocole TCP sera analysé à travers les débits, les délais, les pertes, les retransmissions et la présence des événements de congestion.

Pour obtenir ces métriques, il est nécessaire de mettre en place une infrastructure de mesure et une chaîne d'analyse. La section 3.2 présente l'infrastructure mise en place. La variabilité du trafic dans le temps nous a encouragés à mettre en place une plate-forme de capture de trafic. Le choix de l'outil de capture n'est pas définitif. Il est dépendant du débit associé au lien de capture. Différents outils d'analyses de données passives existent. Dans le paragraphe 3.2.2, nous avons réalisé une comparaison des différents outils selon des critères de sélection. Ces critères sont au nombre de 3 : protection de la vie privée, traitement d'une volumétrie de données importante et le calcul des métriques sélectionnées. Aucun des outils présentés ne répondait à la totalité des critères. A la suite de ce constat, nous avons fait le choix de développer un outil répondant à ces 3 critères. L'avantage de cet outil est qu'il pourra évoluer en parallèle à l'évolution de l'étude.

Ces outils furent mis en place au sein du *Laboratoire d'Informatique et de Mathématiques* dans le cadre d'une phase de test. Les résultats obtenus ont été comparés avec les résultats obtenus par TCPTrace, afin de nous assurer de l'exactitude de nos résultats. Le protocole de mesure mis en place pour cette étude est décrit dans la section 3.3. Dans ce protocole, nous avons présenté les contraintes réglementaires imposées par l'Université. Nous nous

sommes ensuite assurés que le système mis en place pour la capture du trafic n'était soumis à aucune perturbation. Le système choisi pour écouter le lien fut celui de port-mirroring. Cette fonction des routeurs permet de copier l'ensemble des paquets entrant sur un lien vers un second lien. Cette recopie est soumise à la limitation de la capacité de mémoire des équipements. Elle peut entraîner des erreurs au niveau de la datation des paquets et dans l'ordre de ré-émission des paquets vers le lien miroir. Dans cette étude, la capture du trafic s'est faite à l'aide du logiciel TCPDump. Régulièrement, une phase de délestage de la mémoire de la sonde de capture vers un serveur de stockage du laboratoire a été mise en place.

Les résultats présentés dans la section 3.4 nous donnent une vision biaisée du comportement de l'Internet réunionnais. Ces résultats ne peuvent correspondre au comportement de TCP pour l'ensemble de l'Internet de La Réunion. Ces résultats nous donnent des indications sur le comportement de TCP dans le cadre d'une connexion à forte capacité de mémorisation.

Dans la partie supervision, on a vu la prédominance du protocole TCP, des services HTTP et HTTPS. Ces usages s'accompagnent d'une répartition géographique très inégale. L'Europe et l'Amérique du Nord sont les deux continents avec lesquels les interactions sont les plus nombreuses (plus de 48% du trafic pour chaque continent).

Au niveau des performances de TCP, nous avons pu voir que la majorité des flots étudiés sont des flots courts, que ça soit en longueurs, en durées et en débits. Aucun événement de congestion ne fut relevé. Cela indique que la capacité d'envoi des émetteurs n'a pas couvert le BDP du lien. Cela s'est ressenti au niveau de la répartition des paquets. Retransmissions et pertes n'ont représenté près de $0,03\%$ des paquets échangés.

Les contributions de ce chapitre ont fait l'objet d'une publication scientifique lors de la conférence *Next Generation Computing Applications (NextComp)* en 2017 [Noordally2017].

Conclusion & Perspectives

1 Synthèse des travaux

Les travaux de cette thèse sont placés dans le cadre régional de l'accès de l'île de La Réunion à l'Internet. Ils visent à identifier les caractéristiques qui ont une influence sur les performances de l'Internet à La Réunion. La Réunion est un département d'outre-mer situé dans l'Océan Indien. L'île est connectée à Internet à travers deux câbles sous-marins : le SAFE et le LION. Le SAFE relie l'Afrique à l'Asie. Le LION interconnecte Madagascar, l'île Maurice et La Réunion. L'arrivée de ces câbles sur l'île a permis le développement du haut débit et du très haut débit sur l'île, avec l'arrivée des technologies ADSL, VDSL et FTTH. Des extensions à ces câbles permettent de remonter jusqu'en Europe. La Réunion possède REUNIX, un point d'inter-connexion (IXP) pour les opérateurs locaux. Ce type d'accès à Internet est spécifique aux îles de la zone océan indien. Dans un premier temps, nous avons étudié la connectivité de l'île sous l'angle des délais et des routes. Dans un second temps, l'étude a porté sur les flots TCP.

TCP est le protocole de transport majoritaire dans l'Internet qui rend un service de transport fiable et efficace de données. L'efficacité s'apprécie en terme de débit écoulé pour le service rendu et d'utilisation des capacités de transmission du réseau. L'objectif d'efficacité est du ressort du contrôle de flux et du contrôle de congestion. Ces fonctions agissent selon une période correspondant au RTT de la connexion. On voit alors que la performance de TCP est dépendante du délai que va expérimenter la connexion TCP.

Nous avons dans un premier temps étudié l'évolution du délai et de la longueur des routes entre 2012 et 2016. Cette étude a mis en évidence une stabilité des délais malgré une réduction de la longueur des routes. Cette étude a été réalisée depuis un seul point de mesure. Afin d'étudier en détail la connectivité de La Réunion, nous avons déployé une plate-forme de métrologie active spécifique à l'étude. Durant plusieurs mois, nous avons mesuré les délais et les routes depuis et vers La Réunion à l'aide de l'outil Paris-traceroute. L'analyse des résultats a été réalisée à partir de deux outils développés pour le besoin de l'étude : rgeoloc et rtraceroute. rgeoloc sert à la géolocalisation des adresses IP et à l'extraction des délais et de la longueur des routes depuis un fichier de sortie de traceroute. rtraceroute est un outil d'analyse graphique des routes. Il va utiliser les données obtenues depuis rgeoloc pour placer sur une carte les différents pays traversés par les données collectées.

Les résultats ont été étudiés selon quatre critères : les délais, la longueur des routes, la distance géographique entre la source et la destination et l'identification des portes de l'Internet réunionnais. Nous avons ainsi pu mettre en évidence l'indépendance de la longueur de la route en fonction de la distance géographique. Nous avons calculé le délai nécessaire à chaque noeud traversé. Cette valeur est fortement dépendante du sens de circulation de l'information. La relation entre le délai et la distance géographique a mis en évidence une incohérence. Le délai nécessaire pour joindre une destination ou être joint depuis l'extérieur de l'île est inversement proportionnel à la distance géographique. Cela signifie donc que plus la distance est importante, moins le délai est élevé. Nous

avons étudié ce comportement vis à vis des portes de l'Internet réunionnais et mis en avant le fait que plus de 97% du trafic réunionnais passe par la France hexagonale, sans tenir compte si c'est du trafic montant ou descendant. Ce comportement a également été étudié pour les îles de la ZOI, dans le sens montant. Le délai minimal mesuré accompagné du routage analysé peut avoir des conséquences sur les performances d'un protocole de transport dépendant au délai, comme l'est TCP.

L'augmentation de la bande passante sur le réseau de distribution de l'île et sur les liens reliant l'Ile à l'Internet n'ont pas permis la réduction des délais. Cela a pour conséquence l'augmentation de la capacité de stockage des canaux de communication. La capacité de stockage est calculée à partir de la bande passante et du RTT. On parle de Produit Délai-Bande passante (BDP). Si le BDP dépasse la valeur seuil de $12,5$ Ko, alors le canal est considéré comme un réseau à forte capacité de stockage (LFN). Si on considère que le débit d'accès théorique fourni par les FAI est le goulot d'étranglement, alors un canal de communication sur l'Internet depuis La Réunion possède un BDP minimal égal à $22,5$ Ko. Lorsque le transport des données s'effectue avec TCP en passant par un LFN, ceci à des implications sur les performances du service rendu par TCP. L'objectif a été de concevoir un système métrologique pour pouvoir étudier le service et analyser le fonctionnement du protocole. Nous avons mis en place et expérimenté une infrastructure de métrologie passive interne au laboratoire. En parallèle, nous avons conçu un outil d'analyse de traces d'écoute spécifiques à notre étude. L'ensemble de la chaîne de mesure et d'analyse a été testé durant un mois au sein du LIM. Les résultats obtenus ont été validés par comparaison à ceux fournis par d'autres outils.

2 Perspectives

île de La Réunion

La mise en place d'une étude de métrologie passive en collaboration avec les différents FAI permettrait d'étudier le réel impact de l'éloignement de La Réunion sur les performances du protocole de transport TCP. De plus, l'analyse de supervision permettrait d'identifier des leviers pour limiter le rapatriement de trafic commun par les câbles sous-marins.

Zone Océan Indien

Cette thèse a mis en évidence une connectivité particulière en terme de délais et de routes depuis l'île de La Réunion et les îles de la Zone Océan Indien, dans le sens "Depuis". L'asymétrie des routes est fréquente dans l'Internet. C'est pourquoi, une étude des délais et des routes depuis le monde à destination des sondes de la plate-forme RunPL, basées sur les îles de la ZOI peut être pertinente.

Par la suite, une étude de métrologie passive, similaire à celle que l'on veut mettre en place sur le territoire réunionnais, pourrait être réalisée. L'objectif est de mettre en évidence un comportement spécifique en terme d'usage et de performance protocolaire pour l'ensemble des usagers de la zone. Cette étude aura également comme but le calcul de la volumétrie échangée et des services utilisés entre les différents territoires. Si les résultats montrent une prédominance des trafics de consultation (accès à un serveur), la technique d'*offloading* pourrait être envisagée. Cette méthode, inspirée des travaux de [Baron2016], impliquerait l'usage des transports aériens pour charger des caches locaux. D'autres solutions seront également étudiées, comme l'implémentation de serveurs de partage de contenus localisés sur l'île.

Territoires ultra-marins français

La Réunion et Mayotte sont deux territoires français localisés dans la ZOI. Mais d'autres régions ultra-marines peuvent être soumises à des comportements similaires. Pour vérifier cette hypothèse, des études de métrologie active et passive pourraient venir valider ou non cette hypothèse. Pour répondre à cela, nous privilégierons l'envoi de sondes de la plate-forme RunPL.

Zone Isolée

La dernière perspective que l'on souhaite mettre en avant est le concept de Zone Isolée. Si plusieurs résultats des perspectives précédentes sont en adéquation avec les résultats obtenus et présentés dans cette thèse, nous aimerions définir ce concept. Une première définition serait axée sur les trois points suivants :

— Un routage limité : Un maillage important est un standard dans les zones bien connectées. Les routes et les possibilités de trouver le plus court chemin sont nombreuses. Une faible valeur signifie de faibles alternatives, ce qui sous-entend que la route prise n'est pas forcément la plus courte mais celle par défaut.

— *Peering* régional et trafic interne : L'ensemble du trafic d'une zone va vers un *GIX* d'autres pays pour des raisons de coût. L'absence d'accords de peering entre les FAI d'un même pays ou ceux d'une même zone géographique ne permet pas la diversité des routes et augmente ainsi le délai. [Obar2012]

— Forts délais : Le délai est un paramètre important de l'accès Internet. Les fortes latences peuvent impacter les autres paramètres des connexions TCP [RITE2014-1].

Table des figures

Liste des tableaux

Bibliographie

[ANRTIC2016] ANRTIC. Autorité Nationale de Régulation des TIC, 2016.

[ARCEP2004] Autorité de Régulation des Télécommunications. Décision n04-375 de l'autorité de régulations des télécommunications en date du 4 mai 2004 se prononçant sur un différent opposant mobius à france télécom, 2004.

[ARTEC2016] Autorité de Régulation des TEchnologies de Communication. Artec, 2016.

[AXIS] African internet exchange system project, 2016.

[Aben2015] Emile Aben. Infrastructure geolocation - plan of action, 2015.

[Afanasyev2010] A. Afanasyev, N. Tilley, P. Reiher, and L. Kleinrock. Host-to-host congestion control for tcp. *IEEE Communications Surveys & Tutorials*, 12(3), Third quarter 2010.

[Africa1] Telegeography Submarine Cable. Submarine cable map, 2018.

[AfterFibre] Steve Song. African undersea and terrestrial fibre optic cables, Last visit : 09/26/2017.

[Akamai2015] Akamai. Akamai's [state of the internet], 2015.

[Akamai2017] Akamai. Akamai's [state of the internet], 2017.

[Allman2007] Mark Alllman and Vern Paxson. Issues and etiquette concerning use of shared measurement data. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 135–140. ACM, 2007.

[Anelli2012] Pascal Anelli. *Des aléas de la communication : de la transmission au transport*. Habilitation à diriger des recherches en informatique, Université de La Réunion, 2012.

[Archipelago] Kimberly Claffy, Young Hyun, Ken Keys, Marina Fomenkov, and Dmitri Krioukov. Internet mapping : from art to science. In *Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology*, pages 205–211. IEEE, 2009.

[Arduino] Arduino AG. Arduino home.

[Arnal2014] F Arnal, E Dubois, E Chaput, and A Beylot. Internet-draft r. sallantin intended status : Proposed standard e. bouttier expires : April 30, 2015 cnes/-tas/tesa c. baudoin. 2014.

[Augustin2006] Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viger, Timur Friedman, Matthieu Latapy, Clémence Magnien, and Renata Teixeira. Avoiding traceroute anomalies with paris traceroute. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pages 153–158. ACM, 2006.

[Augustin2007] Brice Augustin, Timur Friedman, and Renata Teixeira. Multipath tracing with paris traceroute. In *End-to-End Monitoring Techniques and Services, 2007. E2EMON'07. Workshop on*, pages 1–8. IEEE, 2007.

[Bajpai2015-1] Vaibhav Bajpai and Jürgen Schönwälder. A survey on internet performance measurement platforms and related standardization efforts. *IEEE Communications Surveys & Tutorials*, 17(3) :1313–1341, 2015.

[Baron2016] Benjamin Baron. *Transport intermodal de données massives pour le délestage des réseaux d'infrastructure*. PhD thesis, Paris 6, 2016.

[Bauer2011] Steven Bauer, Robert Beverly, and Arthur Berger. Measuring the state of ecn readiness in servers, clients, and routers. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pages 171–180. ACM, 2011.

[Beaglebone] BeagleBoard.org Foundation. Beagleboard.org - community supported open hardware computers for making.

[Bischof2015] Zachary S Bischof, John P Rula, and Fabián E Bustamante. In and out of Cuba : Characterizing Cuba's connectivity. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, pages 487–493. ACM, 2015.

[Brakmo1994] Lawrence S Brakmo, Sean W O'Malley, and Larry L Peterson. *TCP Vegas : New techniques for congestion detection and avoidance*, volume 24. ACM, 1994.

[Brownlee2002] Nevil Brownlee and KC Claffy. Understanding internet traffic streams : dragonflies and tortoises. *Communications Magazine, IEEE*, 40(10) :110–117, 2002.

[CAIDA-Tools] Center for Applied Internet Data Analysis. Caida tools - overview.

[Cablesmap] Telegeography. Submarine cable map.

[Carlucci2015] Gaetano Carlucci, Luca De Cicco, and Saverio Mascolo. Http over udp : An experimental investigation of quic. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, SAC '15, pages 609–614, New York, NY, USA, 2015. ACM.

[Chappell2010] Laura Chappell and G Combs. *Wireshark network analysis : the official Wireshark certified network analyst study guide*. Protocol Analysis Institute, Chappell University, 2010.

[Chavula2017] Josiah Chavula, Amreesh Phokeer, Agustin Formoso, and Nick Feamster. Insight into africa's country-level latencies. In *AFRICON, 2017 IEEE*, pages 938–944. IEEE, 2017.

[Chiu1989] Dah-Ming Chiu and Raj Jain. Analysis of the increase and decrease algorithms for congestion avoidance in computer networks. *Computer Networks and ISDN systems*, 17(1) :1–14, 1989.

[Chun2003] Brent Chun, David Culler, Timothy Roscoe, Andy Bavier, Larry Peterson, Mike Wawrzoniak, and Mic Bowman. PlanetLab : An overlay testbed for broad-coverage services. *SIGCOMM Comput. Commun. Rev.*, 33(3) :3–12, July 2003.

[Ciullo2009] D. Ciullo, M. Mellia, and M. Meo. Two schemes to reduce latency in short lived TCP flows. *IEEE Communications Letters*, 13(10), October 2009.

[Claise2004] Benoit Claise. Cisco systems netflow services export. 2004.

[Comores2002] Mwezinet. L'arrivée d'internet aux comores, Last Seen : 09/06/2017.

[Coonjah2015] Irfaan Coonjah, Pierre Clarel Catherine, and KMS Soyjaudah. Performance evaluation and analysis of layer 3 tunneling between openssh and openvpn in a wide area network environment. In *Computing, Communication and Security (ICCCS), 2015 International Conference on*, pages 1–4. IEEE, 2015.

[Crovella2006] Mark Crovella and Balachander Krishnamurthy. *Internet Measurement : Infrastructure, Traffic and Applications*. John Wiley & Sons, Inc., New York, NY, USA, 2006.

[Crowcroft1998] Jon Crowcroft and Philippe Oechslin. Differentiated end-to-end internet services using a weighted proportional fair sharing tcp. *ACM SIGCOMM Computer Communication Review*, 28(3) :53–69, 1998.

[DICT2017] Government of Seychelles. Office of the president : Department of information communication technology, 2016.

[Donnet2012] Benoit Donnet, Matthew Luckie, Pascal Mérindol, and Jean-Jacques Pansiot. Revealing mpls tunnels obscured from traceroute. *ACM SIGCOMM Computer Communication Review*, 42(2) :87–93, 2012.

[Downey1999] Allen B Downey. Using pathchar to estimate internet link characteristics. In *ACM SIGCOMM Computer Communication Review*, volume 29, pages 241–250. ACM, 1999.

[EQUINIX] CAIDA. Chicago passive network monitor, Last visit : 12/01/2018.

[Estan2001] Cristian Estan and George Varghese. *New directions in traffic measurement and accounting*, volume 32. ACM, 2002.

[Fanou2015] Rodérick Fanou, Pierre Francois, and Emile Aben. On the diversity of interdomain routing in africa. In *Passive and Active Measurement*, pages 41–54. Springer, 2015.

[Fanou2016] Rodérick Fanou, Gareth Tyson, Pierre Francois, and Arjuna Sathiaseelan. Pushing the frontier : Exploring the african web ecosystem. In *Proceedings of the 25th International Conference on World Wide Web*, pages 435–445. International World Wide Web Conferences Steering Committee, 2016.

[Feige1992] Uriel Feige and Prabhakar Raghavan. Exact analysis of hot-potato routing. In *Foundations of Computer Science, 1992. Proceedings., 33rd Annual Symposium on*, pages 553–562. IEEE, 1992.

[Fraleigh2001] Chuck Fraleigh, Christophe Diot, Bryan Lyles, Sue Moon, Philippe Owezarski, Dina Papagiannaki, and Fouad Tobagi. Design and deployment of a passive monitoring infrastructure. In *Thyrrhenian Internatinal Workshop on Digital Communications*, pages 556–575. Springer, 2001.

[Fraleigh2003] Chuck Fraleigh, Sue Moon, Bryan Lyles, Chase Cotton, Mujahid Khan, Deb Moll, Rob Rockell, Ted Seely, and SC Diot. Packet-level traffic measurements from the sprint IP backbone. *Network, IEEE*, 17(6) :6–16, 2003.

[France2017] Mission Très Haut Débit. Plan france très haut débit, Last seen : 09/06/2017.

[GOTICOM2011] Groupement des Opérateurs en Technologies de l'Information et de la Communication. Goticom, Last Seen : 09/06/2017.

[GSCounter] StatCounter. Statcounter global stats - browser, os, search engine including mobile usage share, Last visit : 13/10/2017.

[Gettys2011] Jim Gettys and Kathleen Nichols. Bufferbloat : Dark buffers in the Internet. *Queue*, 9(11) :40, 2011.

[Gevros2001] Panos Gevros, Jon Crowcroft, Peter Kirstein, and Saleem Bhatti. Congestion control mechanisms and the best effort service model. *IEEE network*, 15(3) :16–26, 2001.

[Graham1997] Ian Graham, Murray Pearson, Jed Martens, and Stephen Donnelly. DAG - a cell capture board for {ATM} measurement systems. 1997.

[Gupta2014] Arpit Gupta, Matt Calder, Nick Feamster, Marshini Chetty, Enrico Calandro, and Ethan Katz-Bassett. Peering at the internet's frontier : A first look at isp interconnectivity in africa. In *Passive and Active Measurement*, pages 204–213. Springer, 2014.

[Ha2008] Sangtae Ha, Injong Rhee, and Lisong Xu. Cubic : A new tcp-friendly high-speed tcp variant. *SIGOPS Oper. Syst. Rev.*, 42(5) :64–74, July 2008.

[Herman2001] Paul Herman. The tcpstat tool. *Publicly available at : http ://www.frenchfries.net/paul/tcpstat*, 2001.

[Huston2000] Geoff Hutson. Tcp performance. *The Internet Protocol Journal*, 3, 2000.

[Huston2006] Geoff Huston. Gigabit tcp. *Internet Protocol Journal*, 9, 2006.

[IANA-port] IANA. Service Name and Transport Protocol Port Number Registry, Last visit : 06/20/2018.

[ICTA2017] Information and Communication Technologies Authority of Mauritius. Icta, Last Seen : 09/06/2017.

[IOX] Government Information Service. Iox submarine cable to drive the new digital economy of mauritius, 2018.

[IPMon] ATL Sprint. Ipmon project.

[Jacobson1988-1] V. Jacobson. Congestion avoidance and control. *ACM Computer Communications Review*, 18(4) :314–329, August 1988.

[Jacobson1989-1] Van Jacobson, Craig Leres, and S McCanne. The tcpdump manual page. *Lawrence Berkeley Laboratory, Berkeley, CA*, 1989.

[Jacobson1989-2] Van Jacobson, Craig Leres, and Steven McCanne. pcap-packet capture library. *UNIX man page*, 2001.

[Jacobson1997] Van Jacobson. Pathchar : A tool to infer characteristics of internet paths, 1997.

[Jain1990] Raj Jain. Congestion Control in Computer Networks : Issues and Trends. *IEEE Network Magazine*, May 1990.

[John2010] Wolfgang John, Sven Tafvelin, and Tomas Olovsson. Passive internet measurement : Overview and guidelines based on experiences. *Computer Communications*, 33(5) :533–550, 2010.

[Johnson2011] David L. Johnson, Veljko Pejovic, Elizabeth M. Belding, and Gertjan van Stam. Traffic characterization and internet usage in rural Africa. In *Proceedings of the 20th International Conference Companion on World Wide Web*, WWW '11, pages 493–502, New York, NY, USA, 2011. ACM.

[Johnson2016] David L Johnson and Gertjan van Stam. The shortcomings of globalised internet technology in southern africa, 2016.

[Katabi2002] Dina Katabi, Mark Handley, and Charlie Rohrs. Congestion control for high bandwidth-delay product networks. In *Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '02, pages 89–102, New York, NY, USA, 2002. ACM.

[Katz2010] Ethan Katz-Bassett, Harsha V Madhyastha, Vijay Kumar Adhikari, Colin Scott, Justine Sherry, Peter Van Wesep, Thomas E Anderson, and Arvind Krishnamurthy. Reverse traceroute. In *NSDI*, volume 10, pages 219–234, 2010.

[Krajsa2011] Ondrej Krajsa and Lucie Fojtova. RTT measurement and its dependence on the real geographical distance. In *Telecommunications and Signal Processing (TSP), 2011 34th International Conference on*, pages 231–234. IEEE, 2011.

[LIL1978] Loi numéro 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Last modification on 19 March 2014.

[Lan2006] Kun-chan Lan and John Heidemann. A measurement study of correlations of internet flow characteristics. *Computer Networks*, 50(1) :46–62, 2006.

[LanYanFock2015] Jean-Christophe Lan-Yan-Fock. Géolocalisation d'adresses IP, 2015.

[Larrieu2010] Nicolas Larrieu and Philippe Owezarski. Metrology of internet networks. *Digital Cognitive Technologies : Epistemology and the Knowledge Economy*, pages 101–117, 2010.

[Leguay2004] Jeremie Leguay, Matthieu Latapy, Timur Friedman, and Kavé Salamatian. Describing and simulating internet routes. *CoRR*, cs.NI/0411051, 2004.

[Leiner1997] Barry M Leiner, Vinton G Cerf, David D Clark, Robert E Kahn, Leonard Kleinrock, Daniel C Lynch, Jon Postel, Lawrence G Roberts, and Stephen S Wolff. The past and future history of the Internet. *Communications of the ACM*, 40(2) :102–108, 1997.

[Lemauricien] Le Mauricien. Projet câble metiss : le contrat décroché par alcatel submarine networks et electra tlc s.p.a, 2018.

[Liu2007] Dan Liu, Mark Allman, Shudong Jin, and Limin Wang. Congestion control without a startup phase. In *Workshop on Protocols for Fast Long-Distance Networks (PFLDnet)*, 2007.

[Lopez2006] Dino Martin López-Pacheco, Congduc Pham, and Laurent Lefevre. Nxg03-4 : Xcp-i : explicit control protocol for heterogeneous inter-networking of high-speed networks. In *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE*, pages 1–6. IEEE, 2006.

[METROPOLIS] Philippe Owezarski. Metropolis, métrologie pour l'internet et les services.

[MGIX2017] Madagascar Internet Exchange Point. Mgix : Mauritius internet exchange point, 2017.

[MIXP2017] Mauritius Internet Exchange Point. Mixp : Mauritius internet exchange point, 2017.

[Maksimovic2014] Mirjana Maksimović, Vladimir Vujović, Nikola Davidović, Vladimir Milošević, and Branko Perišić. Raspberry pi as internet of things hardware : performances and constraints. *design issues*, 3 :8, 2014.

[Mediametrie2018-1] Benoit David. L'année Internet 2017 : Internet méta-média, Last visit : 20/04/2018.

[Mediametrie2018-2] Benoit David. L'observatoire des Usages Digitaux Antilles/-Guyane et Réunion - Panorama 2017, Last visit : 20/04/2018.

[Medina2005] Alberto Medina, Mark Allman, and Sally Floyd. Measuring the evolution of transport protocols in the internet. *ACM SIGCOMM Computer Communication Review*, 35(2) :37–52, 2005.

[Mellia2003-1] Marco Mellia, Andrea Carpani, and Renato Lo Cigno. Tstat : Tcp statistic and analysis tool. In *International Workshop on Quality of Service in Multiservice IP Networks*, pages 145–157. Springer, 2003.

[Mellia2003-2] M. Mellia, I. Stoica, and H. Zhang. TCP-aware packet marking in networks with diffserv support. *Elsevier Computer Networks*, 42(1) :81–100, 2003.

[Mellia2005] Marco Mellia, R Lo Cigno, and Fabio Neri. Measuring ip and tcp behavior on edge nodes with tstat. *Computer Networks*, 47(1) :1–21, 2005.

[Moore2001] David Moore, Ken Keys, Ryan Koga, Edouard Lagache, and K. C. Claffy. The coralreef software suite as a tool for system and network administrators. In *Proceedings of the 15th USENIX Conference on System Administration*, LISA '01, pages 133–144, Berkeley, CA, USA, 2001. USENIX Association.

[NCSUNRL] North Caroline State University - Networking Research Lab, Last seen : 27/02/2018.

[Nagle1984] John Nagle. Congestion control in ip/tcp internetworks. 1984.

[Nicolay2017-2] Xavier Nicolay, Réhan Noordally, Pascal Anelli, Nour Mohammad Murad, and Tahiry Razafindralambo. Where is my next hop ? the case of indian ocean islands. In *2017 Global Information Infrastructure and Networking Symposium (GIIS) (GIIS'17)*, St Denis, Reunion, October 2017.

[Nomikos2016] George Nomikos and Xenofontas Dimitropoulos. traixroute : Detecting ixps in traceroute paths. In *International Conference on Passive and Active Network Measurement*, pages 346–358. Springer, 2016.

[Noordally2016] Réhan Noordally, Xavier Nicolay, Pascal Anelli, Richard Lorion, and Pierre Ugo Tournoux. Analysis of internet latency : The reunion island case. In *Proceedings of the 12th Asian Internet Engineering Conference*, AINTEC '16, pages 49–56, New York, NY, USA, 2016. ACM.

[Noordally2017] Réhan Noordally, Yassine Gangat, Arnaud Ravoavahy, Pascal Anelli, and Xavier Nicolay. How long delays impact tcp performance for a connectivity from reunion island ? In *Next Generation Computing Applications (NextComp), 2017 1st International Conference on*, page 103–108. IEEE, 07 2017.

[ONU2013] ONU. The millennium development goals report 2013. Technical report, Organisation Nations United, 2013.

[Obar2012] Jonathan A Obar and Andrew Clement. Internet surveillance and boomerang routing : A call for Canadian network sovereignty. In *TEM 2013 : Proceedings of the Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association (Victoria)*, 2012.

[OpenVPN] OpenVPN. Openvpn - open source vpn, Last visit : 09/10/2017.

[OpenWrt] OpenWrt. Openwrt project : Welcome to the openwrt project, Last visit : 12/06/2018.

[Orebaugh2006] Angela Orebaugh, Gilbert Ramirez, and Jay Beale. *Wireshark & Ethereal network protocol analyzer toolkit*. Syngress, 2006.

[Ostermann2000] Shawn Ostermann. Tcptrace : A TCP connection analysis tool. *URL : http ://www. tcptrace. org*, 2000.

[Owezarski2003-1] Philippe Owezarski. Métrologie de la qualité de service. *Ecole d'été temps réel (ETR2003)-Systemes, Réseauxet Applications*, 2003.

[Owezarski2004] Philippe Owezarski and Nicolas Larrieu. Internet traffic characterization–an analysis of traffic oscillations. *High Speed Networks and Multimedia Communications*, pages 96–107, 2004.

[PCH] Packet Clearing House. Internet exchange directory, 2014.

[PSAMP] The Internet Engineering Task Force. Packet sampling (psamp), 2017.

[Paris-traceroute] Paris Traceroute Team. Paris traceroute, Last visit : 09/29/2017.

[Paxson1995] Vern Paxson and Sally Floyd. Wide area traffic : the failure of poisson modeling. *IEEE/ACM Transactions on Networking (ToN)*, 3(3) :226–244, 1995.

[Paxson1999] Vern Paxson. Bro : a system for detecting network intruders in real-time. *Computer networks*, 31(23) :2435–2463, 1999.

[Paxson2001] Vern Paxson. Some not-so-pretty admissions about dealing with internet measurements. In *Workshop on Network-Related Data Management (NRDM 2001)*, 2001.

[PeeringDB] Peering DB. Peeringdb facilitates the exchange of information related to peering.

[Periakaruppan1999] Ram Periakaruppan, Evi Nemeth, et al. GTrace : A graphical traceroute tool. In *LISA*, volume 99, pages 69–78, 1999.

[Peterson2007] Larry L Peterson and Bruce S Davie. *Computer networks : a systems approach*. Elsevier, 2007.

[Phidgets] Phidgets. Phidgets, products for usb sensing and control.

[PlanetLab] PlanetLab, an open platform for developing, deploying, and accessing planetary-scale services.

[PlanetLabEurope] PlanetLab. PlanetLab europe, an open platform for developing, deploying, and accessing planetary-scale services, last visit : 09/10/2017.

[Pretet2000] Thierry Prete and Olivier Mas. Avancement du projet SAFE. Technical report, 16 Janvier 2000.

[REUNIX2017] RENATER. RENATER : Connecteur de savoirs - reunix, Last visit : 09/10/2017.

[RFC1072] V. Jacobson and R. Braden. TCP extensions for long-delay paths. RFC 1072, October 1988.

[RFC1105] K. Lougheed and Y. Rekhter. Border Gateway Protocol (BGP). RFC 1105, June 1989.

[RFC1700] J. Reynolds and J. Postel. Assigned numbers. RFC 1700, October 1994.

[RFC1918] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address Allocation for Private Internets. RFC 1918, February 1996.

[RFC1983] G. Malkin (Ed.). Internet Users' Glossary. RFC 1983 (Informational), August 1996.

[RFC2001] W. Richard Stevens. TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms. RFC 2001, January 1997.

[RFC2330] Dr. Guy, T. Almes, Jamshid Mahdavi, Matt Mathis, and Dr. Vern Paxson. Framework for IP Performance Metrics. RFC 2330, May 1998.

[RFC2582] Tom Henderson and Sally Floyd. The NewReno Modification to TCP's Fast Recovery Algorithm. RFC 2582, April 1999.

[RFC2678] J. Mahdavi and V. Paxson. IPPM Metrics for Measuring Connectivity. RFC 2678 (Proposed Standard), September 1999.

[RFC2679] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Delay Metric for IPPM. RFC 2679 (Proposed Standard), September 1999. Obsoleted by RFC 7679.

[RFC2680] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Packet Loss Metric for IPPM. RFC 2680 (Proposed Standard), September 1999. Obsoleted by RFC 7680.

[RFC2681] G. Almes, S. Kalidindi, and M. Zekauskas. A Round-trip Delay Metric for IPPM. RFC 2681 (Proposed Standard), September 1999.

[RFC2756] P. Vixie and D. Wessels. Hyper Text Caching Protocol (HTCP/0.0). RFC 2756 (Experimental), January 2000.

[RFC2914] Sally Floyd. Congestion Control Principles. RFC 2914, September 2000.

[RFC3031] E. Rosen, Viswanathan. A., and R. Callon. Multiprotocol Label Switching Architecture. RFC 3031, January 2001.

[RFC3069] D. McPherson and B. Dykes. VLAN Aggregation for Efficient IP Address Allocation. RFC 3069 (Informational), February 2001.

[RFC3168] Sally Floyd, Dr. K. K. Ramakrishnan, and David L. Black. The Addition of Explicit Congestion Notification (ECN) to IP. RFC 3168, September 2001.

[RFC3232] J. Reynolds. Assigned Numbers : RFC 1700 is Replaced by an On-line Database. RFC 3232, January 2002.

[RFC3376] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan. Internet Group Management Protocol, Version 3. RFC 3376 (Proposed Standard), October 2002. Updated by RFC 4604.

[RFC3649] Sally Floyd. HighSpeed TCP for Large Congestion Windows. RFC 3649, December 2003.

[RFC3742] S. Floyd. Limited Slow-Start for TCP with Large Congestion Windows. RFC 3742 (Experimental), March 2004.

[RFC4250] Chris M. Lonvick and Sami Lehtinen. The Secure Shell (SSH) Protocol Assigned Numbers. RFC 4250, January 2006.

[RFC4782] Pasi Sarolahti, Amit Jain, Sally Floyd, and Mark Allman. Quick-Start for TCP and IP. RFC 4782, January 2007.

[RFC4950] R. Bonica, D. Gan, D. Tappan, and C. Pignataro. ICMP extensions for multiprotocol label switching. RFC 4950, August 2007.

[RFC5166] S. Floyd (Ed.). Metrics for the Evaluation of Congestion Control Mechanisms. RFC 5166 (Informational), March 2008.

[RFC5475] T. Zseby, M. Molina, N. Duffield, S. Niccolini, and F. Raspall. Sampling and Filtering Techniques for IP Packet Selection. RFC 5475 (Proposed Standard), March 2009.

[RFC5681] Ethan Blanton, Dr. Vern Paxson, and Mark Allman. TCP Congestion Control. RFC 5681, September 2009.

[RFC5735] Michelle S. Cotton and Leo Vegoda. Special Use IPv4 Addresses. RFC 5735, January 2010.

[RFC5936] E. Lewis and A. Hoenes (Ed.). DNS Zone Transfer Protocol (AXFR). RFC 5936 (Proposed Standard), June 2010.

[RFC6077] Ed. D. Papadimitriou, M. Welzl, M. Scharf, and Bob J. Briscoe. Open Research Issues in Internet Congestion Control. RFC 6077, February 2011.

[RFC6201] R. Asati, C. Pignataro, F. Calabria, and C. Olvera. Device Reset Characterization. RFC 6201 (Informational), March 2011.

[RFC6248] A. Morton. RFC 4148 and the IP Performance Metrics (IPPM) Registry of Metrics Are Obsolete. RFC 6248 (Informational), April 2011.

[RFC6298] Vern Paxson, Mark Allman, Jerry Chu, and Matt Sargent. Computing TCP's retransmission timer. RFC 6298, June 2011.

[RFC6528] F. Gont and S. Bellovin. Defending against Sequence Number Attacks. RFC 6528, February 2012.

[RFC6691] D. Borman. TCP Options and Maximum Segment Size (MSS). RFC 6691 (Informational), July 2012.

[RFC6761] Marc Krochmal and Stuart Cheshire. Special-Use Domain Names. RFC 6761, February 2013.

[RFC6928] J. Chu, N. Dukkipati, Y. Cheng, and M. Mathis. Increasing TCP's Initial Window. RFC 6928 (Experimental), April 2013.

[RFC7414] M. Duke, R. Braden, W. Eddy, and E. Blanton and. TCP Extensions for High Performance. RFC 7414, February 2015.

[RFC760] DoD standard Internet Protocol. RFC 760, January 1980.

[RFC776] J. Postel. Assigned numbers. RFC 776 (Historic), January 1981. Obsoleted by RFC 790.

[RFC7766] J. Dickinson, S. Dickinson, R. Bellis, A. Mankin, and D. Wessels. DNS Transport over TCP - Implementation Requirements. RFC 7766 (Proposed Standard), March 2016.

[RFC793] Information Sciences Institute. Transmission Control Protocol. RFC 793, September 1981.

[RFC8311] D. Black. Relaxing Restrictions on Explicit Congestion Notification (ECN) Experimentation. RFC 8311 (Proposed Standard), January 2018.

[RFC8312] I. Rhee, L. Xu, S. Ha, A. Zimmermann, and L. Eggert. CUBIC for Fast Long-Distance Networks. RFC 8312, February 2018.

[RITE2014-1] Bob Briscoe, Anna Brunstrom, Andreas Petlund, David Hayes, David Ros, Ing-Jyh. Tsang, Stein Gjessing, Gorry Fairhurst, Carsten Griwodz, and Michael Welz. Reducing internet latency : A survey of techniques and their merits. In *IEEE Communications Surveys & Tutorials*. IEEE, 2014 (To appear).

[RITE2014-2] RITE | Reducing Internet Transport Latency. Slow internet ? -more bandwith is not the answer, 2014.

[RaspberryPi] RASPBERRY PI FOUNDATION. Raspberry Pi, official website, Last visit : 09/102017.

[Ravoavahy2017] Arnaud Ravoavahy. Métrologie Réseaux, 2017.

[Ripe2010] RIPE NCC. RIPE atlas, 2010.

[Ros2005] David Ros. *Protocole de Transport TCP*. Ed. Techniques Ingénieur, 2005.

[SDTAN2013] Région Reunion, Sphère Public, and TACTIS. Schema directeur d'amenagement numerique du territoire de la reunion. Technical report, 2013.

[Sallantin2014] Renaud Sallantin. *Optimisation de bout-en-bout du démarrage des connexions TCP*. PhD thesis, 2014.

[SamKnows] SamKnows Ltd. Samknows.com, 2017.

[Sanchez2013] Mario A Sánchez, John S Otto, Zachary S Bischof, David R Choffnes, Fabián E Bustamante, Balachander Krishnamurthy, and Walter Willinger. Dasu : Pushing experiments to the internet's edge. In *NSDI*, pages 487–499, 2013.

[Scharf2008-1] Michael Scharf, Simon Hauger, and Jochen Kögel. Quick-start tcp : From theory to practice. In *Proc. 6th Intern. Workshop on Protocols for FAST Long-Distance Networks (PFLDnet), Manchester*, 2008.

[Speechecker] Speedchecker Ltd. Internet Performance Monitoring | Speedchecker Ltd., Last visit : 29/03/2018.

[Steenbergen2009] Richard A Steenbergen. A practical guide to (correctly) troubleshooting with traceroute. *North American Network Operators Group*, pages 1–49, 2009.

[Sundaresan2011] Srikanth Sundaresan, Walter De Donato, Nick Feamster, Renata Teixeira, Sam Crawford, and Antonio Pescapè. Broadband internet performance : a view from the gateway. In *ACM SIGCOMM computer communication review*, volume 41, pages 134–145. ACM, 2011.

[Tan2006] Kun Tan, Jingmin Song, Qian Zhang, and Murad Sridharan. A compound tcp approach for high-speed and long distance networks. In *Proceedings-IEEE INFOCOM*, 2006.

[Tirumala2005] Ajay Tirumala, Feng Qin, Jon Dugan, Jim Ferguson, and Kevin Gibbs. Iperf : The tcp/udp bandwidth measurement tool. *htt p ://dast. nlanr. net/-Projects*, 2005.

[Trammell2015] Brian Trammell, Mirja Kühlewind, Damiano Boppart, Iain Learmonth, Gorry Fairhurst, and Richard Scheffenegger. Enabling internet-wide deployment of explicit congestion notification. In *International Conference on Passive and Active Network Measurement*, pages 193–205. Springer, 2015.

[Udoo] UDOO. All you need mini pc android + linux + arduino | udoo.

[Vergoz2013] Michael Vergoz. Classement des opérateurs Internet réunionnais. Technical report, BinarySec, 2013.

[WAND] WAND. Wand network research group, Last visit : 09/25/2017.

[Wang2004] Ren Wang, Giovanni Pau, Kenshin Yamada, MY Sanadidi, and Mario Gerla. Tcp startup performance in large bandwidth networks. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 796–805. IEEE, 2004.

[Wang2018] Jessie Hui Wang and Changqing An. A study on geographic properties of internet routing. *Computer Networks*, 133 :183–194, 2018.

[Wenwei2006] Li Wenwei, Zhang Dafang, Yang Jinmin, and Xie Gaogang. On evaluating the differences of TCP and ICMP in network measurement. *Computer Communications*, 30(2) :428–439, 2007.

[WikiPing] Wikipedia. ping (logiciel), Last visit : 06/10/2017.

[Xu2002] Jun Xu, Jinliang Fan, Mostafa H Ammar, and Sue B Moon. Prefix-preserving IP address anonymization : Measurement-based security evaluation and a new cryptography-based scheme. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conferenceon*, pages 280–289. IEEE, 2002.

[Xu2004] Lisong Xu, Khaled Harfoush, and Injong Rhee. Binary increase congestion control (bic) for fast long-distance networks. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 4, pages 2514–2524. IEEE, 2004.

[Yang2016] Chantal Yang, Hussein Suleman, and Josiah Chavula. A topology visualisation tool for national research and education networks in Africa. In *IST-Africa Week Conference, 2016*, pages 1–11. IIMC, 2016.

[Zhang2007] Jian Zhang and Andrew Moore. Traffic trace artifacts due to monitoring via port mirroring. In *End-to-End Monitoring Techniques and Services, 2007. E2EMON'07. Workshop on*, pages 1–8. IEEE, 2007.

[Zheleva2015] Mariya Zheleva, Paul Schmitt, Morgan Vigil, and Elizabeth Belding. Internet bandwidth upgrade : implications on performance and usage in rural zambia. *Information Technologies & International Development*, 11(2) :pp–1, 2015.

[nPerf2017] nperf awards broadband reunion 2017.

[rtraceroute] Réhan Noordally, Arnaud Ravohavay, and Xavier Nicolay. rtraceroute, Last visit : 18/10/2017.

UNIVERSITÉ DE LA RÉUNION

Pôle Recherche
Ecoles doctorales

LETTRE D'ENGAGEMENT DE NON-PLAGIAT

Je, soussigné(e) NOORDALLY Réhan en ma qualité de doctorant(e) de l'Université de La Réunion, déclare être conscient(e) que le plagiat est un acte délictueux passible de sanctions disciplinaires. Aussi, dans le respect de la propriété intellectuelle et du droit d'auteur, je m'engage à systématiquement citer mes sources, quelle qu'en soit la forme (textes, images, audiovisuel, internet), dans le cadre de la rédaction de ma thèse et de toute autre production scientifique, sachant que l'établissement est susceptible de soumettre le texte de ma thèse à un logiciel anti-plagiat.

Fait à Saint-Denis le : 06/07/2018

Signature :

Extrait du Règlement intérieur de l'Université de La Réunion
(validé par le Conseil d'Administration en date du 11 décembre 2014)

Article 9. Protection de la propriété intellectuelle – Faux et usage de faux, contrefaçon, plagiat

L'utilisation des ressources informatiques de l'Université implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tes droits.
En conséquence, chaque utilisateur doit :
- utiliser les logiciels dans les conditions de licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser des logiciels, bases de données, pages Web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

La contrefaçon et le faux
Conformément aux dispositions du code de la propriété intellectuelle, toute représentation ou reproduction intégrale ou partielle d'une œuvre de l'esprit faite ans le consentement de son auteur est illicite et constitue un délit pénal.
L'article 444-1 du code pénal dispose : « Constitue un faux toute altération frauduleuse de la vérité, de nature à cause un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques ».
L'article L335_3 du code de la propriété intellectuelle précise que : « Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi. Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel (…) ».

Le plagiat est constitué par la copie, totale ou partielle d'un travail réalisé par autrui, lorsque la source empruntée n'est pas citée, quel que soit le moyen utilisé. Le plagiat constitue une violation du droit d'auteur (au sens des articles L 335-2 et L 335-3 du code de la propriété intellectuelle). Il peut être assimilé à un délit de contrefaçon. C'est aussi une faute disciplinaire, susceptible d'entraîner une sanction.
Les sources et les références utilisées dans le cadre des travaux (préparations, devoirs, mémoires, thèses, rapports de stage…) doivent être clairement citées. Des citations intégrales peuvent figurer dans les documents rendus, si elles sont assorties de leur référence (nom d'auteur, publication, date, éditeur…) et identifiées comme telles par des guillemets ou des italiques.

Les délits de contrefaçon, de plagiat et d'usage de faux peuvent donner lieu à une sanction disciplinaire indépendante de la mise en œuvre de poursuites pénales.