MASTER EN SCIENCES INFORMATIQUES

Comment un ISP peut mieux choisir ses fournisseurs d'accès grâce à BGP et à son trafic

Ponsen, Christophe

Award date:
2004

FUNDP
Institut d'Informatique

Rue Grandgagnage, 21
B-5000 Namur Belgique

Comment un ISP peut mieux choisir ses fournisseurs d'accès grâce à BGP et à son trafic

Christophe Ponsen

Promoteurs : J. Ramaekers et O. Bonaventure

Mémoire présenté pour l'obtention
du grade de
Maître en informatique

Année Académique 2003-2004

Je remercie mon promoteur Mr Bonaventure pour la qualité de son soutien et de ses conseils ainsi que Patrice Devemy qui aura été mon guide tout au long de ce stage et mémoire.

Je remercie également tous les professeurs de l'Institut d'Informatique qui nous ont appris tant de choses, ainsi que Pascale Renders sans qui ce mémoire ne serait pas ce qu'il est.

Je remercie aussi spécialement Messieurs Clarinval et Belhomme pour leurs conseils ainsi que toute ma famille et mes amis.

Je remercie enfin toutes les personnes qui m'ont aidé à réaliser ce travail et ce mémoire tant au sein de Skynet que de l'Institut.

RÉSUMÉ

Aujourd'hui, les ISP doivent choisir au mieux leurs connections. Pour ce faire, ils ne disposent que des informations marketings des fournisseurs, de la renommée de ceux-ci ainsi que des spécificités techniques des infrastructures que veulent bien publier ces mêmes fournisseurs. Les ISP ne disposent d'aucun outil pour évaluer un fournisseur sur la base de caractéristiques qualitatives.

Ce mémoire propose une méthode de comparaison qualitative entre plusieurs fournisseurs permettant de classer ceux-ci afin de choisir le meilleur. Cette méthode se base sur les tables BGP de l'ISP et des fournisseurs ainsi que sur le trafic existant de l'ISP. Elle propose de reconstruire une table BGP similaire à celle qu'obtiendrait l'ISP en y intégrant la table d'un ou plusieurs fournisseurs et de simuler l'envoi de trafic au travers de cette table, le trafic utilisé étant un échantillon du trafic de l'ISP. On peut alors consulter les résultats soit de manière graphique et en tirer soi-même les conclusions, soit de manière mathématique par un classement des fournisseurs. Pour permettre la capture du trafic, un outil a été développé et est présenté dans ces pages.

La méthode a été implémentée chez Skynet et est encore utilisée aujourd'hui.

ABSTRACT

Today, the ISP must choose their connections in the best possible way. For that purpose, they only have marketing information, reputation of the providers as well as technical specificities of the infrastructures that these providers want to publish. The ISP do not have any tool to evaluate a provider on the basis of qualitative characteristics.

This thesis proposes a method of qualitative comparison between several providers making it possible to classify them in order to choose the best one. This method is based on BGP tables of the ISP and of the providers as well as on the existing traffic of the ISP. It proposes to rebuild a BGP table similar to that which the ISP would obtain by integrating the table of one or more providers into their own one and to simulate the sending of traffic through this table, the traffic used being a sample of the traffic of the ISP. One can then consult the results either in a graphic way and draw one's own conclusions or in a mathematical way by a classification of the providers. To allow the capture of the traffic, a tool has been developed and is presented in these pages.

The method was implemented at Skynet and is still used today.

TABLE DES MATIÈRES

TABLE DES FIGURES

INTRODUCTION

Ce mémoire est la conclusion d'un stage réalisé chez Skynet sa. à Bruxelles de mi-septembre 2002 à mi-janvier 2003, dans les locaux de Skynet, au sein de la team IT Network. Il a été supervisé par Monsieur O. Bonaventure des Facultés Universitaires Notre-Dame de la Paix à Namur et Monsieur J-F Stenuit de Skynet.

Le but du stage était de réaliser complètement un outil d'aide à la décision pour sélectionner la meilleure combinaison de fournisseurs de trafic en fonction du trafic actuel de Skynet. L'intérêt de l'outil est de pouvoir négocier des contrats de peering de manière plus efficace et avec des données autres que les simples données marketing.

A la suite de l'avènement des connections haut débit auprès du grand public, les ISP sont obligés d'adapter à la fois leur réseau interne et leurs connexions externes, pour faire face aux nouveaux besoins de bande passante. L'adaptation du réseau interne est un problème de structure et de capacité du réseau et, donc, une simple difficulté matérielle. En revanche, l'adaptation des connexions externes représente un problème beaucoup plus complexe, car elle nécessite souvent une augmentation de la bande passante, ce qui oblige l'ISP à revoir ses contrats de connectivité. La modification des contrats peut aussi être voulue pour d'autres raisons, comme l'amélioration de la qualité du réseau ou le besoin de redondance en cas de panne d'une des connections.

L'ISP peut augmenter sa bande passante chez un de ses fournisseurs ou d'ouvrir de nouvelles connections auprès de nouveaux fournisseurs. Dans les deux cas, une reconfiguration interne est nécessaire pour redistribuer correctement le trafic en fonction des capacités des nouvelles lignes. Le choix d'un nouveau fournisseur entraîne en outre des modifications dans les tables de routage des deux parties. Ce choix requiert donc une attention toute particulière.

Plusieurs documents [O. 03, And02, And01, Ing01, Bra02] circulent déjà sur Internet pour aider à ce genre de décision, mais ils sont tous rédigés par des Américains ou pour une infrastructure telle que l'infrastructure anglo-américaine. Or, l'infrastructure Internet européenne est loin d'être aussi développée. Même si les réseaux nationaux sont de taille raisonnable, les interconnexions ne sont pas encore suffisantes (en terme de capacité) en Europe. Actuellement, les seuls liens suffisants passent par les opérateurs américains et, en règle générale, obligent le trafic à traverser l'Atlantique avant de revenir. L'apparition de grands opérateurs européens comme Tiscali commence à permettre de garder le trafic européen en Europe, mais ces sociétés sont encore jeunes et en pleine évolution. Leur réseau, en construction, ne peut encore fournir la capacité et la fiabilité des réseaux américains bien établis.

Un ISP doit obligatoirement tenir compte de tous ces éléments lors de l'établissement de

ses peering, s'il ne veut pas connaître de grave problèmes de trafic (lenteurs, pertes, surcapacité, non-fiabilité).

Notre travail ne tient pas compte des données marketing ni des données de capacité des liens. En effet, ces données ne peuvent intervenir lors de mesures intrinsèques. C'est lors de la prise de décision que tous les paramètres sont pris en compte. Les ressources disponibles pour développer notre outil d'aide à la décision sont :

- les tables BGP envoyées aux routeurs du demandeur par les candidats ;
- les données des infrastructures réseaux communiquées par les candidats ;
- le trafic actuel du demandeur ;
- tous les tests de mesure que l'on peut réaliser en plaçant une machine test sur les réseaux des candidats (si ceux-ci l'acceptent) ;
- les tables BGP et autres données que les candidats acceptent de fournir (pour les candidats avec lesquels une récupération automatique ne peut se faire).

Skynet désire utiliser les tables BGP de ses fournisseurs d'accès potentiels pour sélectionner la meilleure combinaison de fournisseurs, c'est-à-dire celle qui permettra de drainer son trafic de la manière la plus efficace, et surtout le trafic entrant, qui est le plus volumineux et le seul payant.

Le principe de départ proposé par Skynet consistait en une comparaison des tables BGP des fournisseurs, afin de déterminer les meilleures. A la suite des premières analyses effectuées, ce principe, qui semblait le plus naturel et intuitif, fut abandonné au profit d'une nouvelle méthode.

Cette nouvelle méthode reposant elle aussi sur le protocole BGP, il nous paraît nécessaire de donner de ce protocole une explication détaillée, qui fait l'objet du premier chapitre de ce mémoire. Il doit permettre de mieux appréhender le concept de qualité BGP que nous avons défini et qui est au coeur de la solution développée. Le deuxième chapitre propose l'analyse complète du problème rencontré.

Il a fallu dans un premier temps faire un état des lieux et rassembler des informations sur le trafic international. Le troisième chapitre détaille ce qui ne devait être, au départ, qu'un simple outil de collecte d'information et qui, suites aux exigences de Skynet, a du être développé comme un outil complet. Les chapitres 4 et 5 présentent d'abord la solution théorique imaginée et ensuite la tentative de mise en pratique, dans le contexte de Skynet, de cette solution.

Enfin, le dernier chapitre détaille les résultats de cette mise en pratique ainsi que des propositions pour améliorer à la fois la solution théorique et les divers outils développés.

Ce mémoire requiert une certaine connaissance de base des réseaux. Sont supposés connus du lecteur les termes et concepts suivants :

- adresse IP et ce qu'elle représente ;
- TCP et UDP ;
- paquet et datagramme ;
- base de données, SQL et sa syntaxe ;

– représentation binaire de données.

Les autres concepts ou protocoles utilisés dans ce travail ne sont pas redéfinis dans leur totalité. Seules les fonctionnalités exploitées dans un but spécifique font l'objet d'une explication.

1. BGP

BGP (Border Gateway Protocol) est le protocole standard sur Internet qui permet aux différents AS d'échanger des routes. Actuellement, il est utilisé dans sa version 4 définie par le RFC1771 [RL95] et autres RFC connexes.

BGP est un protocole basé sur 4 modules :
- etablissement d'une session BGP ;
- echange des routes ;
- algorithme de sélection de la meilleure route ;
- filtres ;

Ce chapitre propose une vue détaillée du protocole en présentant d'abord son histoire ensuite, le système d'adressage CIDR et le détail des quatre modules qui composent le protocole. Suivra une partie consacrée à la notion de routage Inter et Intra-domaine ainsi que les version de BGP y affairant. Il se terminera par une regard sur les évolutions du protocole depuis sa mise en production.

1.1 Un peu d'histoire

Bien que fondé bien plus tôt par le DOD et ouvert ensuite aux universités et aux institutions publiques américaines puis aux universités et aux centres de recherche mondiaux, c'est dans le début des années 90 que l'Internet a représenté un attrait pour le grand public, notamment grâce à l'apparition des navigateurs et du WWW (World Wilde Web) ainsi qu'au support de firmes commerciales qui voyaient dans l'Internet un nouveau marché prometteur.

Le succès grandissant de l'Internet a provoqué l'explosion du nombre d'ordinateurs connectés et a obligé les autorités régulatrices à revoir plusieurs fois les protocoles et les normes utilisées. Au départ, le système d'adressage de l'Internet était l'IP en version 4. Le système d'adressage, qualifié de CLASSFUL, reposait sur la division des adresses IP en 3 classes principales A, B et C, auxquelles était ajoutée une classe reprenant les adresses privées et réservées.

Les trois classes principales étaient réparties de la sorte :
- 126 classes A (16 777 214 machines chacun) ;
- 65000 classes B (65534 machines) ;
- Un peu plus de 2 millions de classes C (254 machines).

La grande différence de capacité entre les adresses de classe A et celles de classe B a

forcé les autorités à remanier le système. En effet, lors de l'attribution des réseaux, une entité quelconque qui désirait connecter plus de 65534 machines devait demander une classe A. Plutôt que de donner plusieurs classes B, et parce que cela rendait les choses simples dans un premier temps, les classes A furent accordées aux entités de taille sufisante qui en faisaient la demande, jusqu'à épuisement des classes. Comme il n'existe cependant pas ou très peu d'entités qui utilisent pleinement leur classe A, beaucoup d'adresses sont réservées, mais jamais utilisées. Ce problème de gaspillage des adresses IP a vite été pointé du doigt, mais le système CLASSFUL ne permettait pas de le résoudre.

1.2 CIDR Classless Inter-Domain Routing

Les protocoles EGP et IGP sont des protocoles de routage qui échangent des informations concernant les routes à utiliser pour joindre une destination. Toute modification du système d'adressage a donc un effet direct sur ces protocoles.

Face au problème de la réduction du nombre d'adresses IP (classful) disponible ainsi que de la taille grandissante des tables dans les routeurs, un nouveau système d'adressage a été imaginé et proposé : le CIDR [Int93, Y. 93, V. 93].

La particularité du système d'adressage CIDR est que l'on n'est plus tenu d'utiliser des classes d'adresses prédéfinies, mais que l'on peut utiliser l'adresse que l'on souhaite. Dans le système d'adressage CIDR, le masque de réseau est exprimé de manière libre entre un /8 et un /24 sur l'Internet. Des masques exprimés en dehors de cet intervalle seront filtrés et refusés, sauf pour des utilisations internes. Une adresse CIDR doit obligatoirement être accompagnée de son masque réseau, obligation qui n'était pas valable dans l'ancien système puisque chaque IP faisait partie d'une classe bien définie.

L'intérêt d'une telle liberté sur l'expression du masque est qu'elle permet une agrégation souple de routes contiguës.

1.2.1 Agrégation d'adresses contiguës dans les routeurs

80.200.100.0/24 et 80.200.101.0/24 peuvent être agrégés en 80.200.100.0/23 alors que 80.200.99.0/24 ne pourrait pas faire partie de cet agrégat. En effet, voici ce que donnent ces adresses en binaire :
80.200.100.0/24 : 01010000 11001000 01100100 00000000
80.200.101.0/24 : 01010000 11001000 01100101 00000000
80.200.099.0/24 : 01010000 11001000 01100011 00000000

La différence entre les deux premières lignes se situe uniquement au niveau du 24ème bit, alors que la troisième montre aussi une différence aussi au niveau du 23ème bit. Les deux premières lignes peuvent être agrégées avec un masque de /23. Cette agrégation représente alors l'ensemble des adresses IP disponibles dans ce /23. Ajouter la troisième nécessiterait une agrégation en /22, mais il manquerait une partie des IP /22. L'agrégation ne serait pas complète et est donc considérée comme non faisable sur l'Internet par l'ISP qui posséderait

ces trois groupes d'IP : elle serait qualifiée d'illégale.

L'avantage d'un tel système est très visible au niveau des routeurs. Si l'on respectait dès le départ le système CIDR en attribuant les adresses de façon à favoriser les agrégations, les tables des routeurs ne devraient plus contenir que les adresses les plus agrégées possible, ce qui limiterait grandement le nombre de routes à connaître. L'Internet serait alors une vaste hiérarchie d'adresses.

Les figures 1.1 et 1.2 présentent un exemple de ce que sont les tables BGP avec ou sans CIDR.

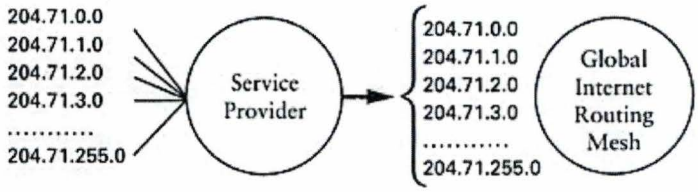

Fig. 1.1: Inter-domaine routing sans CIDR [Joh99]

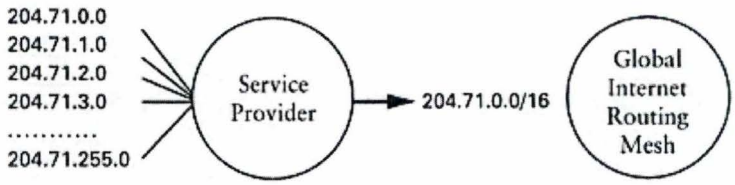

Fig. 1.2: Inter-domaine routing avec CIDR [Joh99]

1.3 Etablissement d'une session BGP

BGP est basé sur le principe d'une session établie entre deux routeurs (session TCP) qui s'échangent des informations durant cette session par le biais de messages. Si la session est rompue ou ne peut s'établir, les routeurs ne s'échangeront rien, même si le canal physique de communication est toujours établi. Un routeur BGP doit être configuré pour établir les sessions BGP avec les autres routeurs. En effet, alors que d'autres protocoles comme OSPF possèdent des algorithmes de découverte de leur réseau, un routeur BGP est incapable de découvrir ses voisins BGP. Cela s'explique par le fait que deux routeurs BGP ne sont pas forcément les deux terminaisons d'un lien physique, mais peuvent s'échanger des informations à travers un réseau IP. Pour que BGP fonctionne correctement sur un réseau, tous les routeurs BGP de ce réseau doivent avoir établi une session avec chacun des autres routeurs de ce réseau (full mesh I- BGP), comme le montre la figure 1.3.

Etablir un full mesh est très lourd pour un réseau lorsque le nombre de routeurs commence à être important. En effet, le nombre de sessions par routeur est égal à n-1 (n étant le nombre

de routeurs) et le nombre total de sessions sur le réseau à $\sum_{i=1}^{n-1} i$

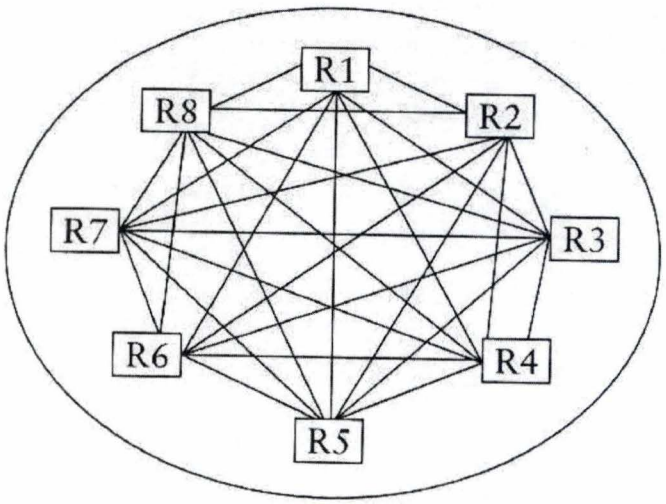

Fig. 1.3: Représentation d'un full mesh BGP [Joh99]

Les annonces BGP utilisent deux méthodes de fonctionnement : statique ou dynamique. En version statique, c'est l'administrateur du routeur ou du réseau qui spécifie, ligne par ligne, les routes BGP à utiliser. En mode dynamique, BGP utilise les données reçues par le routeur en provenance des protocoles de routages IGP (comme IS-IS, RIP ou OSPF). Les deux modes de fonctionnement peuvent être utilisés simultanément.

1.4 Echange des routes

1.4.1 Route BGP

BGP étant un protocole de routage, il échange des routes BGP.

6.1.0.0/16 80.66.129.77 329 78 770 55

Fig. 1.4: Exemple d'une route BGP

Une route BGP est constituée d'un préfixe (avec son masque), de l'adresse IP du routeur à joindre pour atteindre ce préfixe et d'un AS-PATH, qui indique l'ensemble des AS traversés pour rejoindre l'origine de la route, le dernier étant l'émetteur original de la route (55 dans la figure 1.4). Le protocole BGP peut être qualifié de path vector, puisque l'information la plus utile fournie par cette route BGP est justement cette suite d'AS qui montre la route à suivre pour joindre le préfixe et donne un renseignement sur la qualité de cette route. L'AS-PATH peut en effet contenir du prepending, qui permet de mesurer la qualité d'une route. Le prepending est le fait d'ajouter plusieurs fois son numéro d'AS dans l'AS-PATH, ce qui rend celui-ci artificiellement plus long. Un ISP effectue du prepending sur l'annonce qu'il fait

d'une route s'il estime que l'on doit éviter de l'utiliser (pour des raisons de bande passante restreinte ou de route réservée par exemple).

Ce moyen n'est pas totalement fiable, car on ne peut exclure des AS qui trichent dans les deux sens. Un AS peut en effet soit rendre les AS-PATH plus long pour éviter du trafic alors qu'aucune raison ne le demande, soit essayer d'attirer du trafic ou de ne pas être considéré comme un petit ISP en ne faisant pas de prepending, alors qu'il ne peut pas supporter la charge. Les ISP qui trichent sont souvent vite repérés et les mesures sont prises pour parer à leur comportement, mais ce n'est pas toujours le cas.

1.4.2 Echange de routes

Dès qu'une session est établie, les messages suivants circulent entre les routeurs :
- OPEN : premier message échangé. Il sert à identifier les protagonistes (IDENTIFIANT BGP) et à ouvrir la session BGP entre les deux routeurs, en négociant les éventuelles options ;
- UPDATE : message de communication principal, il sert à annoncer un (plusieurs) préfixe(s) ou à annuler un (plusieurs) préfixe(s) précédemment annoncé(s) ;
- NOTIFICATION : message d'erreur, il est employé quand une erreur survient lors d'une session BGP ;
- KEEPALIVE : message employé quand il n'y a pas de route à transmettre, pour signifier au routeur connecté que la session reste vivante.

Le champ IDENTIFIANT BGP est défini dans la norme comme devant être unique, mais la manière de le nommer est laissée libre. En pratique, on retrouvera souvent une des adresses IP publiques du routeur.

Les annonces de routes se font via le message UPDATE. C'est le seul message qui transporte de l'information, les autres messages ne servant qu'au contrôle de la session BGP. Un routeur BGP annonce l'ensemble de sa table BGP à tous les routeurs BGP avec lesquels il a une session active. Ce comportement par défaut est modifiable grâce aux filtres.

Une route BGP est davantage qu'un simple préfixe et un chemin pour le joindre. Chaque route contient des informations supplémentaires qui vont influencer la création de la table de routage BGP du routeur. Cette table est ensuite utilisée pour créer la table de forwarding et pour l'envoi des routes aux autres routeurs.

Ces informations sont définies dans les champs suivants :
- ORIGIN : définit la provenance d'un préfixe (EGP, IGP ou Incomplet, qui signifie en général une entrée statique) ;
- AS-PATH : séquence de listes des AS traversés pour joindre ce préfixe. Deux modes d'annonce existent : AS-SET et AS-SEQUENCE. L'AS-SEQUENCE est le plus employé et consiste en une liste ordonnée d'AS du type XXX XXX XXX. Dans une séquence codée selon un AS-SET, le préfixe est une agrégation de sous-réseaux ayant un AS-PATH différent après l'AS ayant pratiqué l'agrégation. Il se présente sous la forme

{XXX,XXX,XXX} ;
- NEXT-HOP : adresse IP du prochain routeur servant à joindre le préfixe ;
- MULTI-EXIT-DISCRIMINATOR (MED) : permet de donner un poids à une route qui pourrait être reçue sur plusieurs routeurs différents connectés au même ISP. Ce comportement est défini comme le comportement par défaut du champ et non comme le seul et unique possible ;
- LOCAL-PREF : permet de donner un poids uniquement local à l'AS pour influencer les décisions de sélection des routeurs de l'AS.

1.5 Algorithme de sélection de la meilleure route

BGP reçoit des routes qui peuvent provenir de plusieurs routeurs de plusieurs AS. Ces routes peuvent, en toute logique, se recouvrir, donner un chemin différent pour le même préfixe, être identiques au niveau du chemin et du préfixe mais pas des attributs,...

Quand il reçoit une demande de paquet à router, le routeur doit toujours pouvoir le router le plus efficacement possible. Si le routeur ne connaît pas de route, le paquet sera jeté. L'algorithme de sélection de la meilleure route est appelé "Best Path Algorithm" par Cisco© [Cisb] et "The BGP Path Decision Algorithm" par Juniper© [Junb], deux des plus gros fournisseurs de routeurs BGP. Chaque constructeur implémente le processus en respectant la norme suivante [Joh99] :
- Sélection de la route avec la plus grande préférence (LOCAL-PREF). Si plusieurs routes possibles, passage au point suivant ;
- Sélection de la route ayant le plus petit AS-PATH. Si plusieurs routes possibles, passage au point suivant. Si un AS-SET apparaît dans un AS-PATH, il sera considéré comme ayant une valeur de 1 saut ;
- Sélection de la route ayant le plus petit MULTI-EXIT-DISCRIMINATOR, si la prise en compte de ce paramètre est activée et qu'il existe sur la route reçue. Si plusieurs routes possibles, passage au point suivant ;
- Sélection de la route ayant le NEXT-HOP le plus proche[1]. Si plusieurs routes possibles, passage au point suivant ;
- Si toutes les routes ont été apprises via I-BGP, aller au point suivant. Si plusieurs routes sont apprises via E-BGP, sélectionner la route annoncée par le routeur ayant le plus petit identifiant BGP ;
- Si toutes les routes sont reçues par I-BGP, sélectionner la route dont le voisin I-BPG possède le plus petit identifiant.

En plus des attributs BGP standards, chaque constructeur ajoute des attributs spécifiques qui permettent d'influencer le processus. Les règles de décision étant modifiées par chaque constructeur pour tenir compte des attributs ajoutés, il faut consulter le site de chacun pour connaître les modifications apportées.

Il ne faut pas oublier que les routes sont constituées de préfixes CIDR qui peuvent représenter soit un réseau unique, soit une agrégation. BGP est incapable de savoir s'il ren-

[1] En fonction du coût indiqué dans la table IGP pour atteindre ce NEXT-HOP

contre un préfixe agrégé ou non. Ceci est important à signaler car la règle de base de tout algorithme de routage est de sélectionner le préfixe le plus précis possible.

Les AS-SET représentent ici aussi un danger. L'AS-SET peut représenter l'agrégation de plusieurs sous-réseaux dont les AS-PATH sont différents en longueur. L'AS-PATH résultant de cette agrégation peut être n'importe lequel des AS-PATH des sous-réseaux, le plus long comme le plus court. Comme un seul des AS-PATH est exprimé après cette agrégation, la longueur de celui-ci peut ne pas refléter la longueur réelle du chemin menant à un des sousréseaux. Un AS-PATH contenant un AS-SET ne peut donc être considéré comme totalement fiable.

1.6 Filtres

Les premières utilisations du protocole BGP fonctionnaient avec les paramètres par défaut, c'est-à-dire que les AS propageaient toutes les routes qu'ils connaissaient et laissaient l'algorithme de sélection de la meilleure route travailler par défaut. Avec l'accroissement de la taille de l'Internet et des réseaux connectés, de l'importance des aspects commerciaux et des exigeances des utilisateurs, les AS ont commencé à utiliser les options de BGP que sont les filtres entrant et sortant.

Ces filtres représentent actuellement le cœur de la configuration BGP de chaque AS, car ils permettent de configurer complètement les routes à propager, les routes à refuser, la gestion des communautés et d'autres options BGP.

1.6.1 Filtre entrant

Le filtre entrant agit lors de la réception d'une route pour accepter, modifier ou refuser une annonce. Il agit sur l'AS-PATH en utilisant des règles à expressions régulières et/ou sur le préfixe en utilisant de l'exact matching. Il peut aussi changer le next-hop. En revanche, il ne peut filtrer le champ MED : il peut le modifier, mais ne peut refuser une annonce sur la base de ce champ.

Le comportement par défaut des routeurs est d'accepter toutes les annonces. Un AS peut refuser une annonce ou modifier ses propriétés pour influencer le processus de choix du meilleur chemin. Les modifications peuvent être locales (non transitives) ou propageables (transitives).

1.6.2 Filtre sortant

Un AS peut tenter d'influencer le trafic internet qu'il reçoit en modifiant les routes qu'il annonce. C'est le but du filtre sortant. Le filtre entrant n'est pas suffisant car il n'agit que sur les routes BGP reçues, alors que le routeur peut aussi recevoir des routes à annoncer depuis les protocoles IGP. Le filtre sortant joue donc un rôle de policing et/ou de modification des attributs. Son rôle de policing va même plus loin puisque certains ISP, soit pour des raisons commerciales, soit pour des raisons évidentes de répartition de leur trafic, n'annoncent pas toutes leurs routes à tous ceux avec lesquels ils ont une session BGP. Ces modifications sont

elles aussi soit transitives soit non transitives.

En pratique, le champ MED est également utilisé pour raffiner la procédure de sélection de la meilleure route entre différents AS.

1.6.3 *Politique de routage*

Les deux filtres sont très utilisés actuellement, car ce sont eux qui permettent d'influencer le processus de sélection de la meilleure route. Les options de BGP permettent non seulement d'influencer le processus du (ou des) routeur(s) des AS, mais aussi, suite à des accords, de modifier le processus d'un AS voisin ainsi que la manière dont celui-ci va propager les routes qu'on lui envoie. Les raisons peuvent être de :

1. Modifier le trafic sortant de l'AS en fonction des liens disponibles, de leur capacité et de leur coût d'utilisation ;
2. Modifier le trafic entrant en annonçant ses routes de manière à tenter d'influencer le processus de sélection des AS qui vont chercher à lui envoyer du trafic.

L'emploi des filtres est le moyen le plus puissant de BGP pour effectuer de l'ingénierie de trafic. En effet, on peut non seulement utiliser les filtres pour influencer le processus de décision des routeurs (en modifiant les attributs des routes ou le comportement des routeurs voisins via certains attributs spéciaux), mais également demander aux routeurs d'agréger les routes différemment en fonction de la connexion BGP [O. 03].

1.7 *Inter et Intra-Domaine*

La multiplication des réseaux hétérogènes interconnectés, où chacun était soumis à une autorité de contrôle différente, a posé des problèmes qui ont forcé les autorités régulatrices de l'Internet à proposer une solution : diviser l'Internet en AS interconnectés. Ces AS ont pleine autorité sur leur réseau et en sont pleinement responsables. Le routage des données au sein d'un même AS est assuré par les protocoles Intra-Domaine (IGP) comme OSPF, RIP ou IS-IS. Le routage des données entre AS est assuré par les protocoles Inter-Domain (EGP) dont seul BGP est utilisé actuellement. Cette division en AS (chaque AS représentant un domaine) a permis non seulement de simplifier la gestion de tout l'Internet, car il devient dès lors facile d'ajouter ou de supprimer un AS, mais aussi de chaque domaine, puisque l'AS peut gérer son domaine comme il le veut et choisir la politique qui lui convient le mieux.

1.7.1 *Comment devenir AS ?*

Lors de la division en AS, il a fallu établir certaines règles pour désigner les opérateurs autorisés à être AS [J. 96]. La principale est d'être interconnecté avec d'autres AS et d'avoir une politique de routage différente de ses fournisseurs. En outre, une hiérarchie s'est créée au sein des AS. Les AS les plus gros, qui sont tous interconnectés entre eux et forment l'épine dorsale de l'Internet, sont appelés en anglais Tier-1. Les AS plus locaux (Tier-2) donnent accès à toute une région, à un ensemble de pays ou à un continent. Les AS encore plus spécifiques,

qui couvrent par exemple un pays ou une grosse entreprise, sont appelés Tier-3. Un AS peut changer de catégorie suite à des contacts commerciaux, des choix et des investissements.

Skynet est ainsi considéré à cheval entre un Tier-2 et un Tier-3 car il est client de plusieurs Tier-1 et fournit du trafic pour différents AS et pour des particuliers.

1.7.2 I-BGP et E-BGP

Il existe deux versions de BGP : E-BGP (External) et I-BGP (Internal). I-BGP est le même protocole que E-BGP, dans le sens où il utilise les mêmes messages et la même machine à états, mais il existe des différences majeures entre ces deux protocoles, notamment la manière de réannoncer les routes. E-BGP est utilisé pour les sessions BGP Inter-Domaine et I-BGP pour les sessions BGP Intra-Domaine.

Il ne faut pas confondre E-BGP et I-BGP, qui sont deux versions différentes de BGP, avec les termes EGP et IGP, qui désignent les ensembles de protocoles utilisés pour la communication Inter-Domaine (EGP) et Intra-Domaine (IGP).

E-BGP est donc la version EGP de BGP, mais I-BGP ne doit pas être considéré comme une version IGP de BGP. En effet, I-BGP n'est pas un protocole de routage comme un IGP, mais une version de BGP qui lui permet d'échanger des informations à l'intérieur du domaine. Le fait d'être dans un domaine oblige en effet BGP à avoir un comportement différent, notamment sur la manière de propager des routes. Il est évident, par exemple, puisque nous sommes dans un full mesh, qu'il ne doit pas réannoncer, dans le domaine, des routes apprises par un autre routeur du domaine. Récemment, pour diminuer les inconvénients d'un full mesh, on a introduit des réflecteurs de routes, qui centralisent les annonces d'un domaine. L'interaction entre les réflecteurs et les routeurs est gérée par I-BGP seulement.

Chaque fois qu'il sera mentionné BGP dans la suite de ce document, il faut comprendre E-BGP et non I-BGP.

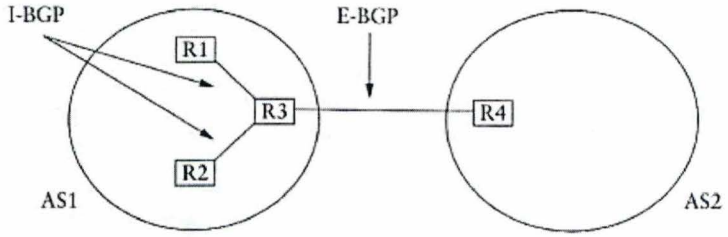

Fig. 1.5: Utilisation de I-BGP et E-BGP [Joh99]

1.8 Evolution de BGP depuis 1995

BGP a été modifié depuis 1995 à la demande des AS, pour faire face à leurs nouveaux besoins. Plusieurs extensions y ont été intégrées. Elles n'ont pas été utilisées pour ce travail,

mais il est intéressant de citer celles qui sont le plus couramment usitées par les ISP :

- ROUTE REFLECTORS : permet d'éviter un fullmesh entre tous les routeurs BGP. Ce système est devenu indispensable vu la taille grandissante des réseaux des ISP ;
- AS CONFEDERATION : permet de découper un réseau en sous-réseaux logiques, chacun d'eux représentant pour BGP un AS dans l'ISP ;
- ROUTE FLAP DAMPENING : le flapping est le phénomène qui apparaît quand une session BGP n'est pas stable. Les routes annoncées par cette session apparaissent et disparaissent en permanence de la table du routeur recevant les routes. Celui-ci va répercuter ces changements à tous ses voisins, introduisant ainsi une instabilité du routage. Le mécanisme de "dampening" a été mis en place pour empêcher une route qui "flap" d'être perçue comme instable. A chaque route est associé un compteur qui est incrémenté lorsqu'une route "flap". Si ce compteur atteint une certaine valeur définie par l'administrateur, la route est considérée comme instable : elle n'entre plus en compte pour la création de la table de forwarding et n'est plus réannoncée. Les compteurs qui ne sont pas à leur valeur minimum (0) sont décrémentés régulièrement, afin de permettre à une route qui a été stabilisée de redevenir entièrement disponible pour le routage. En général, les routes instables ne passent pas plus d'un routeur. Le "route flap dampening" n'est pas efficace à 100%. Le flapping de certaines routes peut passer inaperçu si elle fait partie d'une agrégation. Un route vers un client d'un AS (/24) qui est agrégée par cet AS et annoncée dans un /16 n'apparaîtra jamais comme instable aux yeux des autres AS car elle n'est jamais annoncée directement. Par contre, si la route est annoncée telle quelle, même si le routeur en charge de cette route applique le "route flap dampening", les AS voisins pourraient voir la route apparaître et disparaître régulièrement tant que celle-ci n'est pas devenue stable. Toutefois, ce contrôle permet de rendre moins problématique sur le réseau, car mieux gérée dans le temps, l'apparition et la disparition des routes pour des raisons de flapping ;
- BGP COMMUNITIES : permet d'établir des règles de traitement bien définies au sein d'un AS pour les routes marquées ;
- MULTIPROTOCOL : permet à BGP de transporter des préfixes qui ne sont pas uniquement des préfixes IPv4, mais proviennent d'autres types d'adressages (IPv6, IPX, ...). Le multiprotocol fait l'objet d'une négociation particulière lors de l'établissement de la session BGP.

2. LE PROJET

L'outil d'aide à la décision, destiné à satisfaire un besoin direct chez Skynet, a été développé de manière un peu inhabituelle. L'habitude veut que l'on recherche une solution théorique et que l'on spécifie une architecture de développement lors d'une première phase, pour ensuite coder l'application et finir par une phase de test et de validation. Deux raisons ont empêché le projet d'être développé de cette manière. La première est la méconnaissance pratique de BGP d'un des développeurs. La seconde est l'ensemble des propriétés de stabilité et de vitesse de l'infrastructure réseau utilisée. Ces propriétés sont définies comme des contraintes à respecter, car le réseau utilisé est celui de production de Skynet et non un réseau de test. Il faut un certain temps pour maîtriser ces contraintes et l'ensemble des répercutions qu'elles occasionnent. Pour permettre au développeur de se familiariser avec l'environnement et d'acquérir une certaine maîtrise pratique de BGP, le projet a évolué de manière incrémentale en suivant la progression du développeur.

Ce projet dormait depuis un certain temps dans les cartons, mais, faute de ressources, n'avait jamais pu voir le jour. Un premier plan avait cependant été élaboré par les responsables de Skynet. C'est sur la base de ce plan qu'une analyse détaillée du projet a été réalisée :

- évaluation des outils de collecte des données (15 jours) ;
- création d'un outil de collecte des données (15 jours) ;
- établissement de la stratégie de choix BGP (1 mois) ;
- création de l'outil d'aide à la décision (1 mois) ;
- test et validation (15 jours).

2.1 Evaluation des outils de collecte des données

Cette première phase consistait en une évaluation des outils disponibles sur l'Internet pour collecter des informations provenant des routeurs. Ces outils étant utilisés par d'autres, il semblait utile de partir d'eux plutôt que de concevoir un outil de collecte propre. Les tests étaient très précis :

1. établir la connexion avec un routeur ;
2. collecter les informations de ce routeur suivant des taux d'échantillonnage différents, afin de évaluer la charge que pouvaient tenir les routeurs lors de l'échantillonnage ainsi que la charge que pouvaient tenir la machine de test et ces outils ;
3. introduire les données dans une base de données ;
4. vérifier la validité des données insérées.

Les deux premiers tests n'ont posé aucun problème. Ils ont permis de définir l'échantillonage idéal à 1 pour 1000. Les deux tests suivants, en revanche, se sont révélés catastrophiques. L'outil de collecte stockait les données dans un fichier que le système relisait ensuite pour le stocker dans la base de données, celle-ci reprenant tous les champs définis dans le fichier de sortie (voir la documentation de cflowd dans le Chapitre 3.3 Package cflowd). Cflowd a la particularité de pouvoir renseigner les pertes de paquets subies par le système lors des transferts. Ces pertes étaient nulles sur le système pour un échantillonnage de 1 pour 1000 lors de l'utilisation du package en création de fichier de sortie, mais grimpaient lors de l'insertion dans la base de données. De ce fait, les données stockées dans la base ne représentaient plus le trafic réel. Suite à ces constatations, il a fallu modifier complètement le plan de développement de l'outil pour élaborer le plan final suivant :

- évaluation des outils de collecte des données (15 jours) ;
- adaptation des outils, création de la base de données, vérification de l'outil de collecte (1 mois et 15 jours) ;
- établissement de la stratégie de choix BGP (15 jours) ;
- création de l'outil d'aide à la décision (1 mois) ;
- test et validation (15 jours).

2.2 *Adaptation des outils, création de la base de données, vérification de l'outil de collecte*

Les pertes de performances ont été attribuées à une utilisation processeur excessive à cer- tains moments critiques et à un trop grand nombre d'enregistrements à insérer dans la base de données. Il a donc été prévu de revoir l'outil cflowd, d'y intégrer la possibilité de stocker directement les informations dans une base de données et, enfin, de modifier l'architecture de la base de données pour minimiser le coût des insertions et le coût des traitements, plutôt que d'avoir une base de données conforme aux règles d'architectures habituelles. Les responsables Skynet ont alors imposé de pouvoir *voir* le trafic, via un site intranet et selon différents critères comme le trafic entrant/sortant, le trafic par port ou par AS, le tout sur une période d'un jour, d'une semaine, d'un mois et d'un an. Il a été attribué un mois et demi pour effectuer ces tâches, en réduisant l'établissement de la stratégie de choix BGP à quinze jours, ce qui remplissait tout juste les quatre mois attribués. Vu le timing serré, tout retard ou tout nouveau problème entraînerait le non-développement de fonctionnalités "secondaires".

La base de données est un élément essentiel du projet parce qu'elle va contenir toutes les données de trafic ainsi que toutes les données relatives à la partie BGP du projet, mais aucune définition ou description précise ne peut être donnée. En effet, celle-ci va évoluer avec les différentes parties du projet et sera modifiée ou adaptée selon les besoins.

2.3 *Etablissement de la stratégie de choix BGP*

Cette partie du projet a été prévue comme un temps de réflexion afin de définir la stratégie de choix BGP à appliquer pour le développement de l'outil d'aide à la décision et d'adapter

ensuite cette stratégie aux besoins de Skynet. Les ressources disponibles pour établir ce choix étaient :

1. Les tables BGP de Skynet et les tables BGP des fournisseurs candidats.

   Les tables de Skynet étaient disponibles directement, mais non les tables des fournisseurs candidats. Il fallait donc prendre contact avec eux et voir quelle technique utiliser pour récolter les informations. Deux solutions ont été envisagées : l'établissement d'une session BGP de test entre un des routeurs de Skynet et un des routeurs du candidat ou le placement chez le candidat d'une machine de test permettant de récolter les tables en étant connecté directement sur son réseau. Cette dernière solution, la plus facile, a pu être utilisée dans tous les cas, car les candidats possédaient un point de connexion propre dans les environs.

   Le placement des machines de test sur les réseaux des candidats a fait germer dans l'esprit de l'équipe l'idée d'utiliser ces machines pour d'autres tests que la récupération des tables BGP. Puisque ces machines étaient connectées directement sur le réseau interne du candidat, il devenait intéressant de pouvoir faire des tests de mesure de délai qui n'étaient pas envisageables depuis le réseau Skynet. Le fait de se retrouver directement sur le réseau interne d'un candidat permet de mesurer les délais qu'il rencontre quand on envoie une requête depuis son réseau.

2. Les données de trafic de Skynet.

   Les données de trafic Skynet devenaient utilisables dès l'instant où l'outil de collecte était terminé.

3. L'expérience de la Team Network Skynet.

   L'expérience de la Team Network est un élément primordial car, le temps étant compté, il peut coûter très cher au projet d'évoluer dans une mauvaise direction quant au choix de la stratégie BGP. Le protocole BGP, sous son allure simple, est en fait très compliqué quand on veut interpréter toutes les données correctement et le choix d'une stratégie de sélection est toujours quelque chose de non évident. L'expérience de la team étant jugée plus que satisfaisante, il ne sera pas nécessaire de faire appel à une aide extérieure pour excepté pour des conseils éventuels.

2.4 Création de l'outil d'aide à la décision

Après la définition de la stratégie de choix, le développement de l'outil d'aide à la décision comportera deux phases importantes, la création d'un simulateur BGP et le choix de la meilleure combinaison de fournisseurs.

Le simulateur recevra en entrée les tables BGP des candidats et le trafic entrant de Skynet, permettra de sélectionner les tables que l'on veut combiner pour les tests, simulera le passage de trafic dans la table résultant de la combinaison des tables de test et proposera les résultats de ce passage sous forme de graphique suivant la théorie développée dans la stratégie de choix BGP. S'il est possible d'exploiter les mesures de délai fournies par les machines de tests placées chez les candidats, ces mesures seront intégrées aux résultats.

Ceci clotûre donc l'analyse fonctionnelle du projet, qui n'a pu être complétée qu'au bout des tests effectués sur les outils de collecte. Le schéma de la figure 2.1 montre les différents éléments et les relations entre ces éléments. Cette analyse a ceci de particulier que tous les éléments seront développés l'un après l'autre et qu'avant de les développer, un ajustement de l'analyse donnée ci-dessus pourra être fait avant de commencer le développement de l'élément suivant. Ce détail est obligatoire dans la situation présente car, en fonction des problèmes rencontrés lors du développement d'un élément, qui pourraient provenir de facteurs dont il n'a pas été tenu compte dans l'analyse principale (problèmes dus à la vitesse de fonctionnement des routeurs, aux tables BGP des candidats que nous ne connaissons pas encore, aux machines de tests et à leur installation), les fonctionnalités de l'élément à développer pourraient être modifiées.

La figure 2.1, qui présente le plan global du projet, indique également la nature de certains processus. Les processus indiqués comme prédéfinis sont des processus entièrement automatiques, alors que les processus manuels requièrent une intervention humaine pour sélectionner les données à traiter ou encore changer les paramètres d'exécution du processus. Deux processus sont définis comme *hybrides*, c'est-à-dire qu'ils peuvent fonctionner en mode entièrement automatique, mais permettent aussi une paramétrisation. Les *Données stockées* sont simplement les étapes impliquant un stockage dans la base. Ces étapes sont importantes car ce sont les étapes où l'on va fixer des données afin de permettre des traitements ultérieurs comme l'archivage ou la vérification. Ce sont les seules étapes où l'on peut *voir* les données.

Les responsables souhaitent que le projet n'utilise que des technologies gratuites. Il est obligatoire que l'outil soit développé sous Linux en utilisant la distribution Debian [Deb] et, de préférence, les outils proposés par cette distribution.

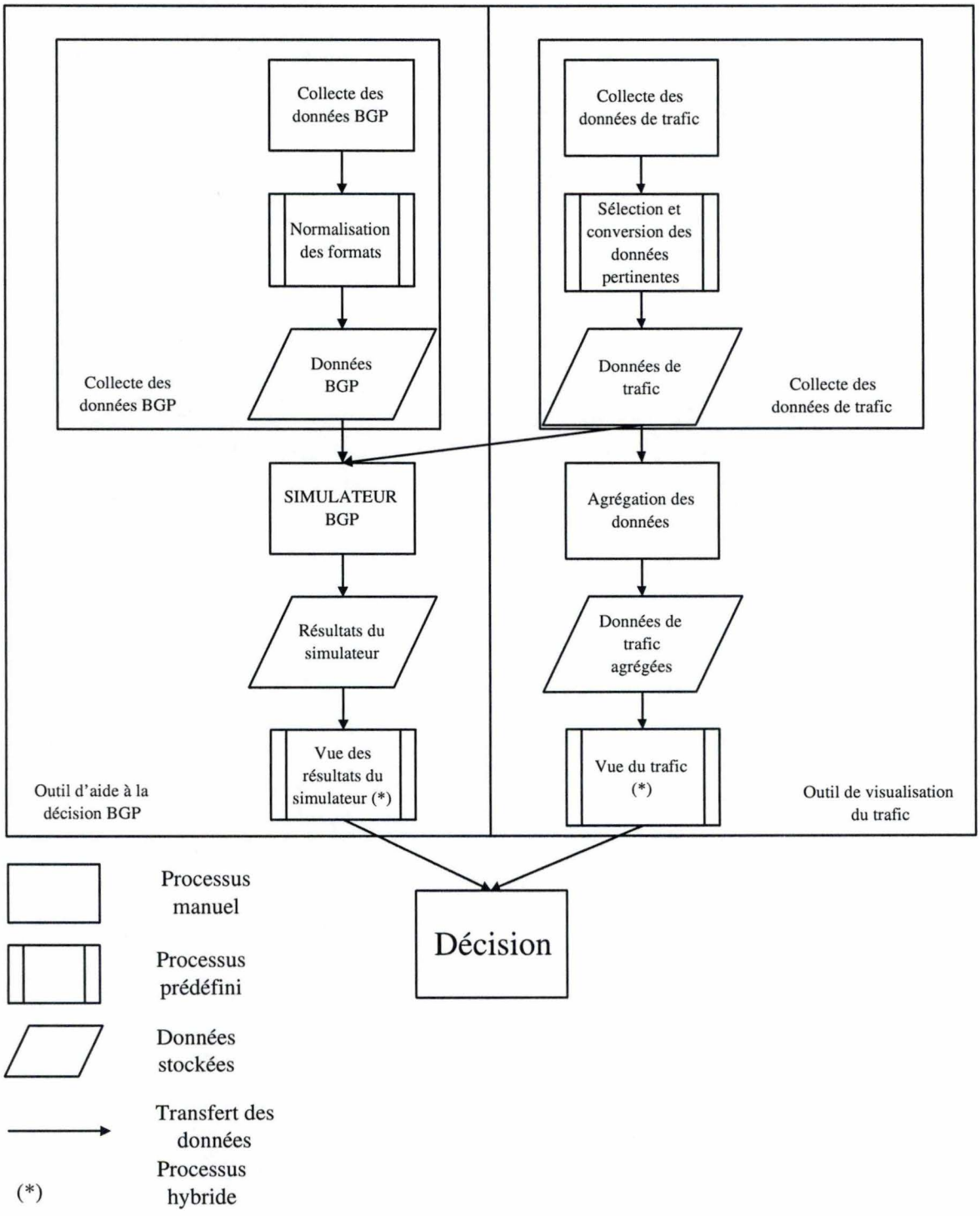

Fig. 2.1: Diagramme des flux du projet

3. VISUALISATION DU TRAFIC

L'outil de visualisation a été créé en plus du projet original. A la suite des discussions menées avec les dirigeants de Skynet lors du développement de l'outil de collecte des données, il a été décidé de le développer de manière plus approfondie pour permettre non seulement de collecter les données, mais aussi de les visualiser selon les critères désirés (ports, AS, répartition sur les liens des fournisseurs, ...).

3.1 Travaux déjà effectués

Afin de pouvoir fournir au lecteur les moyens de développer une stratégie d'ingénierie de trafic de manière automatique, quelques travaux ont analysé la répartition du trafic Internet, en un point d'échange ou pour un ISP, selon des critères géographiques, de délais et/ou d'efficacité du routage.

3.1.1 CAIDA

Le travail de CAIDA [Ing01] s'intéresse à la répartition géographique du trafic. Il se fonde sur des traces de trafic prises à un point de peering gratuit (AIX : NASA AMES Internet Exchange). Ces points, très convoités par les ISP, ne fonctionnent pas comme un peering normal, d'abord parce qu'il faut un accord explicite entre les deux parties pour autoriser un peering entre elles et, ensuite, parce que les ISP ne sont pas obligés d'annoncer toute leur table de routage en ce point.

Le travail du groupe CAIDA montre que la majorité du trafic généré sur ce point est produit par les USA (92%). Le reste est produit par les autres pays, le Japon générant 22% des 8% restants. En ce qui concerne les destinations, le pourcentage de trafic à destination des USA chute à 69%. Avec 23% du trafic restant (7% du total), le Japon est la deuxième destination privilégiée, suivi par le Royaume-Unis (22%) et la Suède (19%). CAIDA en conclut que les USA sont la source principale du trafic internet de ce point et que les américains consomment eux-mêmes presque tout leur trafic. Seul 31% du trafic est orienté vers l'international. CAIDA estime que la répartition du trafic est en général de 80/20% (80% de trafic généré en ce point est à destination du pays où se trouve le point). Cette répartition devrait se vérifier à tous les points de peering d'envergure internationale, mais n'est pas valable pour l'étude du trafic au niveau des Etats (Américains) que l'on pourrait comparer à des points de peering au niveau régional ou interrégional en Europe.

Cette conclusion est juste à un détail près. Un point de peering gratuit représente les échanges gratuits de trafic entre les peer **présents**, sur base d'un accord explicite quant aux préfixes échangés. On ne rencontre pas de trafic de transit sur un point d'échange gratuit. Ce

travail ne peut donc être considéré comme une analyse détaillée et complète du trafic Internet mondial, mais uniquement comme une étude montrant que sur les points gratuits du réseau, le trafic généré est fonction de la position géographique du point choisi. En ce qui concerne l'échange de trafic payant et donc commercial, il faudrait une nouvelle étude plus complète qui fasse en outre la distinction entre les ISP intervenants, sachant que tous les ISP ne font pas du transit et que tous ne sont pas de taille mondiale.

Ce travail ne nous donne aucune information quant aux tables de routage utilisées. Le travail a été publié pendant l'hiver 2001, mais les données ne sont pas datées.

3.1.2 Les travaux de Steve Uhlig

Les traces analysées par Steve Uhlig [UB] montrent la répartition du trafic sur la base de données collectées chez deux ISP : un ISP offrant du trafic aux universités et réseaux de recherche belges (BELNET) et un ISP privé offrant un accès DIAL-UP (Yucom). Les traces sont datées de décembre 1999 pour BELNET et avril 2001 pour Yucom et couvrent respectivement 6 et 5 jours de trafic. Le réseau BELNET [Bel] est construit autour d'une étoile dont les branches sont des liens à 34 Mbps reliant notamment les universités. Les liens vers l'extérieur sont assurés par deux connexions (34 et 45 Mbps) contractées chez deux ISP commerciaux et par une présence aux points de peering gratuits BNIX (Bruxelles) et AMS-IX (Amsterdam). Chaque poste du réseau est connecté via une ligne à 10 Mbps.

Aujourd'hui, il faut prendre ce travail avec certaines précautions, dues à l'évolution des infrastructures des ISP et à l'évolution des techniques d'accès grand public. D'après Steve Uhlig, BELNET peut être considéré comme un fournisseur proposant un service de type ADSL. Or, malgré la vitesse de connexion minimum de 10 Mbps, supérieure aux 3.3 Mbps actuellement proposés par les fournisseurs ADSL en Belgique, la charte de BELNET et le comportement des utilisateurs du réseau font que le trafic Internet de BELNET ne peut représenter celui d'un ISP privé. En effet, BELNET n'autorise le passage par son réseau que d'informations à caractère éducatif ou scientifique, alors que la majeure partie des utilisateurs privés utilisent des logiciels de partage de fichiers (MP3 et autres). Cette différence d'attitude influence directement le trafic.

Yucom, quant à lui, représentait certainement un ISP non négligeable, à l'époque des prises de mesure, par son trafic DIAL-UP. Mais aujourd'hui, les ISP n'offrant qu'un point d'accès de type DIAL-UP ne peuvent plus refléter une répartition correcte du trafic Internet généré en Belgique, pour deux raisons : le nombre d'utilisateurs ADSL est supérieur aux utilisateurs DIAL-UP et la différence de vitesse fait qu'un seul utilisateur ADSL représente cinquante utilisateurs DIAL-UP (56 kbps contre 3,3 Mbps). L'ISP privé Skynet, par exemple, n'enregistre plus que 1% de son trafic généré par le DIAL-UP et cette valeur est à la baisse.

L'analyse de Steve Uhlig met en évidence diverses caractéristiques du trafic des deux ISP. La première est la longueur moyenne de l'AS-PATH, 4.2 pour Yucom et 4.5 pour BELNET. Pour Yucom (dont les traces sont les plus récentes), 80% du trafic passe par des routes dont l'AS-PATH est de longueur trois AS ou moins. Beaucoup des préfixes les plus actifs sont distribués avec des routes performantes en terme d'AS-PATH et hébergés par des AS de

moyenne, voire de grande importance. En effet, puisque Yucom et BELNET vont eux-mêmes chercher leur connectivité internationale chez un fournisseur, cela signifie qu'il n'y a plus que deux AS derrière ce fournisseur pour rejoindre le préfixe, ce qui est relativement performant.

Un deuxième point important est la distribution des préfixes avec lesquels il y a échange de trafic. Elle est semblable pour les deux ISP : à savoir, concernant le top 100 des AS (respectivement des préfixes), 72% du trafic absorbé pour Yucom (52%) et 60% pour BELNET (40%). 90% du trafic est absorbé par 4.7% des AS et par 4.1% des préfixes pour Yucom alors que Belnet enregistre 9.8% des AS et 4.5% des préfixes. La différence s'explique certainement par le temps entre les mesures (16 mois), ce que semble étayer le cas de Skynet, qui a connu une évolution non négligeable de sa bande passante au fil du temps.

Un troisième élément important de cette analyse est le pourcentage de trafic par AS. A une distance de 1 hop (BGP hop), 64% du trafic de Yucom passe par 1 seul AS (42% pour Belnet). Si l'on considère les trois AS les plus importants, le taux monte à 87% et 83%. La différence entre BELNET et Yucom ne peut s'expliquer par la seule évolution de l'infrastructure de l'Internet sur 16 mois, mais également par la différence de comportement des utilisateurs. BELNET s'adresse majoritairement à des universitaires qui maîtrisent souvent mieux l'anglais que les utilisateurs privés et naviguent plus fréquemment sur des sites anglophones. D'autre part, un universitaire utilise le net pour ses recherches, tandis qu'un utilisateur privé y cherche plutôt du loisir ou des informations précises dans des domaines tout à fait différents (les voyages, la vente de bien, la communication, ...).

Enfin, Steve Uhlig montre que lors de traces mesurées sur un laps de temps supérieur à 15 minutes, un ISP de taille moyenne échange des informations avec une grande partie de l'Internet, ce qui veut dire que même les préfixes les moins utilisés génèrent du trafic.

En conclusion, nous noterons la proportion des AS et des préfixes qui absorbent le trafic afin de les comparer avec les données récentes de Skynet. Ceci est capital pour notre travail, puisque notre but est de trouver la combinaison d'ISP qui offre les meilleures performances au niveau des peering, l'un des facteurs étant la proximité en terme de nombre d'AS traversés pour atteindre un préfixe.

3.2 Analyse

3.2.1 Analyse fonctionnelle

L'outil de collecte initialement prévu devait, en utilisant Netflow [Sys] comme protocole de communication avec les routeurs, recevoir les données de ceux-ci et les stocker. Ce trafic récolté, nous avons utilisé Flowscan [CAIb] pour afficher les résultats et vérifier que le système de capture fonctionnait bien. Le seul défaut était que toutes les informations stockées dans la base de données n'étaient pas utilisées par Flowscan, alors que certaines d'entre elles étaient fort intéressantes pour les responsables Skynet. Ceux-ci ont dès lors demandé que ces informations soient rendues disponibles. Le but de ce contrôle n'est pas de savoir si les utilisateurs visionnent plutôt des sites de loisir, de travail ou de jeu, mais tenter de connaître les propor-

tions de trafic de type Peer to Peer (P2P), HTML, FTP, telnet et autres. Flowscan demandant beaucoup trop d'adaptation de sa configuration pour afficher ce genre de données, un autre outil devait être développé, ce qui était tout à fait possible, puisque l'ensemble des données brutes était à disposition.

Vu les nombreuses options et les premiers tests avec la base de données, les 15 jours initialement prévus pour le développement de l'outil de collecte ont été allongés à un mois, en réduisant le choix de sélection de la stratégie BGP à 15 jours. Les options suivantes doivent apparaître dans l'outil :

- vue du trafic entrant et sortant par AS ;
- vue du trafic entrant et sortant par port (HTTP = 80, FTP 20 et 21,...) ;
- vue du trafic entrant et sortant par peer connectés.

Chacune de ces trois options doit proposer une vision à partir des données journalières et une autre à partir des données hebdomadaires. Les données journalières proviennent directement de la base de données, sans traitement, alors que les données hebdomadaires ne sont disponibles que sous forme concaténée. Deux concaténations, une en tranche horaire et une en tranche journalière, doivent être disponibles. Les pages web doivent proposer une vue chiffrée très lisible pour les comparaisons et une vue graphique permettant de voir les évolutions. Le site web servant à la consultation des données respectera la forme suivante :

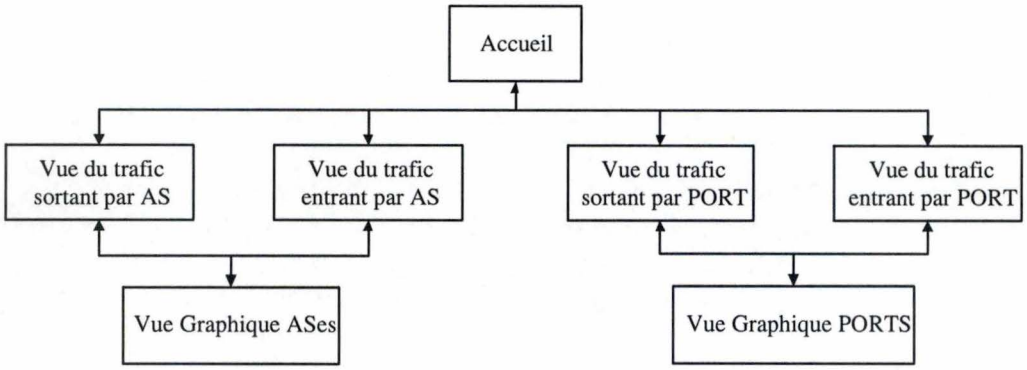

Fig. 3.1: Diagramme du site de consultation des données de trafic

Chaque page en mode texte doit permettre de :

- sélectionner les AS ou ports pour lesquels on désire une vue graphique des données ;
- permettre le dessin cumulé en ce qui concerne les ports ;
- proposer un affichage du trafic global.

Les pages en mode graphique ne doivent pas faire l'objet d'une attention particulière. Les seules exigences sont la clarté du graphique et la possibilité de pouvoir exporter celui-ci aisément.

3.2.2 Analyse non fonctionnelle

La base de données étant mise à jour toutes les heures, le temps de calcul d'un graphique ne peut dépasser une heure. Un temps de calcul plus long provoquerait les problèmes suivants :

1. L'affichage de résultats erronés, dus à l'exécution simultanée des requêtes d'insertion et de sélection ;
2. La corruption des données de la base, car, en cas de surcharge, mysql rompt les requêtes en cours sans faire de rollback (Mysql 3 n'est pas transactionnel, voir Chapitre 5 §2.1).

De plus, pour le confort d'utilisation de l'application, il est évident que la minimisation du temps de génération est un facteur important.

Enfin, donner la possibilité de sélectionner les données à afficher fait que les graphiques ne peuvent être précalculés.

3.3 Netflow

Netflow est un standard développé par Cisco [Cisb]. Il permet à des routeurs de transmettre des informations en envoyant des copies de paquets au format Netflow à une adresse IP. C'est l'outil idéal pour effectuer des mesures de trafic de la manière la plus transparente et la plus fiable car ce protocole est intégré dans les routeurs. Les données sont donc prises à la source.

Il existe plusieurs versions de Netflow. Seule la version 5 est supportée par les routeurs cisco et Juniper [Junb] qui équipent Skynet.

Les figure 3.2 et 3.3 montrent la structure de données utilisée par la version 5 de Netflow.

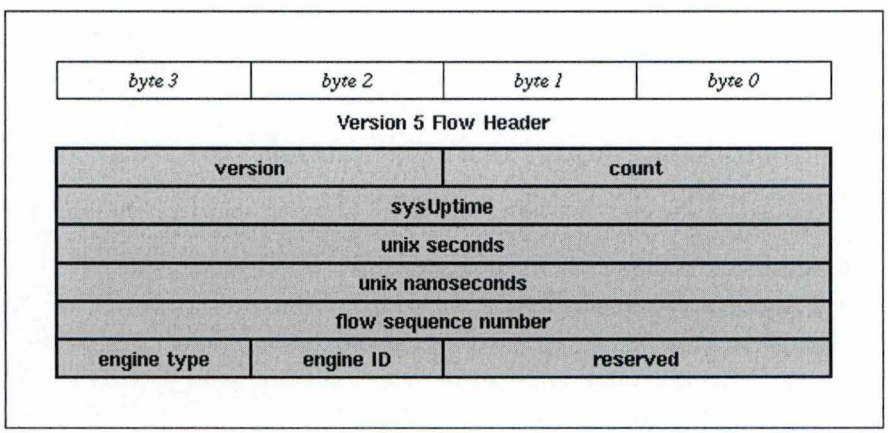

Fig. 3.2: Header de flux Netflow

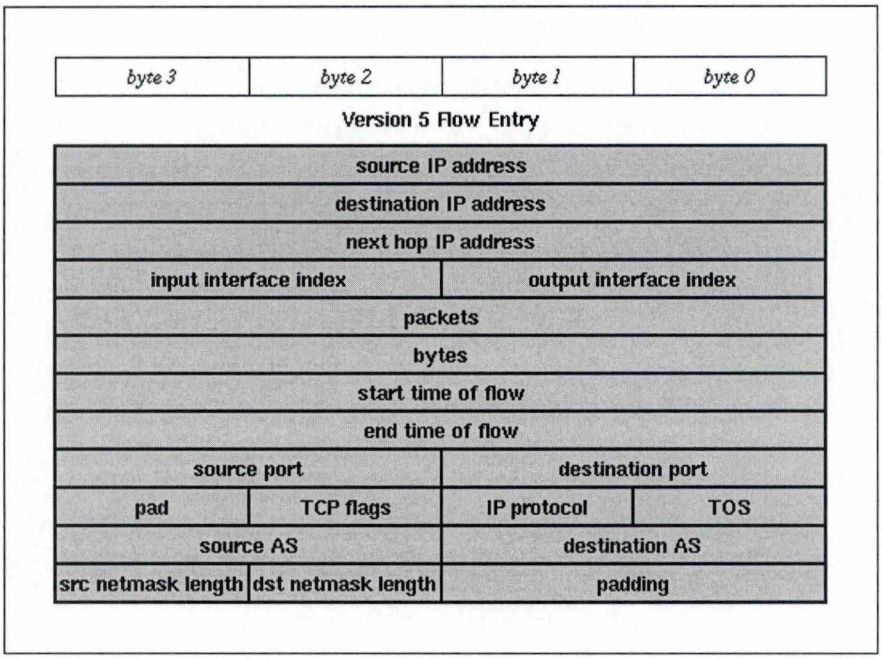

Fig. 3.3: Contenu de flux Netflow

Cette version permet deux modes de communication : avec ou sans échantillonnage. Si le protocole est configuré pour tourner dans le premier mode, le routeur envoie une copie de paquet suivant un taux d'échantillonnage défini. Dans le deuxième mode, c'est une copie de chaque paquet qui est envoyée.

Skynet étant un ISP à caractère international qui supporte une bande passante de plusieurs Gb/s, il est impossible de faire tourner Netflow en mode non échantillonné. Deux raisons à cela :

1. Aucune machine n'est capable de recevoir plusieurs Gb/s d'informations tout en les traitant ;
2. Les routeurs qui équipent Skynet ne sont pas capables de tourner en mode non échantillonné, même s'ils offrent la possiblité de le faire. Leurs performances se dégradent de manière trop importante.

Nous avons opté pour un taux d'échantillonnage de 1/1000, ce qui ramène la bande passante à une vitesse plus raisonnable de quelques Mb/s.

Lorsqu'on active le mode échantillonnage d'un appareil, il paraît logique que celui-ci respecte les normes de prise de mesures et effectue son échantillonnage suivant une distribution de Poisson [Bég]. Or, les routeurs fonctionnent à de très hautes vitesses. Pour éviter de surcharger le routeur par des opérations de calcul superflues et non indispensables à son fonctionnement, le mode d'échantillonnage est un mode linéaire : si l'on demande un échantillonnage de 1/1000, le routeur envoie la copie d'un paquet puis attend 999 passages de paquets avant d'envoyer une nouvelle copie. Vu la vitesse du trafic sur les routeurs, cela ne représente rien de significatif en ce qui concerne les mesures. A des vitesses beaucoup plus faibles, il faut, dès que possible, augmenter le taux d'échantillonnage ou passer en mode non échantillonné.

3.4 Package cflowd

Les flux Netflow sont envoyés directement vers une machine. Ces flux doivent être reçus et décodés, pour ensuite placer dans la base de données uniquement les données définies dans le cadre du projet. La réception des flux peut être effectuée soit par un nouvel outil à développer à cet effet, soit par un outil existant, à adapter au besoin. Le choix, vu les contraintes de temps, a été d'opter pour un logiciel existant et disponible gratuitement sur l'Internet : le package cflowd [CAIa].

Ce package de capture de flux, développé sous licence GPL [Ope91], se compose de trois applications distinctes (figure 3.4) qui s'enchaînent pour stocker les données reçues dans un format spécifique (arts). La première, cflowdmux, récupère les flux envoyés par les routeurs et les écrit en mémoire (figure 3.5). La deuxième, cflowd, lit ensuite la mémoire partagée et formate les données en suivant ses classes internes. Les données reformatées sont accessibles et utilisables soit par les outils d'analyse de flux fournis avec le package, soit par des applications qui se connectent directement à cflowd. La troisième et dernière application, cfdcollect, se connecte à cflowd pour récupérer les données et les archiver sous un format arts (figure 3.6). Les options par défaut sont un fichier par jour et par routeur. Le format de fichier arts n'est pas directement exploitable par des outils non spécifiques. Il en va de même pour les données brutes cflowd. La nécessité de retransformer le fichier arts ou les données cflowd est une source importante de perte de performances.

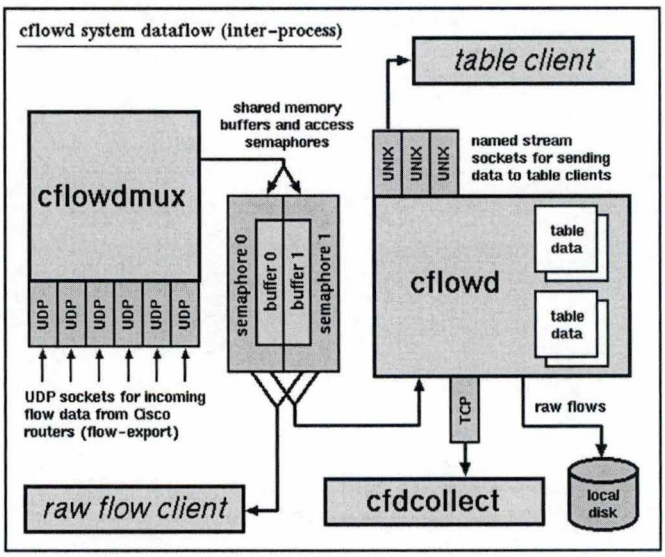

Fig. 3.4: Description du fonctionnement du package cflowd

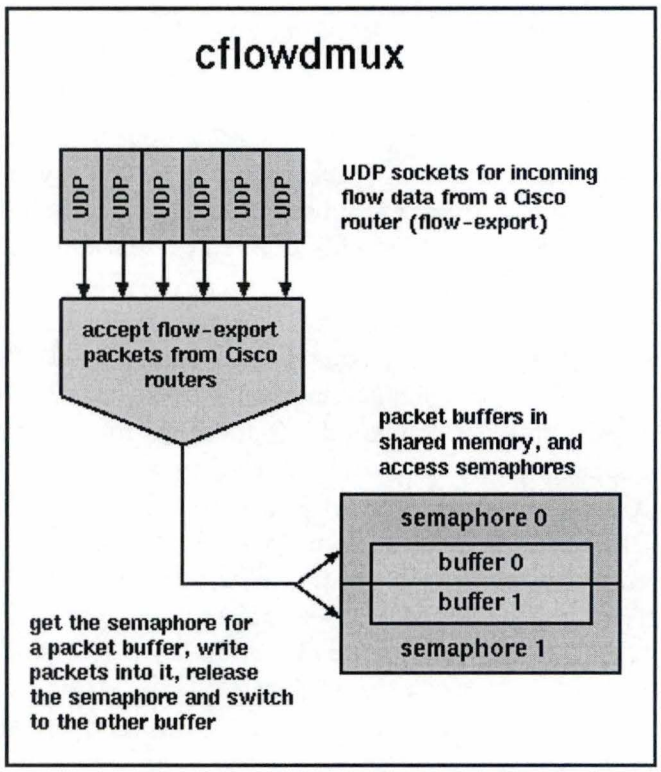

Fig. 3.5: Description de cflowdmux

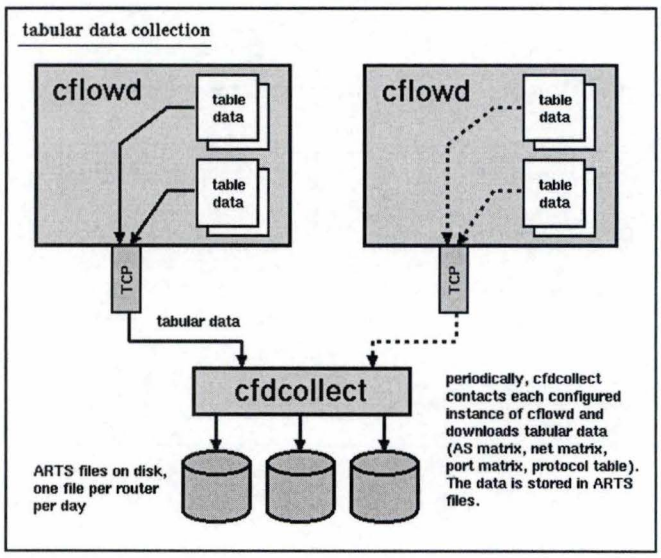

Fig. 3.6: Description de cfdcollect

L'utilisation de cfdcollect permet en outre de voir si des paquets ont été perdus lors des échanges. Ce contrôle est essentiel, car tout flux perdu entraîne automatiquement une

erreur dans la représentation du trafic et donc, ensuite, dans la pondération des tables BGP. Des pertes de flux peuvent être engendrées soit par le manque de place mémoire qui oblige cflowdmux à effacer des flux avant que cflowd ne les ai relus, soit quand les flux arrivent trop vite et qu'entre deux relectures de la mémoire, cflowd n'a pas eu le temps de terminer le traitement des flux précédemment lus.

Les auteurs de l'application reconnaissent eux-mêmes que cflowd n'écrit pas directement sous forme de fichiers les données formatées parce que les I/O sont encore actuellement trop lentes pour permette à cflowd de suivre des flux à haut débit.

Après utilisation en charge réelle et recherche de la meilleure configuration, nous n'avons pu trouver une méthode qui, en utilisant le package tel quel, nous permette de réduire les pertes de flux tout en conservant un maximum de données.

Dans le souci de pallier ce problème, nous avons modifié cflowd afin de pouvoir rediriger directement le flux de sortie à notre guise et dans le format souhaité et d'éviter, ainsi, les pertes de données dues aux multiples I/O et à l'utilisation CPU faite par cfdcollect.

3.4.1 Analyse des modifications

Cflowd est un logiciel écrit en C++. Des trois parties du package, seule la deuxième, cflowd, sera modifiée afin de ne plus devoir utiliser cfdcollect dans un autre but que le contrôle des pertes de flux.

Cflowd utilise des classes internes pour récupérer les flux Netflow 5 et les convertir en un objet que la classe cflowdRawFlow permet de reformater pour la sortie. C'est cette classe que nous allons modifier afin qu'elle puisse écrire les informations que nous souhaitons. En outre, si cflowd, dans la documentation, est censé ne pas sortir de fichier, des fichiers rawflow (données brutes) sont créés sur le disque. Nous avons profité de notre travail dans les classes cflowdRawFlow pour désactiver la fonction d'écriture des fichiers de données brutes et gagner ainsi en performance.

Le fonctionnement de cflowd est très complexe et utilise un nombre important de classes différentes. Nous nous sommes focalisés uniquement sur les modifications que nous souhaitions faire, sans chercher à découvrir tous les mécanismes du logiciel et sans modifier son fonctionnement interne, qui ne fera donc l'objet d'aucune explication dans ces pages.

Les modifications à apporter au module de création du fichier de sortie sont :

- ajouter la création d'un fichier dans un format personnalisé ;
- ajouter la possibilité d'insérer directement, dans une base de données, les données contenues dans les flux.

Ces modifications étant des options supplémentaires ajoutées au logiciel, il faut aussi changer les options disponibles dans la ligne de commande, ainsi que les fichiers de configuration.

Le traitement des fichiers de configuration est réalisé par les règles et fonctions définies dans un format LEX. Pour traiter la nouvelle configuration, il faut modifier les règles LEX et y ajouter de nouvelles règles pour les nouvelles options de configuration. Ces dernières

doivent permettre de traiter un fichier de configuration pour la base de données comportant les options habituelles d'accès à une base de données, à savoir l'adresse IP du serveur, le port de communication, le nom de l'utilisateur, son mot de passe si nécessaire ainsi que le nom de la base à laquelle on souhaite se connecter.

Ces options doivent permettre à l'application de se connecter à n'importe quel type de base de données qui accepte les connections TCP pour son interrogation.

Pour respecter l'architecture de cflowd, nous avons créé un module de contrôle de l'accès à la base de données. Ce module est activé par la ligne de commande et peut recevoir un certain nombre de paramètres. Ceux-ci permettent notamment d'activer le module soit uniquement en insertion dans une base de données, soit en écriture directe de fichiers, d'activer les deux modes ou encore de spécifier le nom du fichier de sortie en fonction de l'unité de temps que l'on souhaite pour la capture (un fichier par heure ou un fichier par jour) afin de pouvoir insérer manuellement ce fichier dans une base de données. Cette dernière option est directement utile, car, le package permettant de faire tourner plusieurs instance de cflowd, on peut, pour des raisons de sauvegarde, avoir une instance qui génère des fichiers horaires à traitement direct et une autre qui génère des fichiers journaliers à des fins d'archivage.

L'ensemble de ces options servent uniquement au contrôle direct du module. On peut se demander pourquoi ne pas utiliser uniquement la ligne de commande ou uniquement les fichiers de configuration. Il est vrai que les paramètres de fonctionnement du module auraient pu être intégrés dans le fichier de configuration, mais cflowd est développé de manière à transmettre via la ligne de commande les options de contrôle direct des modules et à écrire dans les fichiers de configuration les données de connexion vers des outils extérieurs.

Les modifications permettent de conserver une utilisation classique de cflowd, il sufit de ne pas utiliser le nouveau module.

Liste des fichiers modifiés :
- /classes/src/CflowRawFloLogger : écriture du flux, soit dans un fichier, soit dans la base de données, soit dans les deux ;
- /classes/src/CflowConfig.cc.in : configuration par défaut ;
- /classes/src/Makefile.in : sert à compiler et à installer l'application, échange des configurations LEX ;
- /classes/src/configplus.lex : contient toutes les règles LEX, les anciennes et les nouvelles ;
- /classes/src/CflowdConfig.cc : configuration par défaut générée à partir du .cc.in ;
- /classes/include/CflowdDbModule.hh : header du module de base de données ;
- /classes/include/CflowdConfigLex.hh : header de la configuration LEX ;
- configure.in : permet l'utilisation de la commande configure de Linux.

3.5 JPGraphe

Le projet requiert la production de graphiques sur des pages WEB. Il existe l'outil RRDTOOL [Tob] qui tourne sous linux et qui permet de tracer des graphes personnalisés. Cet

outil est très puissant, mais surtout très complexe à mettre en oeuvre pour ceux qui ne l'ont jamais utilisé. Nous avons recherché un autre outil, plus simple, qui permette d'atteindre le même résultat.

Cet outil est JPGraph, une bibliothèque PHP, donc portable alors que RRDTOOL est un outil exclusivement unix. JPGraph permet de tracer des graphiques et d'autres schémas de manière très simple.

3.6 La base de données, réalisation et exemples de résultats

3.6.1 La base de données du trafic

La base de donnée BGP, décrite dans le chapitre 5 (5.2.2, p.54), permet, grâce aux tables des candidats ainsi qu'aux données de trafic, de présenter, en résultat du simulateur, une estimation réaliste de ce que deviendrait le trafic avec la table de routage créée à partir des tables des candidats. Cela permet de constater que le simulateur à besoin de deux types d'information en entrée : les tables de routage des candidats et des données concernant le trafic de l'ISP étudié. Alors que les premières font partie de la base BGP, les secondes sont fournies par la partie "trafic" de la base.

La figure 3.7 montre les tables principales de la partie "trafic". Seule la table BGPPEER ne lui appartient pas : elle apparaît ici pour permettre d'établir le lien entre les deux bases.

Cette partie de la base a aussi été développée au fur et à mesure de l'évolution du projet pour rencontrer les besoins que nous dégagions.

ROUTERINTERFACE

Table contenant les informations des interfaces des routeurs. Cette table permet d'automatiser la récupération des données en autorisant le suivi de la configuration de la capture des flux pour faire en sorte que tout changement sur un routeur soit facilement pris en compte par l'outil. Tous les autres champs sont susceptible de changer de valeur dans le temps.

Le type d'interface est I ou O, (In ou Out), selon qu'il s'agit d'une interface d'entrée vers le réseau de l'ISP ou de sortie du réseau de l'ISP. ACTUAL peut prendre les valeurs 1 ou 0, 1 indiquant une interface en cours d'exploitation et 0 une interface non utilisée.

ASHX

Tables comprenant les agrégations par heure du trafic par AS. Les données sont insérées directement dans ces tables qui sont numérotées de 0 à 49, permettant de stocker 48 heures de données. Le format de ces tables est toujours le même.

La clef primaire est ROUTER,IDPEERSRC,IDPEERDST,SRCAS,DSTAS,HEURE. En effet, l'ensemble de ces champs détermine un seul échantillon.

L'ensemble des tables traitant des AS a la même structure. Seul le nom de la table permet de savoir si l'agrégation appliquée à l'information est de type "horaire" (H), "journalière" (D) ou encore "mensuelle" (M), sachant que l'on stocke huit jours d'informations pour les

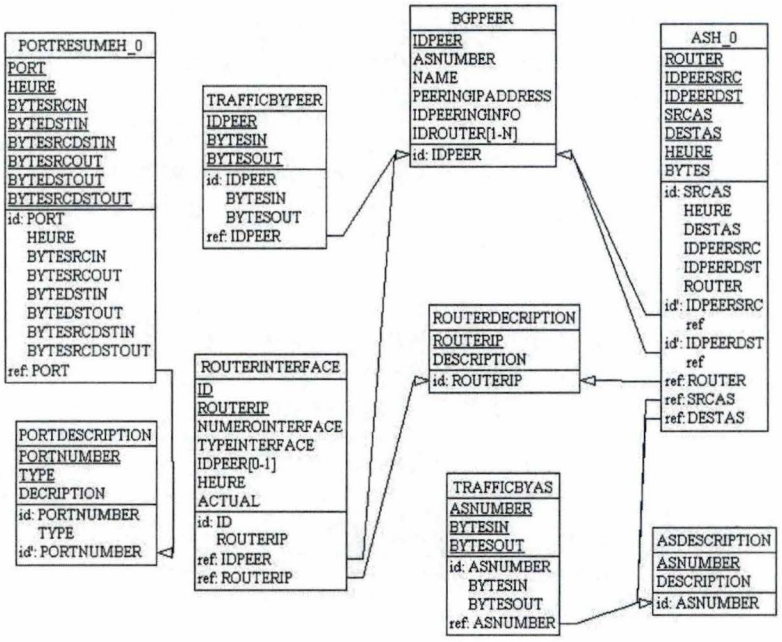

Fig. 3.7: Partie trafic de la base de données, tables principales

agrégations journalières et treize mois pour les mensuelles. Ensuite, on a le choix entre archiver les données mensuelles ou encore les agréger en données annuelles.

PORTRESUMEHX

Les tables d'agrégation des ports respectent la même nomenclature que pour les AS, mais leurs structures sont différentes. Il faut ici stocker les informations directement en fonction des ports et non des adresses IP source ou destination.

Comme pour les tables ASHX et pour la même raison, la clef primaire est définie explicitement comme incluant tous les champs, sauf le champs BYTES.

La technique d'agrégation est la même que pour le trafic par AS.

ROUTERDESCRIPTION

Table contenant la description des différents routeurs sur lesquels nous collectons les données.

ASDESCRIPTION

Table contenant la description des AS. Cette table sert de tampon afin d'éviter de consulter systématiquement le RIPE (Réseaux IP Européens) ou tout autre organisme Internet qui permet d'identifier un numéro d'AS. Si un numéro d'AS apparaît dans les données de trafic et n'est pas connu dans cette table, sa description y sera ajoutée.

PORTDESCRIPTION

Cette table sert à stocker une description des ports afin de mieux comprendre et identifier

le trafic lors de l'affichage des informations. Une liste "officielle" de la description des ports TCP-IP est maintenue par l'IANA [IAN04] et permet de remplir cette table pour les ports dit *Well Known*. les *Registered* ne sont pas fiables car pas toujours effectivement utilisés pour l'usage décrit : nous avons préféré laisser ce type de trafic *inconnu* ou tenter de l'identifier nous-mêmes et d'ajouter alors la description qui nous convenait.

TRAFFICBYPEER

Table comprenant la répartition du trafic par peer. Elle permet de surveiller les liens établis avec les fournisseurs de notre ISP. Elle est créée non pas avec les données concernant les AS dans les paquets reçus, mais en identifiant l'interface utilisée pour transmettre le paquet, en attribuant le trafic au PEER associé à cet interface.

TRAFFICBYAS

Table comprenant la répartition du trafic par AS. Le but recherché est d'identifier, par AS, les quantités de trafic entrant et sortant.

3.6.2 Développement des caches

Etant donnée la taille importante des tables utilisées et le temps de calcul nécessaire pour générer une page, nous avons décidé de créer des caches. Ceux-ci ne sont en aucune manière obligatoires : ils apportent uniquement un confort supplémentaire à l'utilisateur. Ils doivent être paramétrés correctement afin de garder un caractère très récent pour les données.

Les tables des caches peuvent être créées comme on le désire, en fonction des données que l'on souhaite afficher rapidement, tout en gardant à l'esprit que l'on ne peut pas mettre des caches sur toutes les tables : on risquerait d'obtenir un système incapable de satisfaire les requêtes pour rafraîchir ces caches, tant ces requêtes peuvent être lourdes, ce qui annihilerait complètement le rôle des caches.

3.6.3 Réalisation

L'ensemble des données se trouvant dans la base de données, il ne reste plus qu'à les afficher dans un format correct. Pour ce faire, nous avons utilisé des scripts PHP qui permettent de récupérer les informations de la base.

Afin de permettre tous les calculs d'agrégation du trafic et de calculer les quantités entrantes et sortantes, il est important de bien dissocier les informations fournies par les paquets Netflow. Le calcul du trafic par AS ne pose aucun problème, il suffit de stocker les informations comme elles viennent. Cela n'est pas aussi simple pour les ports, qui demandent de regrouper le trafic correctement, puisqu'on ne désire pas calculer le trafic par port par préfixe, mais par port uniquement. Il faut donc convertir les données et répartir le trafic par port et non plus par préfixe. De plus, afin de pouvoir calculer le trafic entrant et sortant, il faut, pour chaque port, ventiler les informations en connaissant le nombre de paquets (entrants ou sortants) qui utilisent ce port soit comme *destination*, soit comme *source* ou encore comme *source et*

destination. Il est important de faire les trois distinctions, sinon le trafic ayant le même port *source* et *destination* pourrait ne pas être comptabilisé correctement.

Lors du développement, nous nous sommes aperçus que les références données dans les paquets Netflow, qui permettent de caractériser les paquets entrants ou sortants, n'étaient pas stables. En effet, Netflow indique l'interface de sortie du paquet (voir description du protocole Netflow) par un numéro que le routeur sélectionne à chaque démarrage. Les routeurs n'étant pas sujets aux redémarrages fréquents, ceci nous avait échappé jusqu'au jour où les courbes de trafic dessinées par l'outil ne correspondèrent plus aux courbes réelles données par les autres outils de management du trafic interne à Skynet. Après découverte de la source du problème, nous avons modifié les données insérées dans la table. Chaque numéro d'interface renseigné dans un paquet est ainsi remplacé par un numéro virtuel de type d'interface, géré via une page WEB (figure 3.8). Lorsqu'un routeur redémarre, le responsable vérifie le numéro et le type de chaque interface et, si nécessaire, effectue les changements via la page web.

Un deuxième problème a été mis en évidence lors du développement : le temps de calcul des scripts. Parfois, le nombre d'informations à lire dans la base rend les scrips PHP très longs, voire trop. C'est le cas pour l'affichage du trafic total de Skynet en mode chiffre, par AS. Il a été décidé de développer un système de cache qui se met à jour automatiquement suivant le type de données demandé. Ainsi, les données relatives au trafic des dernières 48 heures sont remises à jour toutes les deux heures et celles relatives à la dernière semaine, toutes les six heures.

Enfin, une fois l'outil de présentation terminé et soumis à l'approbation des responsables, ceux-ci ont émis une simple critique : le nombre de lignes dans l'affichage, par port ou par AS, des données chiffrées étant trop important, il serait souhaitable de pouvoir personnaliser cet affichage. Des filtres ont été ajoutés afin de permettre à l'utilisateur de demander l'affichage des ports ou des AS générant plus de X % du trafic.

3.6.4 Exemples de résultats

Une démonstration complète des résultats est effectuée dans les annexes. Nous ne présenterons ici que quelques exemples d'écran pour offrir une vue concrète des renseignements que l'outil peut fournir.

La figure 3.9 montre la page d'accueil de l'outil baptisé SkyITM (Skynet International Trafic Monitoring). Elle donne les statuts des caches ainsi que les liens vers les différents types de graphiques disponibles. Elle donne aussi accès à la page de management des routeurs et aux fichiers nécessaires pour les machines de tests, à savoir :

- le top 100 des destinations qui envoient du trafic à Skynet ;
- le top 100 des destinations qui envoient du trafic HTTP ;
- le top 100 des destinations qui envoient du trafic FTP.

Ce dernier est une demande spécifique de Skynet et montre que l'outil permet de demander le top 100 de n'importe quel type de trafic.

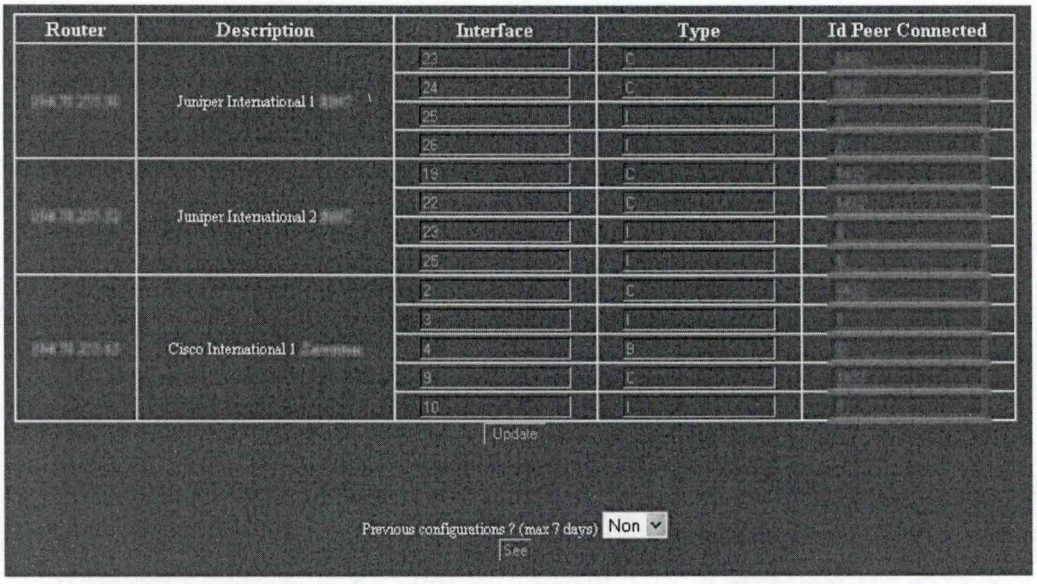

Fig. 3.8: Page de contrôle des interfaces des routeurs

Les figures 3.10 à 3.12 fournissent un exemple du trafic par AS en mode numérique. La ligne *total monitored* indique le pourcentage du trafic que représentent les données affichées.

La figure 3.13 présente un exemple du trafic entrant et sortant par peer sur une période de six heures. Ce graphique a pour intérêt de montrer exactement le taux d'occupation des lignes de chacun des fournisseurs, afin de permettre de renégocier certains contrats, de changer des règles de routage pour la répartition du trafic sur ces liens ou, encore, de mettre en évidence un déséquilibre qui pourrait ne pas avoir été perçu par les autres outils de contrôle.

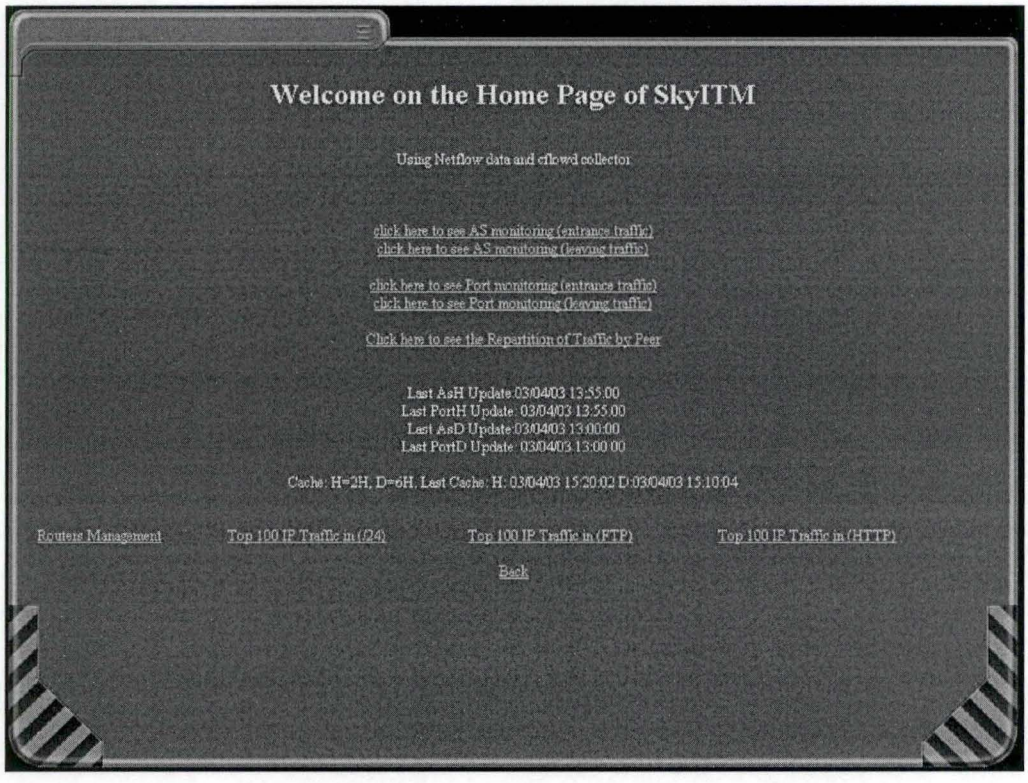

Fig. 3.9: Page principale du site Intranet de contrôle de trafic

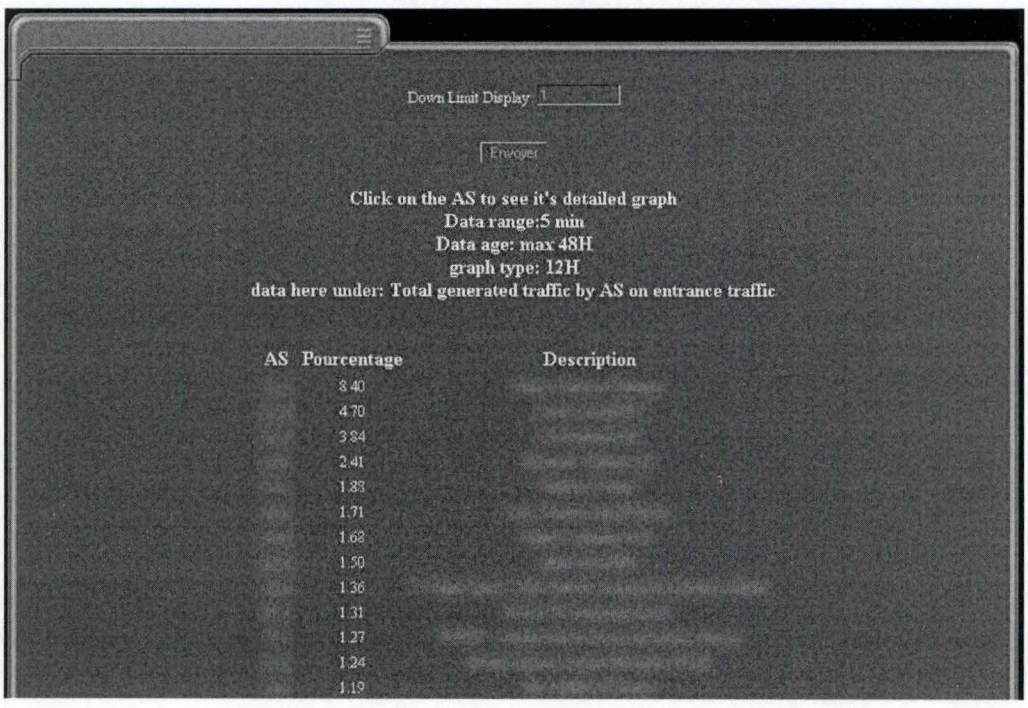

Fig. 3.10: Vue de la distribution du trafic entrant par AS (première partie)

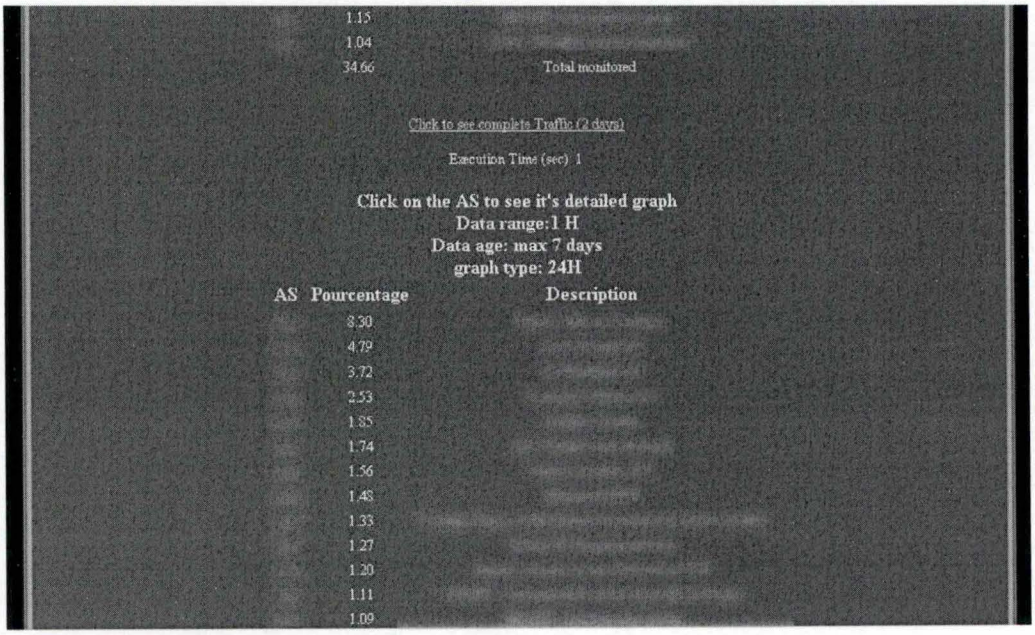

Fig. 3.11: Vue de la distribution du trafic entrant par AS (deuxième partie)

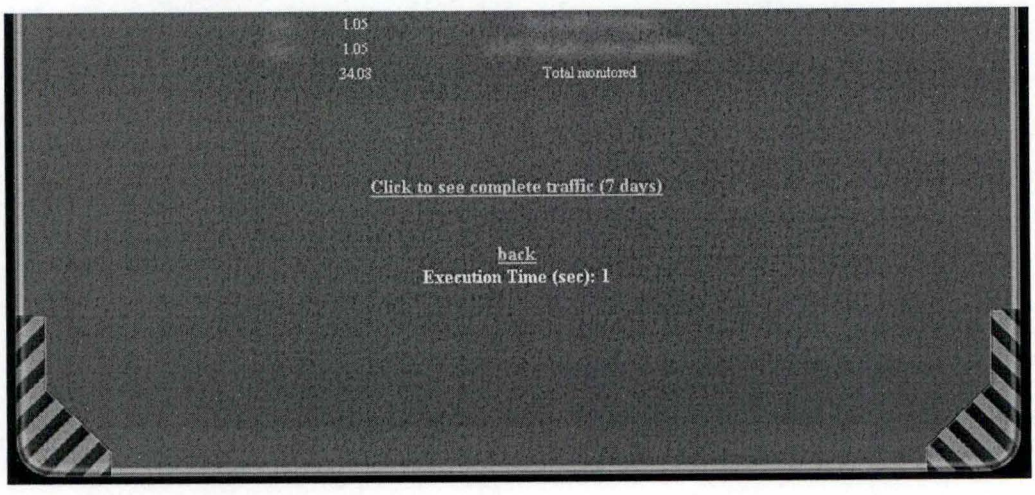

Fig. 3.12: Vue de la distribution du trafic entrant par AS (troisième partie)

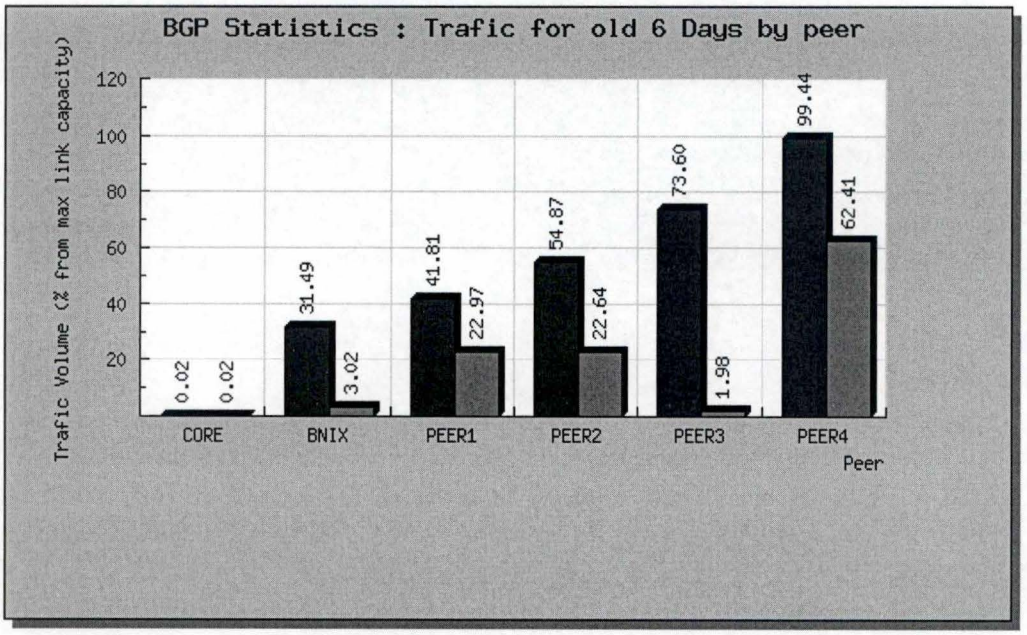

Fig. 3.13: Vue de la quantité de trafic entrant (gauche) et sortant (droite), par peer, en Mb/s (6 jours)

4. SOLUTION THÉORIQUE

4.1 Remarques préliminaires

Ce chapitre propose une solution théorique pour résoudre le problème du choix d'un ISP concernant l'établissement d'un nouveau lien en vue d'échanger du trafic. Cette solution, basée sur l'ensemble de l'expérience que nous avons acquise avant et pendant le stage, n'est pas parfaite. C'est plutôt une base de travail validée, permettant pas la recherche d'un développement plus efficace ou plus précis.

Notre solution repose sur un procédé en plusieurs étapes. Tout d'abord, il faut définir une qualité BGP afin d'établir des critères de comparaison entre diverses routes et/ou diverses tables BGP. Ensuite, il faut définir le type de l'ISP pour lequel la solution va résoudre le problème. Ce choix est important car il conditionne l'ensemble des règles à appliquer au niveau de la capture du trafic. L'étape suivante est la définition des critères de sélection des fournisseurs. La quatrième étape est l'application de l'algorithme de comparaison des fournisseurs, qui donnera une série de résultats pour chacun d'eux. L'étape finale consiste enfin à établir un classement des fournisseurs en y intégrant à la fois les données calculées par l'étape précédente et d'autres données, qui ne sont pas calculables ou ne représentent pas une information assez importante pour être prises comme critère de comparaison, mais bien comme aide à la décision.

4.2 Qualité BGP, qu'entendons nous par là ?

Le protocole BGP est utilisé pour échanger des routes, rien de plus. L'algorithme de sélection de la meilleure route effectue son travail de manière automatique en fonction des attributs des routes et des attributs définis dans les filtres. De ce fait, la table BGP produite est toujours la meilleure possible en fonction des attributs définis. Nous ne pouvons donc pas définir une qualité BGP sur une table BGP seule. Nous allons établir la qualité BGP d'un AS en comparant les tables créées par la réception des annonces de différents AS dans la table déjà existante (Skynet). En effet, puisque tout est automatique (sauf la configuration), si l'on intègre toutes les nouvelles annonces en même temps, les meilleures routes sont automatiquement sélectionnées et aucune comparaison de qualité entre les différentes tables reçues n'est possible.

En théorie, il est impossible pour un ISP d'influencer de manière sûre les processus de décision de tous les routeurs par lesquels vont passer les données à destination de cet ISP.

Après plusieurs tests et observations sur le trafic de Skynet, nous avons considéré que :

1. 1. si l'on sélectionne une des routes ayant l'AS-PATH le plus court [1], donc une proximité d'AS minimum, et
2. 2. si l'AS destination respecte les règles BGP standards (pas de politique de routage excluant des routes que l'algorithme de sélection choisirait),

alors, les routeurs de cet AS feront probablement le même choix de meilleure route pour nous joindre que nous pour lui envoyer du trafic. La numérotation des routeurs jouant un rôle, il est possible que les routes ne soient pas les mêmes, mais la longueur de l'AS-PATH devrait être identique et passer par des ISP de qualité équivalente.

En nous basant sur cette règle, nous avons décidé d'analyser et de comparer l'ensemble des routes reçues par les différents ISP afin de tenter de déterminer quelle combinaison d'ISP offrait une table BGP la plus performante possible. Nous avons apporté à cette règle trois restrictions. La première est que la longueur de l'AS-PATH ne peut dépasser trois AS. La deuxième est que la totalité de l'AS-PATH doit se présenter sous la forme exclusive d'AS-SEQUENCE. La troisième est que les réseaux traversés doivent tous proposer une capacité suffisante pour absorber le trafic à destination de leur domaine ou d'un de leurs sous-domaines et inversément.

4.2.1 Limite de trois AS dans l'AS-PATH

Attention à ne pas considérer cette limite comme générique. Cette limite a été calculée sur les connections payantes de Skynet, non sur les connexions gratuites (BNIX par exemple). La limite devrait être recalculée dans le cadre du BNIX mais n'a pas grand intérêt dans le cadre de cette réflexion et cela pour deux raisons. Tout d'abord, toute connection BNIX étant gratuite, elle est d'office considérée comme bonne. Ensuite, il va de soit que l'intérêt d'accepter des connexions au BNIX est de pouvoir avoir une connexion plus directe vers un réseau que via une connexion payante. Le but étant d'avoir un maximum de liens au BNIX et de garder les liens payants pour atteindre les réseaux non présents au BNIX (ou tout autre point d'échange gratuit).

Pour considérer que le chemin suivi à l'aller sera sûrement le même au retour (en terme de longueur BGP), nous avons imposé une longueur de l'AS-PATH non supérieure à trois. Cette limite est propre à Skynet et devra être réévaluée pour tout autre ISP. Il existe deux raisons à cette limite. D'abord parce que pour Skynet, au delà de trois AS différents, la probabilité que certains AS, pour des raisons économiques, appliquent des filtres sur les routes reçues devient trop importante. Ensuite, parce que les ISP situés à plus de trois AS de Skynet peuvent être considérés comme des ISP de petite capacité et, donc, drainant une faible part de trafic. Si on analyse les tables de routage BGP de Skynet, on constate qu'un saut BGP dirige vers un fournisseur international qui garantit une capacité suffisante ; deux sauts dirigent, dans la plupart des cas, vers un autre fournisseur international ou un fournisseur de taille suffisante (équivalente à Skynet), qui n'a donc pas de problème pour drainer tout son trafic. Trois sauts amènent, au mieux, à un fournisseur international ou de la taille de Skynet et, dans le pire

[1] Plusieurs routes peuvent avoir un AS-PATH de même longueur, mais être différentes par leur contenu

des cas, à un client d'un fournisseur comme Skynet. Forts de l'expérience de Skynet avec ses clients AS, nous estimons que ceux-ci ne sont pas la cible de plus de trafic qu'ils ne peuvent en absorber.

De plus, les contrats liant les ISP comme Skynet avec leurs fournisseurs comprennent souvent des SLA, qui spécifient le délai maximum entre l'entrée et la sortie d'un paquet sur leur réseau. La limite de trois AS dans l'AS-PATH garantit qu'un contrat de même type existe entre au moins deux des trois AS en question. Le seul point qui reste non garanti est la qualité des liens entre Tier-1, mais on peut espérer que ces liens soient suffisants pour drainer tout le trafic des ISP comme Skynet.

Dès que le contexte BGP change (changement de niveau de Tier, d'ISP,...), il faut bien sûr réestimer cette valeur du nombre d'AS maximum pour la fiabilité de l'analyse BGP. En effet, si l'ISP source, celui qui souhaite établir la comparaison BGP, est déjà client d'un ou plusieurs ISP non Tier-1, il ne contrôle déjà pas la manière dont ces ISP envoient son trafic ni le chemin exact qu'utilisent les données pour revenir. Même en contrôlant ses propres annonces, il ne peut obliger ses fournisseurs à lui révéler par quels fournisseurs passe son trafic, ni prévoir comment vont réagir les Tier-1 face à ses annonces, puisque celles-ci peuvent elles-mêmes être modifiées par ses fournisseurs. Tout ceci rend donc très complexe le choix du nombre d'AS maximum d'une route, car plus cette route est longue, plus la probabilité de modification d'annonces ou de choix de routage économique est grande. Toute modification unilatérale d'une annonce rendrait l'analyse BGP totalement nulle car une des règles permettant cette analyse est le fait que tous les acteurs respectent les règles de base de BGP et ne modifient pas les routes.

4.2.2 *Problèmes liés à l'utilisation du type AS-SET dans l'annonce de l'AS-PATH*

Si l'on reprend l'algorithme d'agrégation des AS-PATH indiqué dans la RFC la plus récente parlant de BGP [Y. 95b], le traitement d'AS-PATH identiques ne pose pas de problème alors que le traitement d'AS-PATH comportant des numéros d'AS différents peut se faire de plusieurs manières. Reprenons celles-ci en résumé :

- Si deux AS ne se suivent pas directement dans les deux AS-PATH, les AS compris entre ces deux AS sont annoncés sous forme d'un AS-SET qui, dans l'AS-PATH résultant de l'agrégation, est placé entre les deux AS communs ;
- Si deux AS se suivent directement dans un AS-PATH et pas dans l'autre, les AS qui se trouvent entre ces deux AS sont annoncés sous forme d'un AS-SET, qui, dans l'AS-PATH agrégé, est placé entre les deux AS.

Dans l'AS-PATH agrégé, si plusieurs occurences d'un même AS apparaissent, on supprimera toutes les occurences sauf celle qui se trouve le plus à droite.

On voit donc apparaître trois problèmes. Le premier est la longueur de l'AS-PATH agrégé, qui peut ne plus correspondre à une longueur réelle. La règle de calcul de la longueur d'un AS-PATH pour le protocole BGP dit qu'un AS-SET doit être comptabilisé pour une unité. Or, la règle d'agrégation permet d'agréger plusieurs AS consécutifs dans un seul AS-SET, ou

bien d'ajouter dans l'AS-PATH un AS-SET contenant des AS qui n'existent que dans un des deux AS-PATH agrégés. Dans les deux cas, la règle de calcul de la longueur de l'AS-PATH rend un résultat incorrect par rapport aux AS-PATH originaux.

Puisque l'AS-PATH agrégé peut contenir des AS qui n'existent que dans un seul des AS-PATH originaux ou bien supprimer des occurences d'AS qui sont apparues à cause de l'agrégation, le chemin indiqué dans l'AS-PATH agrégé peut ne pas correspondre à un chemin réel. Cela constitue un deuxième problème.

Le troisième inconvénient est que l'on ne puisse pas reconstituer les AS-PATH originaux ni les préfixes qui ont été agrégés.

Un AS-PATH qui comporte au moins un AS-SET peut donc conduire à une interprétation erronée. L'ensemble de ces trois problèmes et le fait qu'il existe peu d'AS-PATH contenant des AS-SET dans les tables de routage nous ont poussé à ignorer tout préfixe annoncé avec un AS-PATH contenant un AS-SET.

Il peut arriver que cette règle pénalise l'une ou l'autre route, car certains ISP n'hésitent pas à pratiquer une telle agrégation pour économiser des annonces BGP. Cependant, vu les capacités actuelles des routeurs, cette économie n'a plus vraiment d'utilité. D'ailleurs, les quelques AS-SET que nous avons rencontrés provenaient uniquement d'AS en fin d'AS-PATH et, souvent, pour des AS-PATH d'une longueur supérieure à cinq. Le fait de perdre ses routes n'influencera que très peu (moins de 1% du trafic) les résultats du simulateur.

4.2.3 Capacité des fournisseurs

Si, pour envoyer 20 kb/s de trafic vers un réseau, il faut choisir entre un chemin direct qui propose 2 kb/s et un autre chemin, plus long, qui passe par trois liens à 40 kb/s, il est évident que le second choix reste le meilleur, même si au niveau BGP le premier paraîtrait supérieur. Le travail de sélection du meilleur choix de peering ne tient pas compte des performances des connexions. Ce paramètre, tout aussi vital qu'une bonne table de routage, ne peut être jugé qu'extérieurement aux données BGP et doit être l'objet d'une attention particulière.

4.3 ISP type

Les infrastructures des ISP variant énormément en fonction de la demande de leurs clients, des services offerts et de la couverture géographique, nous avons restreint la portée de cette réflexion en fixant un ISP type pour le développement de cette solution. La figure 4.1 reproduit le schéma de notre ISP type résumé à son minimum. BR1 et BR2 représentent des Border Routers et ISP1 et ISP2 les fournisseurs actuels de notre ISP. Les liens tracés entre les BR et les ISP peuvent être multiples.

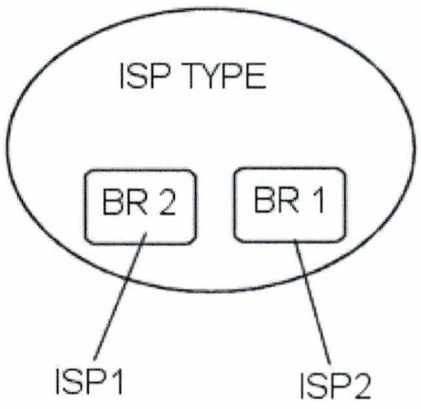

Fig. 4.1: Schéma d'un ISP type

4.3.1 Type de connectivité

Notre ISP type est un ISP n'offrant pas ou peu de trafic de transit (ISP Stub). Il est la source et/ou la destination de tout son trafic. De plus, il est le seul à contrôler totalement ses tables de routage car ses clients, s'ils génèrent du transit, ne le font que de manière limitée sans chercher à influencer les tables de routages de notre ISP en utilisant les fonctionnalités BGP (voir chapitre BGP). Notre ISP type propose à ses clients un service de connexion à large bande (type ADSL ou cable), service que recherche aujourd'hui la majorité des utilisateurs et qui est proposé par la majorité des ISP.

Connaître les types de connectivité proposés par l'ISP est une donnée importante. Ils ont en effet des caractéristiques différentes. L'ADSL et le cable, les plus utilisés aujourd'hui auprès du grand public, offrent une connectivité asymétrique, tandis que les autres types, comme le SDSL ou les lignes louées, offrent des connectivités synchrones et donc symétriques. L'ADSL étant la connectivité qui génère le plus de trafic chez Skynet, tout le trafic Skynet est vu comme asymétrique : le trafic entrant est beaucoup plus important que le trafic sortant. Cela veut dire que Skynet reçoit plus de trafic que ce qu'il envoie, parce que le trafic entrant est généré principalement par les demandes des utilisateurs de Skynet plutôt que par des demandes provenant de l'extérieur, qui généreraient du trafic sortant.

4.3.2 Types de services offerts

Outre l'absence de transit, notre ISP type n'offre pas de service de garantie de qualité (pour faire du Voice Over IP ou autre) par l'intermédiaire de l'activation de services QOS sur ses routeurs. Il assurera plutôt que la bande passante disponible soit toujours sufisante. Cette option simplifie le problème car on ne doit pas chercher un fournisseur qui offre les garanties QOS souhaitées, mais uniquement de la bande passante.

Alors qu'un ISP qui utilise de la QOS va chercher à optimiser son réseau pour maintenir ses

contrats de qualité sans chercher à augmenter sa bande passante, un ISP qui ne se préoccupe pas de QOS va plus simplement augmenter sa bande passante, de manière à garantir une capacité suffisante, et veiller à ce que les routeurs de son réseau soient capables de traiter tous les paquets sans pertes. En cas de pertes, il sera temps de voir si l'on doit changer la configuration des routeurs, mettre à jour ceux-ci et/ou acquérir des routeurs plus performants.

En excluant toute gestion de QOS, nous simplifions le problème non seulement au niveau de l'analyse du trafic interne, mais aussi au niveau de la négociation des services que doit offrir un fournisseur candidat.

4.3.3 Propriétés géographiques

Certains ISP qui couvrent une très large zone géographique peuvent essayer de répartir la charge de trafic en utilisant les propriétés de l'attribut MED (voir chapitre 1 : BGP), qui permet de router le trafic en fonction de choix géographiques si l'on possède avec le fournisseur plusieurs liens situés à différents endroits. Afin de simplifier le calcul lors du choix du fournisseur, nous considérons notre ISP type comme un ISP dont tous les points de connexion sont centralisés en un même lieu. Ceci simplifie le processus de choix car toute route annoncée à notre ISP, quel que soit son attribut MED, sera traitée sans tenir aucun compte de cet attribut.

4.4 Détermination des critères de présélection d'un ISP

La difficulté la plus importante lors du choix d'un fournisseur réside surtout dans la détermination des critères de choix de cet ISP. Faut-il plutôt choisir l'ISP qui offre le meilleur prix, ou, sans tenir compte de l'aspect budgétaire, celui dont le réseau est le plus performant ? Dans le deuxième cas, comment déterminer la performance d'un réseau ? En se basant uniquement sur son infrastructure ?

A nos yeux, la meilleure solution est plus complexe. Pour des raisons évidentes, nous pouvons éliminer le critère économique pour promouvoir la voie de la performance, mais il n'est pas aussi aisé de démontrer la performance d'un réseau pour les besoins de notre ISP type. En effet, alors que la performance intrinsèque d'un réseau est liée à son infrastructure et sa configuration, le fait de devoir obtenir une performance qui soit la meilleure en fonction de nos besoins change complètement la donne. Le réseau le mieux dimensionné, le plus rapide et couvrant un maximum d'adresses IP n'est pas forcément celui qui convient, pour les raisons suivantes :

- La source et l'origine du trafic généré par notre ISP peuvent ne pas se situer dans les IP couvertes directement par ce réseau ;
- La distance qui nous sépare de ce réseau peut pénaliser celui-ci (ex : temps minimum moyen de transmission vers les USA : 200 ms) ;
- La stabilité BGP du réseau peut être trop faible et entraîner des perturbations dans le maintien des tables de routage de notre ISP ;

- Le lien établi entre notre ISP et le fournisseur peut être d'une capacité trop faible, due au coût d'installation de ce lien.

Prenons l'exemple d'un ISP belge qui envoie du trafic en France et qui a le choix entre un fournisseur européen et un fournisseur américain. Une comparaison établie sur la base des quatre points cités ci-dessus met en évidence des différences entre les deux fournisseurs :

- L'européen, sachant qu'actuellement la majeure partie du trafic généré par un ISP belge offrant de l'ADSL est échangé avec la France, couvrira sans doute directement ou avec 1 seul hop les adresses IP impliquées. La distance séparant le point d'entrée belge et le coeur du réseau est certainement de l'ordre de quelques centaines de kilomètres au maximum, la stabilité de la table BGP est probablement identique à celle de l'américain et, enfin, les liens proposés par les fournisseurs européens actuels sont de l'ordre du Gigabit/s. Ils ont une infrastructure interne en plein développement, mais encore fort faible en terme de bande passante : de l'ordre de quelques Gigabits/s (moins de dix).
- L'américain, lui, pourrait couvrir une partie de nos besoin en IP (ils ont obtenu des adresses européennes par le biais des rachats et fusions d'ISP), mais il se trouve majoritairement à au moins un saut de la destination, voire plus. La majorité des ISP américains ont plusieurs point de présence en Europe qui, en utilisant le *MED* (voir p.10), permettent l'échange de trafic entre ces points sans devoir revenir au coeur du réseau (aux USA). Malgré cela, ces points de présences ne sont pas aussi nombreux que ceux des opérateurs européens et, à moins de se trouver près d'un de ces points, le prix de l'installation d'un lien coûte trop très cher. La stabilité est certainement la même que l'ISP européen. Enfin, le réseau global des ISP américains est actuellement architecturé autour de liens 10 Gb/s au minimum, la tendance allant vers des infrastructures de l'ordre des 40 Gb/s en simple ou double réseau.

Avant même de prendre en compte les données BGP, une simple lecture des données de trafic et des capacités des fournisseurs donne donc un aperçu des ISP qui peuvent déjà être éliminés, même s'ils venaient à passer les tests BGP haut la main : actuellement, les opérateurs américains restent très présents sur le marché européen car offrant une structure rapide et stable. On espère cependant que les ISP européens tels TISCALI pourront bientôt concurrencer les américains en proposant plus de points de présences et un tarif moins important du fait de la localisation de l'ISP totallement en Europe.

4.5 *Détermination d'un algorithme de comparaison*

Pour comparer les ISP candidats, nous disposons d'une série de données qui ont un caractère certain, c'est-à-dire dont la valeur ne peut être mise en doute par une erreur de mesure ou de calcul, et des données incertaines. En outre, il faut définir, pour chaque type de données, un poids ou une métrique pour les comparer.

4.5.1 Données certaines

Les tables de routage de notre ISP type ainsi que celles de chacun des candidats sont considérées comme certaines car elles ne sont pas mesurées, mais récoltées auprès des routeurs. Ce sont les seules données certaines que nous possédons. Ce sont principalement, pour chaque préfixe, sa longueur ainsi que la longueur de l'AS-PATH. Ces données seront à la base du mécanisme de sélection du meilleur ISP candidat, mais ne représentent pas à elles seules des données significatives.

4.5.2 Données incertaines

Les données incertaines, sont les données que nous récoltons par mesures : les données de trafic et les mesures de délai.

Données de trafic

Les données de trafic sont peu soumises à des erreurs de mesures, car ces erreurs ne sont introduites que par l'échantillonnage effectué par les routeurs. Actuellement, pour la prise d'échantillons, les routeurs ne respectent pas un algorithme implémentant une distribution de Poisson, mais utilisent un algorithme basé sur un simple comptage des paquets. La perte de précision induite par cet algorithme peut être considérée comme négligeable, étant donné le taux d'échantillonnage appliqué et la vitesse des liens surveillés (voir p.26). C'est pourquoi les données de trafic serviront comme deuxième argument lors de la sélection de l'ISP candidat.

Mesures de délai

Les mesures de délai sont les données les moins certaines, car même en respectant la prise de mesure suivant une distribution de Poisson afin de garder un bon niveau de représentativité, ces données sont soumises à la charge des réseaux, aux pertes éventuelles de paquets, à l'arrêt imprévu d'une des machines de mesure. Elles doivent donc faire l'objet d'une attention particulière si l'on ne veut pas risquer leur invalidation.

La mesure de délai a pour but de montrer, chiffres à l'appui, la stabilité du réseau candidat (variation du délai) et son intérêt pour nous (nombre de préfixes atteints). Pour cela, nous proposons la méthode de prise de mesure suivante :

1. Définir le top 100 des préfixes HTTP desquels notre ISP type reçoit le plus de trafic. Il est nécessaire de prendre le top 100 HTTP pour avoir des machines que l'on puisse atteindre de manière quasi certaine. Il serait en effet très difficile de mesurer un délai sur une machine hébergeant un service autre que le HTTP ou permettant de renvoyer les requêtes ICMP. Même si le top 100 HTTP ne représente pas, en terme de volume, une quantité importante de trafic, il reste un des meilleurs choix, puisque son port de communication est stable et connu.

2. Définir les facteurs de l'algorithme de prise de mesure suivant une distribution de Poisson (nous recommandons d'étaler les mesures sur une heure, afin de ne pas surcharger le réseau candidat et ne pas paraître suspect aux yeux d'éventuels pare-feux), comme indiqué dans le RFC2330 [V. 98].
3. Etablir une moyenne des mesures en donnant plusieurs valeurs statistiques, telles que la variance et la moyenne, qui permettent de voir la stabilité des mesures d'un simple coup d'oeil.
4. Ne garder, dans les mesures prises en compte, que les mesures pour lesquelles toutes les machines ont des résultats. On placera une machine par candidat. Afin d'obtenir des données toujours comparables, si une machine ne renvoie pas de données, on annulera toutes les mesures pour cette période.

Le poids accordé à ces mesures est plus faible que le poids de la comparaison des routes, mais il peut faire la différence entre deux ISP candidats (qui auraient accepté les tests de mesure de délai) qui seraient proches lors de la comparaison de routes.

4.5.3 Méthode de comparaison

A partir de ces trois informations (tables de routage, mesures de trafic et mesures de délai), il est possible de proposer une méthode permettant de comparer les ISP. Il convient d'utiliser cette méthode quand on possède plusieurs jours de mesure de trafic, car la comparaison sera d'autant plus affinée que la quantité de trafic sera grande, mais il sera nécessaire de remettre de temps en temps les compteurs à zéro afin de pouvoir observer les modifications du comportement des internautes et, donc, du trafic. Les contrats de peering étant généralement renégociés tous les six mois, il semble raisonnable de synchroniser les deux phénomènes en utilisant la même période pour remettre les compteurs à zéro.

Cette méthode permet de comparer n'importe quelle combinaison d'ISP, qu'elle comporte ou non notre ISP. Toutefois, le but étant de voir avec quel ISP nous augmentons le mieux nos performances, il va de soi que notre ISP fera partie de chaque sélection, afin de pouvoir comparer les tables BGP que nous possédons déjà avec de nouvelles données. La méthode de comparaison se déroule comme suit :

1. Récupérer les tables de routage des candidats et celles de l'ISP type ;
2. Sélectionner les ISP à comparer ;
3. Construire la table de routage, qui résulte des tables de routages comparées, en ne retenant que l'AS-PATH comme critère de sélection. La table produite ne contiendra qu'une seule fois un préfixe ; toutefois, si un même préfixe est annoncé par plusieurs ISP avec la même longueur d'AS-PATH, la table contiendra cette information afin de pouvoir comparer complètement les ISP en une seule fois ;
4. Simuler, à travers cette nouvelle table de routage, le passage du trafic récolté ;
5. Proposer les résultats sur des graphiques. Ceux-ci doivent montrer les évolutions apportées au pourcentage de trafic qui passe par X AS, ce qui, selon Skynet, est l'élément le plus intéressant ;

6. Ajouter au rapport les valeurs de délai obtenues pour chacun des AS, sous forme d'un tableau reprenant les valeurs définies dans la base de données.

4.6 Proposition de classement des ISP en fonction de la comparaison

4.6.1 Valeur d'un ISP

Dire qu'un ISP est l'ISP idéal est impossible, car la valeur d'un ISP n'a pas de sens en temps que telle. Il faut pouvoir faire entrer en ligne de compte d'autres ISP et mettre chacun d'eux en concurrence avec les autres.

On pourrait essayer de donner une valeur intrinsèque à un ISP, mais cette valeur ne serait pas significative pour toute autre personne que celle qui l'a établie, car les critères utilisés pour établir cette valeur sont souvent subjectifs et sujets à controverse.

4.6.2 Méthode de Classement

La méthode de comparaison proposée ci-dessus produit une série de résultats, qui peuvent ensuite être utilisés pour établir un classement des ISP candidats.

La méthode de classement des ISP tient compte de toutes les informations produites lors de la comparaison. Le meilleur ISP sera celui qui nous permettra d'obtenir la plus grande quantité de trafic le plus proche de nous (c'est-à-dire qui traverse le moins d'AS pour arriver à destination), en tenant compte des valeurs avec prepending, et qui possédera la moyenne de délai la plus faible ainsi que la variance la meilleure.

On peut aussi proposer une formule plus mathématique pour donner le poids d'un ISP par rapport aux autres, en utilisant la formule suivante :

Soit les préfixes (Pj), j étant le nombre de préfixes générant du trafic,

$$\sum_{0<j<n}^{j} (prefP_j.avgP_j.asPath_{P_j}.traf_{P_j})$$

où :

- pref = la quantité de trafic mesurée pour le préfixe en cours ;
- avg = le pourcentage moyen de ce trafic par rapport au trafic total ;
- asPath = la longueur du plus long AS-PATH possible pour l'ensemble des préfixes + 1 - la longueur de l'AS-PATH du préfixe sélectionné ;
- traf = la quantité de trafic (en %) qui passe par ce préfixe lors de la simulation [2].

[2] En effet, on pourrait obtenir qu'un préfixe se voit **voler** du trafic par un préfixe plus précis acquis lors de l'intégration d'une nouvelle table de routage et ceci, pour respecter l'algorithme de décision

La multiplication de la quantité de trafic par le pourcentage qu'il représente permet d'établir une relation de force entre les routes les plus utilisées et les routes les moins utilisées. La présence de la variable asPath sert à avantager les routes les plus courtes. Nous multiplions le tout par le trafic qui passe effectivement par cette route lors de la simulation, pour permettre aux routes les plus fréquentées de peser davantage dans la balance.
On pourrait ajouter un facteur relatif à la valeur de délai mesurée, mais l'intégrer directement dans la formule serait commettre une erreur, pour deux raisons. Tout d'abord parce qu'on ne peut pas savoir, lorsque l'on établit une mesure de délai, si la machine ciblée est en bordure du réseau ou en son plein milieu. Ensuite, parce qu'on ne peut pas non plus, si une mesure montrait un délai plus important que prévu, connaître l'origine exacte du problème, puisque l'on ne maîtrise pas le chemin que prend une requête ICMP ou un paquet IP. Si ces deux points étaient fixés, on pourrait ajouter directement le facteur de délai comme terme, ce qui permettrait assurément de classifier les routes de manière plus raffinée.

Le calcul doit être répété pour chaque fournisseur, donc en faisant varier j. Le but de ce calcul est de donner une valeur à la table BGP d'un fournisseur en fonction du trafic mesuré par préfixe et en tenant compte de la longueur de l'AS-PATH.

La figure 4.2 nous montre un exemple de calcul de comparaison de tables.

4.7 Autre utilisation de la solution

Cette solution pourrait être utilisée pour établir un premier lien pour un ISP, mais cela fonctionnerait différemment puisque, par définition, un ISP qui débute n'a pas encore de données suffisantes pour déterminer le type exact de son trafic et pour le simuler. Il ne peut utiliser la formule de comparaison définie précédemment, ce qui reviendrait au même résultat que s'il laissait les routeurs faire le travail. Ce procédé peut donc être appliqué dans le cas d'un premier lien, mais les résultats devront être réévalués par la suite, quand l'ISP aura d'avantage d'informations sur son trafic réel.

Exemple :

Une trace indique 1 Mbit de trafic pour l'IP (en /24) 25.30.0.0 et 2 Mbits pour l'IP 32.86.0.0. On simule le passage de ce trafic via une table composée notamment des annonces qui seraient celles sélectionnées par un routeur (pour les besoins de comparaison, si une route est annoncée plusieurs fois, nous gardons toutes les annonces possibles) :

Network	Next Hop	Metric	Weight	Path
25.30.0.0/16	200.41.12.15	-	0	5152 5214 5378
25.30.0.0/16	80.66.129.77	-	0	1239 3561 5378
32.86.0.0/16	80.66.129.77	-	0	1239 7018
32.86.110.0/24	200.41.12.15	-	0	5152 1516 7018

Les annonces proviennent de deux tables qui contiennent respectivement :

Network	Next Hop	Metric	Weight	Path
Fournisseur 1				
25.30.0.0/16	80.66.129.77	-	0	1239 3561 5378
32.86.0.0/16	80.66.129.77	-	0	1239 7018
Fournisseur 2				
25.30.0.0/16	200.41.12.15	-	0	5152 5214 5378
32.86.110.0/24	200.41.12.15	-	0	5152 1516 7018

Si l'on estime que le simulateur fait passer 100% du trafic par ces deux préfixes, on obtient les valeurs suivantes par fournisseur :
- pref : 1 000 000, avg 0.33, asPath = 4-3 = 1, traf = 1 pour un résultat de 330 000
- pref : 2 000 000, avg 0.66, asPath = 4-2 = 2, traf = 0.30 pour un résultat de 792 000

ce qui donnerait une cote de 1 122 000 pour le fournisseur 1.

Si l'on estime que le simulateur fait passer 100% du trafic par ces deux préfixes, on obtient les valeurs suivantes par fournisseur :
- pref : 1 000 000, avg 0.33, asPath = 4-3 = 1, traf = 1 pour un résultat de 330 000
- pref : 2 000 000, avg 0.66, asPath = 4-3 = 1, traf = 0.70 pour un résultat de 924 000

ce qui donnerait une cote de 1 254 000 pour le fournisseur 2.

Le résultat montre que malgré une longueur d'AS-PATH plus petite, le premier fournisseur obtient un score plus petit. Cet exemple reflète bien le fait que, si l'on place ces deux tables dans un même routeur, la table du deuxième fournisseur draînera plus de trafic que celle du premier. Il faut bien faire attention ici que ces résultats ne sont à prendre en compte qu'en comparaison de deux ou plusieurs tables et non comme résultat de qualité pour **une seule** table.

Fig. 4.2: Exemple d'application de la formule de comparaison

5. L'OUTIL DE SÉLECTION D'UN MEILLEUR FOURNISSEUR

Ce chapitre montre l'implémentation chez Skynet de l'outil BGP, sur la base de la théorie du chapitre précédent ainsi que des travaux et études déjà réalisés dans le domaine.

Dans les pages suivantes seront successivement traités :
- les travaux déjà effectués
- la base de données de l'outil ;
- l'outil en tant que tel ;
- un outil permettant d'ajouter des mesures de délai.

5.1 Travaux déjà effectués

5.1.1 Les métriques selon CAIDA

Le travail de CAIDA [Bra02] sur les métriques nous concerne directement. En se basant sur des mesures préalables de RTT, il montre que quatre paramètres peuvent faire évoluer ces mesures :

1. IP-PATH length : le nombre de sauts traversés par un paquet ;
2. Autonomous System (AS) : le nombre d'AS traversés par un paquet ;
3. Geographical Distance : la distance entre la source et la cible de la mesure ;
4. RTT : le temps aller-retour d'un paquet.

Seules les conclusions concernant l'analyse de la longueur de l'AS-PATH sont intéressantes pour nous. La valeur de la longueur de l'IP-PATH n'est pas utilisable, car la méthode développée n'utilise que les données BGP. Or, ces dernières ne permettent pas de connaître directement le nombre de sauts IP d'une route, mais uniquement la quantité d'AS traversés. Pour connaître ce nombre, il faut effectuer des analyses supplémentaires, notamment des "traceroute", et utiliser d'autres méthodes permettant de déterminer le chemin IP d'une route.

Les deux conclusions principales du travail de CAIDA sont la relative instabilité de l'AS-PATH par rapport à l'IP-PATH et la variabilité de la longueur moyenne de cet AS-PATH. La différence de variation entre les deux PATH tendrait à prouver que le nombre d'AS a augmenté pour joindre une destination, mais pas le nombre de sauts IP. La longueur moyenne de l'AS-PATH est passée quant à elle de 4.1 (+/- 1.3) à 4.5 (+/- 1.3), ce qui apporte une preuve supplémentaire de l'apparition de nouveaux AS.

Il faut pourtant garder sur ces résultats un oeil critique. En effet, aucun détail, aucune des tables de routage analysées n'est donnée. On ne peut donc pas savoir, par exemple, si la longueur de l'AS-PATH comprend ou non l'AS à partir duquel les mesures sont faites.

Ce travail montre aussi que l'AS-PATH n'est pas toujours un indicateur de qualité pour un chemin. Cependant, puisque nous ne possédons que ce renseignement-là, nous prendrons les données de l'AS-PATH, éventuellement combinées aux mesures de délai, comme données suffisantes pour la qualité d'une route.

Le groupe CAIDA n'ayant pas eu accès à toutes les tables BGP, il n'a pas fondé ses analyses sur ces tables, mais a recomposé l'AS-PATH à partir de l'IP-PATH des traces récoltées. Il a bien sûr comparé cette méthode avec au moins une table de routage et a pu ainsi conclure que 90% des routes reconstituées étaient identiques à la route correspondante dans la table de routage. Le fait que 10% ne correspondent pas ne posait pas un problème, car seulement 1% du trafic empruntait ces routes [And02, And01].

5.1.2 Infonet

Le travail du groupe Infonet [O. 03] reprend l'analyse de Steve Uhlig et essaie d'apporter une solution pour maîtriser le trafic en utilisant BGP. Il établit préalablement une différence entre les ISP qui contiennent de l'information et les ISP qui l'absorbent. Cette distinction est importante dans la mesure où un ISP offrant de l'information génère beaucoup de trafic et essaie avant tout que ce trafic sorte facilement et de manière équilibrée, alors qu'un ISP absorbant ce trafic essaie de contrôler la manière dont le trafic entre dans son réseau. Or, le fonctionnement de BGP permet de gérer facilement la sortie du trafic d'un ISP, mais beaucoup plus difficilement la manière dont le trafic y entre.

Le but de l'outil développé dans ce mémoire n'est en aucune façon de faire de l'ingénierie de trafic, mais de choisir, à partir des tables BGP reçues et du mécanisme standard de sélection de la meilleure route, ainsi que sur la base de divers paramètres mesurés en dehors de notre ISP, la meilleure combinaison de fournisseurs pour drainer le trafic entrant et sortant de notre ISP. Même si un des paramètres les plus importants se base sur le trafic entrant (en volume et par préfixes) pour pondérer certains calculs, cela ne relève pas de l'ingénierie de trafic. Cette ingénierie sera éventuellement effectuée à posteriori pour optimiser les liens et le trafic, mais n'intervient pas dans le processus de décision.

Il est cependant intéressant de garder ce document comme référence pour toute personne qui voudrait, après la sélection de ses fournisseurs, optimiser au mieux son trafic en utilisant BGP.

5.2 La base de données

La partie de la base de données réservée à l'outil BGP est plus importante que la partie de consultation du trafic. Cette différence résulte simplement du fait que la partie dédiée au

trafic ne joue qu'un rôle de stockage pour une consultation ultérieure. L'importance de la partie BGP s'explique par l'ensemble des traitements que l'on doit appliquer aux données et par l'ensemble des tables qui permettent de contrôler ces traitements.

Comme nous l'avons indiqué dans le deuxième chapitre (voir p. 16), la base de données n'a pas été définie lors de l'analyse globale du projet, mais laissée libre pour être développée en même temps que chaque module. La partie qui suit expose le choix du moteur de la base de données et les raisons de notre choix, et donne ensuite une description détaillée de la base, dans l'état où elle se trouve lors de la rédaction de ce mémoire.

5.2.1 Mysql

Mysql, utilisée ici dans sa version 3.5X, est une base de données non transactionnelle et partiellement relationnelle.

Non transactionnelle car elle ne contient aucune méthode d'accès, ni aucune interface de programmation, qui permette de déclarer l'ouverture d'une transaction et de la gérer. La base de données comprend un format de fichier spécial qui permet de garder une certaine cohérence si une requête venait à se terminer de manière anormale ou si la machine hôte s'arrêtait brutalement, mais elle ne possède pas de réel mécanisme de gestion de transaction.

Partiellement relationnelle car, si la base de données respecte la syntaxe standard du langage SQL et gère les contraintes liées aux clefs primaires et à l'unicité de certains champs des tables, elle est toutefois incapable de gérer les déclarations de relation entre les tables que sont par exemple les clefs étrangères, même si la syntaxe est acceptée dans la déclaration des tables.

Le choix s'est porté sur mysql à cause des performances de ce moteur, de sa simplicité d'utilisation et de sa légèreté sur un système. Actuellement, il n'existe aucun autre système de base de données totalement *libre*[1] et capable de travailler aussi rapidement. Mysql est connu et reconnu comme tel par l'ensemble de la communauté spécialisée. Plus de renseignements sont disponibles à des adresses telles que : `http://www.mysql.com/information/benchmarks.html` ou encore `http://www.sloppycode.net/benchmark/`. Bien d'autres documents peuvent être trouvés via les moteurs de recherche habituels.

La base de données ne devant stocker que des informations sans lien entre elles (ou très peu), il n'est pas nécessaire d'utiliser les relations entre données et entre tables. D'autre part, les machines actuelles, leurs performances, la granularité de nos requêtes et la fiabilité de Linux ainsi que la reconnaissance des qualités de Mysql nous suffisent pour ne pas vouloir absolument de version transactionnelle.

[1] en anglais "free", à ne pas confondre avec "free of charges" (gratuit)

5.2.2 Développements BGP

La partie centrale de la partie BGP de la base est la table des annonces reçues ainsi que la table de résultats du simulateur. Cette partie BGP se compose de pas moins d'une vingtaine de tables. La figure 5.1 montre les tables principales servant de support à toute la partie BGP. Un schéma en annexe présente l'ensemble des tables utilisées chez Skynet. Pour permettre de mieux comprendre les liens que nous réalisons entre les tables par nos scripts, le schéma est réprésenté comme un schéma physique d'une base de données transactionnelle.

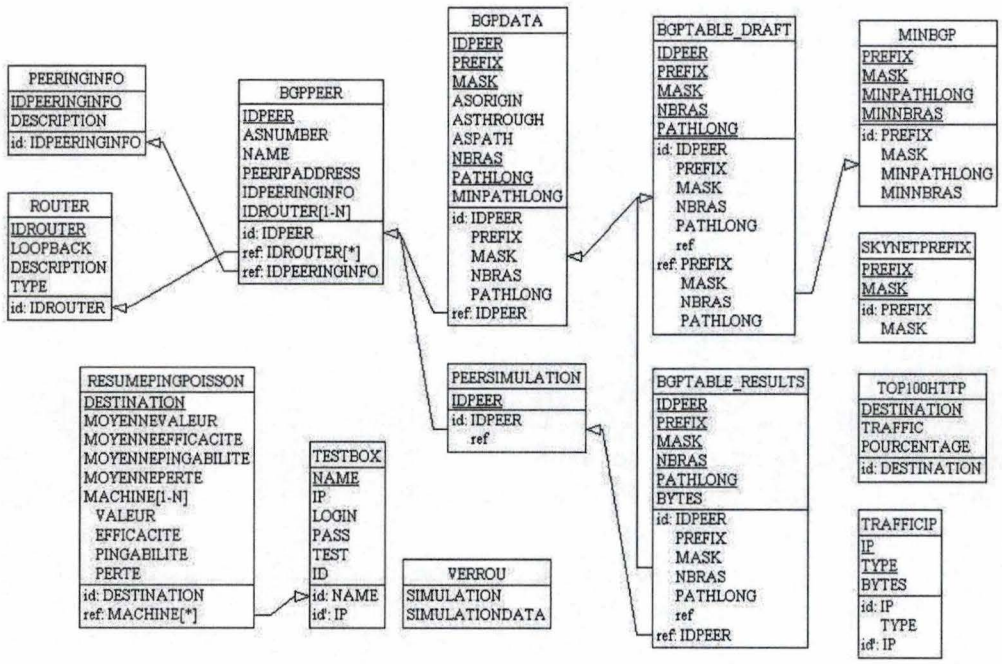

Fig. 5.1: Partie BGP de la base de données, tables principales

BGPPEER

Table contenant la description des fournisseurs avec un identifiant interne. Cette table permet de faire une translation entre le numéro d'AS du fournisseur et son numéro interne à Skynet.

Les champs ASNUMBER et PEERIPADDRESS sont uniques, mais peuvent varier dans le temps, puisqu'un AS peut disparaître ou apparaître.

BGPTABLEDRAFT

Table contenant les importations des tables BGP des candidats. Elle est utilisée par le simulateur.

Les champs PATHLONG et NBRAS représentent les données originelles, avec prepending s'il y en a.

Cette table est la plus importante, car elle contient la liste, par préfixe, de tous les préfixes les plus courts. Elle n'inclut aucune route possédant un AS-SET, mais elle peut, par contre,

contenir plusieurs fois un même préfixe, pour autant que celui-ci soit annoncé par des fournisseurs différents avec une même longueur d'AS-PATH. En effet, cette table est le résultat de la jointure de la table MINBGP avec la table BGPDATA en retenant tous les préfixes ayant des AS-PATH dont la longueur correspond à la longueur minimum des AS-PATH possibles par préfixe. Cette particularité du simulateur est expliquée en détails à la page 59.

PEERSIMULATION

Table contenant les identifiants des fournisseurs sélectionnés pour faire partie d'une simulation.

MINBGP

Table contenant, pour chaque préfixe annoncé et pour chaque masque associé à ce préfixe, la longueur de l'AS-PATH minimum contenu dans la table BGPDATA ainsi que le nombre d'AS correspondant à cet AS-PATH.

Cette table a été créée pour pallier au fait que Mysql ne permet pas d'écrire de requête imbriquée.

BGPTABLERESULT

Table contenant les résultats du simulateur. C'est une table temporaire, remise à jour à chaque fois que le simulateur est utilisé. De ce fait, un système de protection doit être mis en place pour empêcher plusieurs simulateurs de tourner simultanément et assurer qu'un utilisateur qui utilise le simulateur puisse consulter le résultat avant que le simulateur ne soit relancé. Parmi les divers types de protection possibles, nous avons choisi une technique par verrou (voir ci-dessous) car c'est celle qui consomme le moins de ressources.

Cette table contient les routes qui résultent de l'application de l'algorithme du simulateur. Si plusieurs AS annoncent une route dont la longueur correspond à la longueur minimum pour un préfixe, tous les AS correspondants sont retenus dans la table ainsi que les routes correspondantes.

TRAFFICIP

Table contenant, par IP, la quantité de Bytes reçus. Les addresses IP sont regroupées en /24 pour des raisons de place et parce qu'il n'existe pas, dans les tables de routage BGP, d'annonce plus précise que des préfixes /24.

Le champ TYPE peut valoir I ou O (In/Out).

VERROU

Table contenant les variables qui spécifient si un verrou a été placé. Dans un premier temps, cette table contiendra de manière explicite chacun des verrous possibles : on ne pourra pas créer de verrou sans modifier cette table. Ceci oblige à essayer d'utiliser les verrous déjà présents et, surtout, à utiliser des noms de verrou bien définis. Il aurait aussi été possible de définir une table dans laquelle on pouvait créer à volonté des verrous. Dans le contexte qui nous intéresse, le nombre de verrous est très faible et très ciblé. De ce fait, il est préférable de bien définir chacun d'eux plutôt que de permettre d'en créer autant que possible. Les champs sont définis par défaut à 0, indiquant que le verrou n'est pas appliqué. L'autre valeur possible

est 1, signifiant que le verrou est placé.

La règle d'utilisation des verrous est la suivante. Le verrou SIMULATIONDATA doit être placé en même temps que le verrou SIMULATION. Le verrou SIMULATION ne peut être placé que si le verrou SIMULATIONDATA est à 0. Le verrou SIMULATION est relâché quand le simulateur a terminé son exécution et le verrou SIMULATIONDATA est relâché quand les résultats ont été consultés. Le fait d'avoir deux verrous permet d'indiquer si le simulateur est en marche ou si les résultats sont en attente d'être consultés.

RESUMEPINGPOISSON

Table contenant les valeurs brutes des données de délai. Elle est regénérée à chaque récupération de données. Les moyennes sont calculées sur la base des données prises en compte depuis la première mesure de délai correctement relevée pour l'ensemble des machines. Si une machine ne transmet pas de résultats lors d'une récupération, l'ensemble des résultats des machines pour cette récupération n'est pas pris en compte. Si une nouvelle machine est placée, l'ensemble des résultats déjà calculés est stocké et cette table est remise à zéro. Ainsi, nous assurons que les résultats comparatifs sont toujours justes.

Cette table permet de générer un rapport comparatif clair en fonction des destinations, par machine (donc par candidat), avec l'ensemble des données utiles.

La table est représentée sur le graphique 5.1 comme contenant un attribut composé car cet attribut doit être présent autant de fois qu'il y a de machines dans la table TESTBOX. En pratique, cet attribut composé devient une liste d'attributs préfixé par le nom de la machine et suffixée par le nom de la valeur enregistrée.

PEERINGINFO

Table définissant les différents types de peering, Skynet ayant décidé de séparer ses fournisseurs en quatre types : les fournisseurs internationaux, les fournisseurs gratuits, Belgacom et les fournisseurs en test.

ROUTEUR

Table contenant la description des routeurs de Skynet. Les routeurs Skynet sont qualifiés par une location, un type et leur adresse de loopback.

SKYNETPREFIX

Table contenant l'ensemble des préfixes appartenant à Skynet. Cette table permet de s'assurer qu'aucun préfixe présent dans la table TRAFFICIP n'appartient à Skynet. Cette table peut en outre être utilisée en dehors du problème qui nous intéresse, par exemple à chaque fois que l'on veut filtrer les IP appartenant à Skynet.

TOP100HTTP

Table contenant les 100 préfixes HTTP (regroupé en /24) qui envoient à Skynet le plus de données. Cette table est utilisée pour la réalisation des mesures dans l'outil de mesure de délai. Elle est recréée à la demande en consultant la table contenant le trafic reçu par IP.

TESTBOX

Table contenant les identifications des machines testbox utilisées pour récupérer les tables de routage chez les candidats et/ou effectuer les mesures de délai. Cette table apporte non seulement une centralisation de la gestion de ces machines, mais permet, en plus, d'automatiser la récupération des données. Elle doit contenir l'ensemble des informations nécessaires pour se connecter à une des machines de test, y ouvrir une session et connaître les tests en cours.

5.3 Outil d'analyse BGP

5.3.1 Analyse

L'outil Skynet BGP Analysing Tool reprend l'ensemble des composants qui traitent BGP et a pour but, en utilisant un site intranet, d'aider les ingénieurs réseau de Skynet à configurer les routeurs et choisir leurs fournisseurs.

Outre ces deux buts directs de l'outil, il existe d'autres motivations qui ont mené à son développement et qui sont liées à d'autres facteurs :

- etudier les possibilités de load balancing (facteur sécurité) ;
- pouvoir pallier à la perte d'un carrier (facteur sécurité) ;
- avoir du poids dans la discussion avec un candidat potentiel, sur la base d'autres informations que celles qu'il fournit via le marketing et la négociation (facteur économique) ;
- pouvoir renégocier les contrats avec des carriers actuels sur la base de données tangibles (facteur économique).

Pour ce faire, cet outil utilise les données de trafic de l'ISP impliqué ainsi que les tables BGP de tous les candidats.

A. Collecte des données BGP

La première étape du processus est de récolter les données BGP des différents candidats et des fournisseurs actuels. Ces données peuvent être collectées de plusieurs manières :

1. directement sur les routeurs de Skynet, si le candidat est déjà carrier ou s'il accepte d'établir une session BGP-MULTIHOP ;
2. par mail, en demandant au candidat de nous envoyer sa table dans un format cohérent ;
3. en implantant sur le réseau du candidat une machine de test qui pourra récolter les données grâce à un logiciel tel que Zebra [IP].

La phase de collecte achevée, nous possédons toutes les données BGP des candidats dans des fichiers. Ces fichiers ne sont pas tous dans le même format.

B. Conversion de format

Aucun format n'est défini au départ, car il existe divers moyens de collecter les données sur un routeur et les formats rendus par les routeurs de type ou de fabriquant différents ne sont pas tous identiques (voir figure 5.2). Chaque table reçue sera donc l'objet d'une analyse préliminaire pour définir son format et, si besoin est, créer un module de conversion (voir figure 5.3). Avant de créer ce module, on vérifiera que les modules existants ne conviennent pas.

sh ip bgp
BGP table version is 53916943, local router ID is 206.24.146.1
Status codes : s suppressed, d damped, h history, * valid, > best, i internal
Origin codes : i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*i 4.0.0.0	206.24.194.62	128	80	0	1 i
*>i	206.24.194.62	128	80	0	1 i
*i 4.22.240.0/21	206.24.194.62	128	80	0	1 7843 i

Fig. 5.2: Exemple de fichier BGP non standardisé

5463 , '194.183.224.0' , 19 , '5463' , '5463' , '5463' , 1 , 1

Fig. 5.3: Exemple de fichier BGP standardisé

Le format standardisé reprend les champs suivants :
- le fournisseur proposant la route ;
- le préfixe annoncé ;
- la taille du masque ;
- l'origine de la route ;
- l'AS-PATH original ;
- l'AS-PATH sans doublon ;
- le nombre d'AS de l'AS-PATH original ;
- le nombre d'AS de l'AS-PATH sans doublon.

La raison de donner l'AS-PATH et sa longueur sans doublon vient du fait que nous recherchons la différence entre l'AS-PATH avec ou sans prepending, afin de pouvoir donner une idée de qualité de la route, tout en gardant à l'esprit (cf. chapitre 2 : BGP) que, pour nous, le prepending indique une route qu'il vaut mieux éviter puisque nous risquons d'y trouver un goulot d'étranglement ou un lien de moins bonne qualité.

N'oublions pas, comme expliqué dans le chapitre 4 (p. 41), que certaines routes vont disparaître à cause de la présence d'AS-SET.

Après cette étape, toutes les données BGP des candidats sont dans un format standardisé et prêtes à être utilisées.

C. Simulateur BGP

La partie la plus importante de notre outil se situe à ce niveau. Le but du simulateur est de reprendre les données des candidats, de construire une table BGP semi-réelle et de l'utiliser pour simuler le trafic Skynet et visualiser ainsi les performances BGP de l'ensemble.

Le simulateur fonctionne en deux étapes :
- sélection des candidats et création de la table BGP ;
- simulation du trafic passant par cette table.

Lors de la création de la table BGP, le simulateur est configuré pour ne tenir compte que des candidats désirés par l'utilisateur. Il est en effet indispensable de pouvoir sélectionner les candidats que l'on désire utiliser. Le but du simulateur est de définir les meilleurs candidats en donnant des résultats permettant de les comparer.

Skynet, par exemple, possède actuellement deux fournisseurs internationaux et aimerait avoir un troisième. Le simulateur sera utilisé une première fois pour analyser l'état actuel du trafic et une seconde fois, en ajoutant certains candidats, pour voir lequel améliore le plus la situation. Utiliser le simulateur avec les tables de tous les candidats donnerait certainement le meilleur résultat possible, mais n'indiquerait pas quel candidat apporte le plus.

La table BGP ainsi créée ne reflète pas une table BGP réelle. Nous ne pouvons pas inclure tout le processus de l'algorithme de sélection et ce n'est pas non plus le but de ce travail. Notre simulateur ne cherche que le meilleur chemin possible pour un préfixe. Si plusieurs chemins sont aussi courts, il les garde tous. Cela permettra de posséder des informations supplémentaires : par exemple, savoir qu'un préfixe est annoncé de manière performante par plusieurs candidats, de sorte que, si un candidat tombe, les autres pourront reprendre le trafic vers ce préfixe de manière tout aussi efficace.
D'un point de vue pratique, une double requête permet de simuler le processus de sélection de la meilleure route en ne tenant compte que de l'AS-PATH et en gardant toutes les routes ayant une longueur d'AS-PATH minimum.

Les figures 5.4 et 5.5 montrent les deux requêtes SQL principales servant à déterminer de manière automatique, respectivement :

1. l'AS-PATH minimum ainsi que le nombre d'AS correspondant par préfixe/masque.
2. la sélection des routes les meilleures, c'est-à-dire les routes correspondant à la longueur minimum trouvée.

La simulation peut alors commencer. Elle a besoin, pour être réaliste, d'au moins une semaine de données, afin de couvrir la majorité des besoins habituels des utilisateurs. Un échantillon plus petit enlèverait certainement des adresses cibles d'utilisateurs qui ne sont présentes que lors de certains jours.

```
insert into MinBgp
select prefix,mask,min(pathlong) as minpath,min(nbrAs) as minas
from BGPDATA as a,fournisseurSimulation as b
where a.idfournisseur = b.idfournisseur
group by prefix,mask
order by prefix,mask
```

Fig. 5.4: Requête de détermination de la plus petite longueur d'AS-PATH par préfixe

```
insert into BgpTableDraft
select a.idfournisseur,a.prefix,a.mask,b.minpathlong,b.minnbras
from MinBgp as b, BGPDATA as a, fournisseurSimulation as c
where a.prefix = b.prefix
and a.mask = b.mask
and a.pathlong = b.minpathlong
and c.idfournisseur = a.idfournisseur
```

Fig. 5.5: Requête de détermination des meilleures routes, pour les candidats choisis

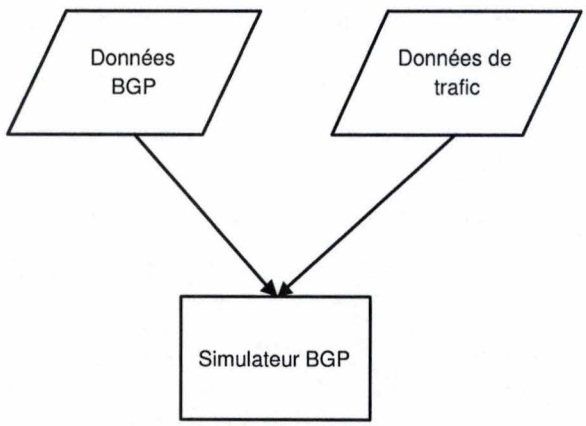

Fig. 5.6: Diagramme de fonctionnement du simulateur

L'algorithme du simulateur se présente comme suit :

```
   Variables :
- masque[ ] : Tableau contenant les masques IP de /8 à /24.
- IP[ ] : Tableau contenant le nombre de bytes reçus pour une adresse IP (/24).
- prefix[ ] : Tableau contenant les préfixes.

              Pour Chaque IP dans la table des IP reçues
                   Tant Que masque non trouvé OU plus de masque
                        Si Comparer IP à masque
                        Alors Ajouter NbrBytes à masque
                        Sinon Ajouter 1 à NbrIPerreur
                   Fin Tant Que
              Fin Pour
```

Cet algorithme devra faire l'objet d'une attention particulière lors de l'implémentation. Il faut en effet le rendre le plus performant possible, car il va utiliser énormément d'informations. La multiplication du nombre d'adresses IP qui envoient des données et du nombre d'entrées dans la table BGP du simulateur représente le nombre minimum d'opérations à effectuer. On peut utiliser le simulateur avec deux types de données en entrée :

1. l'adresse IP destination des paquets (dans le trafic sortant) ;
2. l'adresse IP source des paquets (dans le trafic entrant).

Comme Skynet fournit des services de type ADSL et a donc une bande passante fortement asymétrique, c'est en entrée qu'il reçoit le plus de trafic. De plus, lors de l'établissement de contrats de peering, les ISP tels que Skynet paient le trafic entrant. Il convient, dans ce cas, de se baser sur le trafic entrant en utilisant les adresses sources.

Lors de la capture des données de trafic, aucun contrôle n'est effectué quant à la validité (joignabilité et adresses IP réservées ou non) des adresses IP récoltées. Ceci semble à première vue anodin et surtout logique, car on pourrait croire que toute adresse IP qui passe sur le réseau est une adresse valide. Or, il n'en est rien. Les fournisseurs actuels ne mettent pas toujours en action les filtres nécessaires et laissent transiter des paquets contenant comme adresse IP source ou destination aussi bien des IP valides que des IP invalides. Les IP invalides proviennent de tentatives d'attaque ou d'erreurs de programmation ou, encore, du fait que certains fournisseurs laissent passer sur Internet des paquets provenant de réseaux privés.

Un attaquant, par exemple, essaie d'envoyer un paquet pour exécuter du code malicieux sur une machine distante. Dans le souci de ne pas se faire repérer, il ne donne pas son adresse IP personnelle, mais une autre adresse ou une adresse non valide.

Adresse IP origine : 2.0.0.1

Adresse IP destination : 138.48.5.12

L'adresse IP destination est ici une adresse valide, le paquet arrivera donc à destination sans problème. L'adresse source semble valide aussi, mais la consultation des tables BGP actuelles de l'Internet montre qu'aucune route ne mène à cette adresse IP. Comme l'adresse

de base n'est pas une adresse privée, les filtres des fournisseurs ne considéreront pas ce paquet comme invalide.

Ce phénomène d'adresses invalides peut poser un problème dans le simulateur si l'on cherche à vérifier la quantité de trafic entrée dans le simulateur avec la quantité qui en sort. Cette donnée est importante, car on peut vérifier ainsi si un candidat se disant Tier-1 est capable de router toutes les adresses IP transitant chez Skynet. Lorsque l'on effectue ce test, on devrait obtenir 100% du trafic routé, ce qui ne sera probablement pas le cas. Un nombre avoisinant les 98 à 99% est une valeur correcte pour un Tier-1 car environ 1 à 2% du trafic Internet actuel (mesure effectuée sur le trafic Skynet) contient des paquets avec des adresses invalides.

Une fois le simulateur terminé, une page web permet de visionner les résultats sous forme graphique. Deux graphiques sont disponibles :

1. le nombre de préfixes en fonction de la longueur de l'AS-PATH, avec le pourcentage de trafic en deuxième ordonnée ;
2. le nombre de préfixes par AS traversé (on ne tient pas compte ici des doublons dans l'AS-PATH), le pourcentage de trafic étant donné également en seconde ordonnée.

Les deux graphiques représentent bien deux notions différentes. Le premier ne tient pas compte des AS traversés, mais simplement du nombre d'éléments dans l'AS-PATH, alors que le deuxième donne les informations sur le nombre d'AS traversés. La vue des deux graphiques permet de déterminer d'un simple coup d'oeil la quantité de trafic qui arrive directement à destination. Si 90% du trafic arrive à destination au bout de trois AS et que le même pourcentage se retrouve quand on tient compte du nombre d'éléments dans l'AS-PATH, sachant que le simulateur choisit toujours les meilleures routes, on peut conclure que 90% du trafic atteint son objectif en trois sauts et qu'il n'y a pas de prepending sur ces routes. Le but recherché est de ramener la majorité du trafic, dans les deux graphiques, le plus près possible de un saut.

5.3.2 Analyse non fonctionnelle

Comme nous l'avons expliqué lors de la présentation globale du projet, la performance de l'outil est un aspect important. Le simulateur ne sera pas utilisé tous les jours, mais lors de la sélection d'un fournisseur ou lors de la renégociation avec celui-ci. Puisque le but du simulateur est de créer des graphiques permettant de comparer des candidats, il apparaît clairement que le temps de génération des graphiques ne peut être trop important. Or, le nombre de données à traiter est assez énorme. Si l'on n'optimalise pas l'algorithme, mais que l'on fait des boucles de recherche classiques, Skynet recevant du trafic en provenance d'un centième des adresses IP disponibles (environ 50 000 000 d'adresses) à classer parmi les quelques 110 000 routes annoncées, on obtient un nombre moyen de boucles égal à 50 000 000 * 55000 = 2 750 000 000 000 (si l'on considère que les adresses IP sont réparties uniformément dans les routes annoncées), ce qui représente un nombre très important d'itérations, d'autant plus que la recherche n'est pas la seule opération à effectuer dans les boucles.

Un deuxième point important en ce qui concerne le simulateur a déjà été évoqué dans la description de la table BGPTABLERESULT et de la table des verrous. Le simulateur prenant un certain temps pour effectuer son travail, il convient :

1. d'empêcher le simulateur de s'exécuter plusieurs fois en parallèle, ce qui aurait des conséquences désastreuses sur les performances ;
2. de protéger les résultats en empêchant l'exécution d'un simulateur tant que les résultats n'ont pas été visionnés au moins une fois.

Le système de verrous est une solution à ce problème.

Une autre solution aurait été de permettre au simulateur de générer une table contenant les résultats par exécution et de permettre à la personne visionnant la page de supprimer cette table une fois son analyse des résultats terminée. Le problème est que les ressources nécessaires pour générer un graphique sont très importantes et que permettre la génération de plusieurs rapports simultanément pourrait coûter beaucoup et empêcher la machine de faire les autres tâches.

Pour permettre ce genre de chose, il faudrait multiplier les machines traitant le problème afin de centraliser les opérations critiques sur une ou plusieurs machines et désolidariser la génération des rapports en utilisant pour ce faire une autre machine.

5.3.3 Réalisation

L'outil d'analyse BGP se basant principalement sur des routes, des adresses IP et autres strings, le choix du langage de développement s'est naturellement porté sur PERL [Per]. Tout en restant simple d'utilisation, ce langage présente des fonctionnalités très poussées de traitement de chaînes de caractères. De plus, PERL est un outil où le fichier source est compilé puis exécuté à la volée (sauf si l'utilisateur en décide autrement), ce qui permet d'éviter les problèmes inhérents à la multiplication des versions et à la sauvegarde, puisqu'il n'existe pas de fichier résultant d'une compilation et donc dificilement identifiable.

Tous les scripts de traitement des données, de récupération des informations et d'insertion dans la base de données sont donc développés en PERL.

Les propriétés de compilation à la volée n'ont posé aucun problème tant que nous nous sommes limités aux fonctions de base du projet, mais, lorsque l'on a suscité davantage la base de données, les performances globales de la machine se sont effondrées, y compris les scripts PERL. Or, ceux-ci effectuant notamment des traitements d'agrégation, cette baisse de performance a posé un problème insoluble qui nous a obligé à changer notre manière de travailler. En effet, un script développé et optimisé pour tourner vingt minutes en temps normal prenait plus de quarante minutes. Comme certains scripts d'agrégation s'enchaînaient (on agrège les données par heure, puis les données agrégées par heure en agrégations par jour), chacun attendait la fin du script précédent avant de démarrer. Si le temps d'exécution d'un script devenait trop important, c'est l'ensemble de la chaîne des scripts qui était mise en dificulté puisque certains scripts ne pouvaient pas se lancer à chaque heure.

Nous avons alors cherché à optimiser le plus de tâches possibles en utilisant, si nécessaire, un langage différent. Toutes les fonctions d'agrégation ont été regroupées au sein d'un programme C dont la fonctionnalité est de récupérer les données à insérer dans la base pour les placer dans un fichier. Le programme parcourt ensuite ce fichier afin d'effectuer, au vol, les agrégations de tout type et produire des fichiers dont le format permet l'insertion immédiate dans la base.

Ce procédé ne laisse plus au PERL que les scripts de traitement des informations avant affichage et le simulateur.

A terme, il a été décidé de remplacer tous les scripts PERL par des programmes C pour les opérations d'insertion et d'agrégation des données de trafic, car le gain de vitesse est de l'ordre de 1000 dans la majorité des cas. Les scripts de traitement des tables BGP, eux, sont conservés en PERL, pour une plus grande facilité d'emploi et parce que les facilités de traitement des chaînes restent un atout plus avantageux que la vitesse offerte par le C.

5.4 Outil de mesure de délai

Après lecture des résultats donnés par les premières simulations, nous avons souhaité donner un poids supplémentaire à nos conclusions. Pour ce faire, nous avons décidé d'ajouter en parallèle des mesures de délai, effectuées à partir de machines de test toutes identiques et placées à l'intérieur même des réseaux des candidats qui l'acceptaient (démarche apparemment inhabituelle pour les candidats). Ces résultats devaient soit confirmer la simulation, soit l'infirmer ; dans ce dernier cas, il nous fallait trouver pourquoi et remettre en cause notre hypothèse sur la qualité BGP.

L'outil de mesure de délai est un outil très simple. Il interroge le top 100 des destinations qui nous envoient le plus de trafic avec des paquets ICMP normaux et, si ces mesures échouent, avec des paquets TCP, moins sensibles aux pertes. Il indique ensuite les cibles qui deviennent parfois injoignables.

Le procédé consiste à disperser les prises de mesure de délai selon une méthode de Poisson. En effet, vu la vitesse des liens utilisés, des mesures faites sans prendre cette précaution pourraient ne pas refléter le comportement du réseau candidat. Nous avons choisi d'étaler nos mesures de délai suivant une répartition de Poisson sur une heure. Idéalement, il aurait fallu interroger les destinations de manière aléatoire (toujours selon une dispersion de Poisson) et proportionnellement à leur importance dans notre classement. Mais, étant donné que le comportement des internautes interrogeant une cible varie non sur un laps de temps d'une heure, mais sur des laps de temps de l'ordre du jour voire de la semaine, cela n'a que peu d'impact sur la représentativité de nos mesures.

Les données sont stockées sur les machines dans un fichier, par heure. Ce fichier est rapatrié sur une machine Skynet où les données sont traitées. Un nouveau problème apparaît à ce stade : le calcul du seuil de validité des valeurs mesurées. En effet, il est bien connu en

statistique qu'il faut accepter des erreurs de mesure et établir les bornes de validité de l'ensemble contenant les valeurs d'une donnée. Or, tout 0 qui apparaît dans nos mesures n'est pas obligatoirement une erreur de mesure ; une oscillation forte, courte et périodique ne l'est pas forcément non plus. N'oublions pas que nous avons affaire à des réseaux interconnectés, pas toujours stables et pas toujours fiables. Dans cette perspective, aucune valeur n'est déclarée incorrecte ou hors norme. On indiquera simplement dans les résultats le nombre de valeurs à caractère exceptionnel, la variance et l'écart type et cela sur l'ensemble des valeurs, afin de montrer toutes les caractéristiques des sites mesurés.

5.5 Exemple de résultat de l'outil

Les figures 5.7 et 5.8 montrent le trafic actuel de Skynet tel qu'il se présente à travers le simulateur.

Le graphique 5.7 offre deux informations :

1. Le trait sombre représente le nombre de préfixes en fonction de la longueur de l'AS-PATH (en tenant compte du prepending) ;
2. Les deux autres traits montrent la quantité de trafic passant par les routes dont la longueur est en abscisse, en pourcentage (trait le plus sombre) et en pourcentage cumulé (trait le plus clair).

Le graphique 5.8 fournit les mêmes informations que le graphique précédent, mais en retirant le prepending.

L'outil BGP se résume, pour l'utilisateur et dans l'état actuel de la théorie proposée dans le chapitre 3, à la lecture des graphiques qui montrent la simulation du trafic dans les tables de routage. Si la lecture d'un tel document peut ne pas sembler parlante pour des néophytes de BGP et du trafic international, les spécialistes y trouvent une source importante d'informations sous un format directement exploitable.

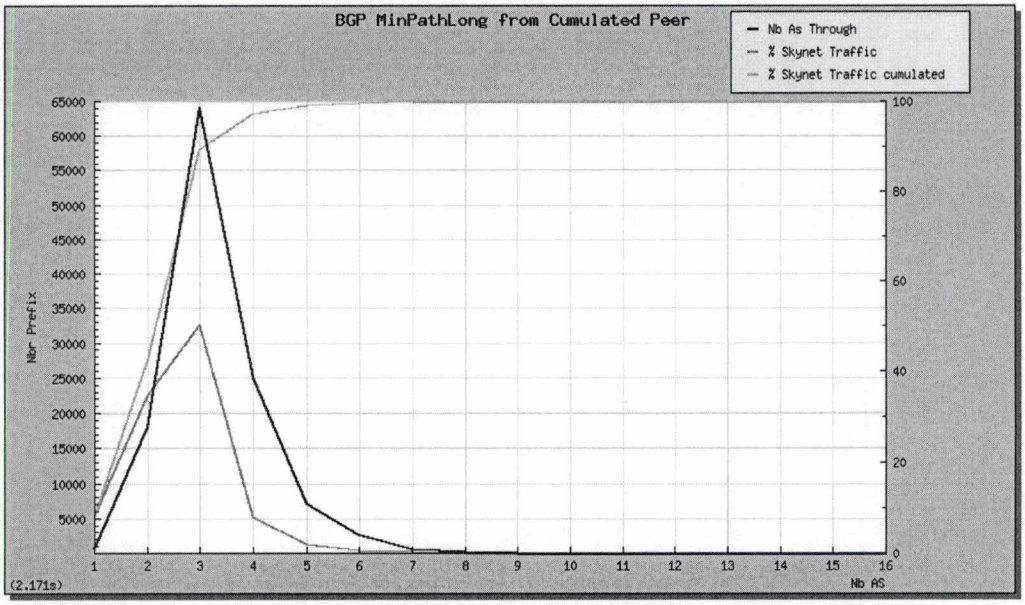

Fig. 5.7: Nombre d'AS traversés et nombre de routes annoncées (avec prepending)

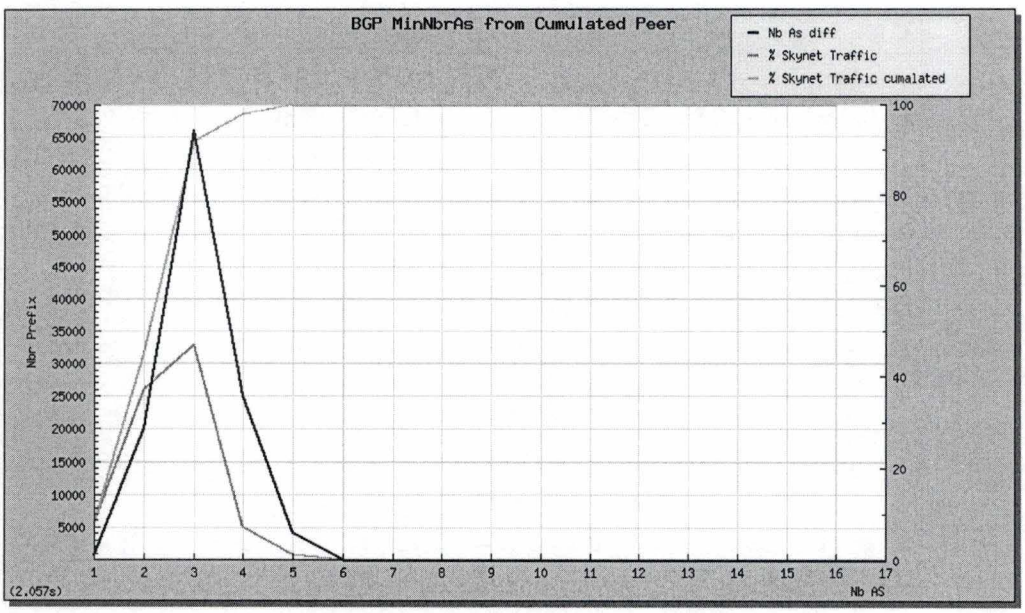

Fig. 5.8: Nombre d'AS traversés (sans prepending)

6. PRÉSENTATION DES RÉSULTATS ET CONCLUSION

6.1 Résultats

6.1.1 L'outil de visualisation du trafic

Remarque : Pour des raisons évidentes de confidentialité, des zones floues sont appliquées sur certains types de données dans les graphiques qui suivent.

L'ensemble des pages disponibles apporte diverses informations. Le graphique 6.1 montre la page principale du site de visualisation du trafic. Son fonctionnement a été décrit à la page 36. Les graphiques 6.2 à 6.4 présentent la page de vue du trafic réparti par AS, qui permet de voir avec quels AS nous échangeons principalement du trafic. En conservant un historique de ces pages, on peut évaluer, dans le temps, les habitudes des internautes.

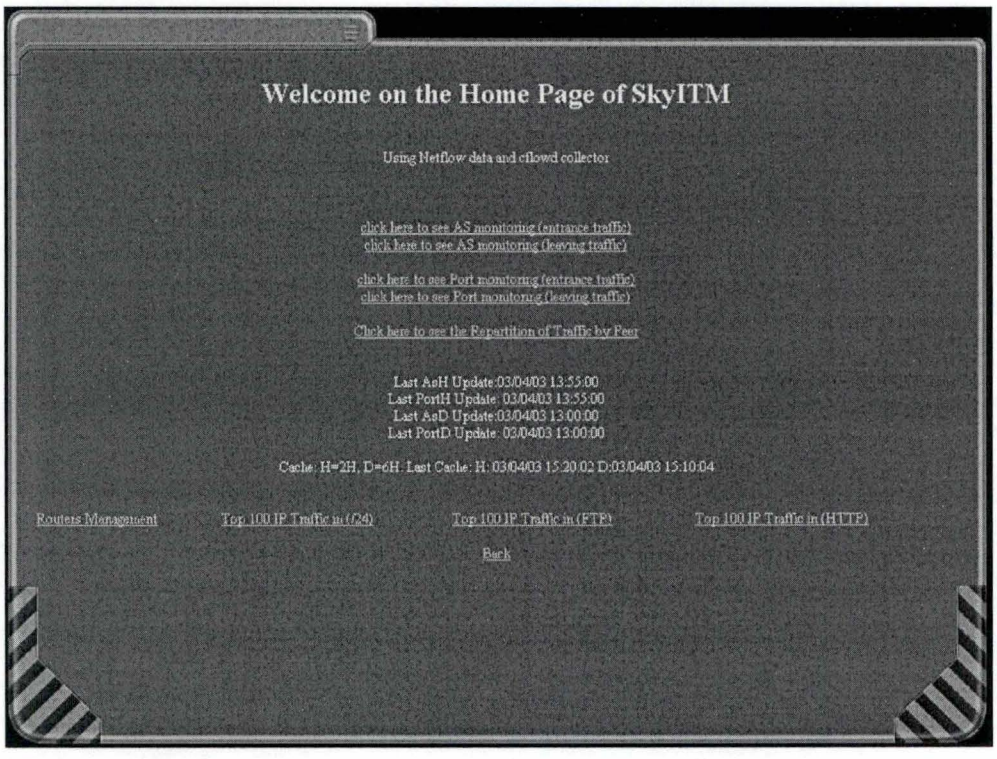

Fig. 6.1: Page principale du site Intranet de contrôle de trafic

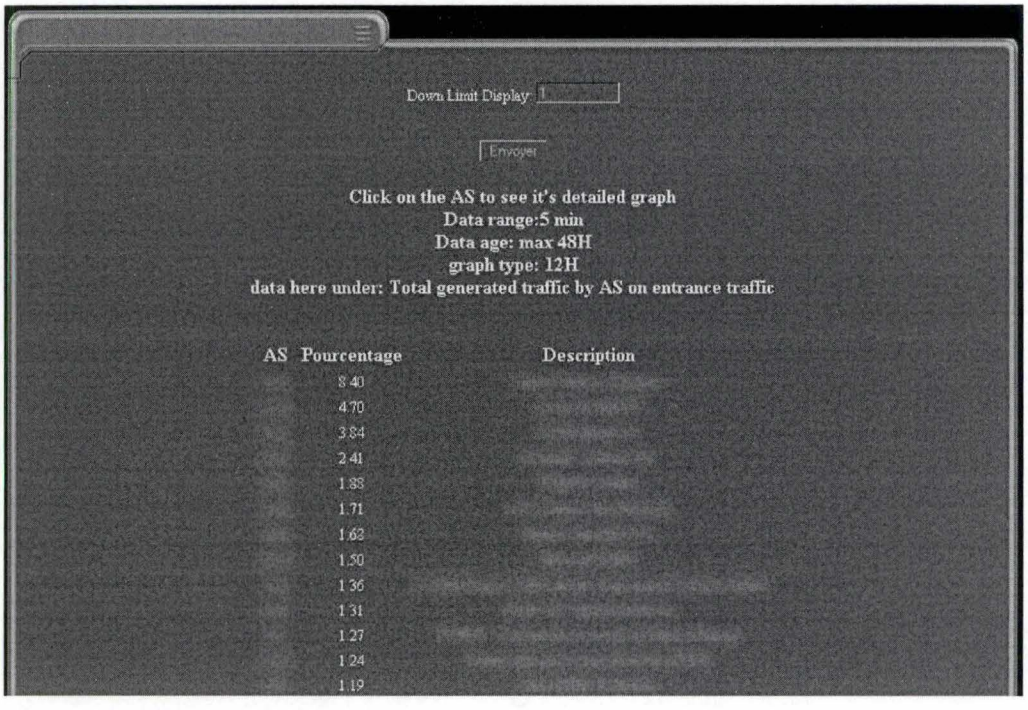

Fig. 6.2: Vue de la distribution du trafic entrant par AS (première partie)

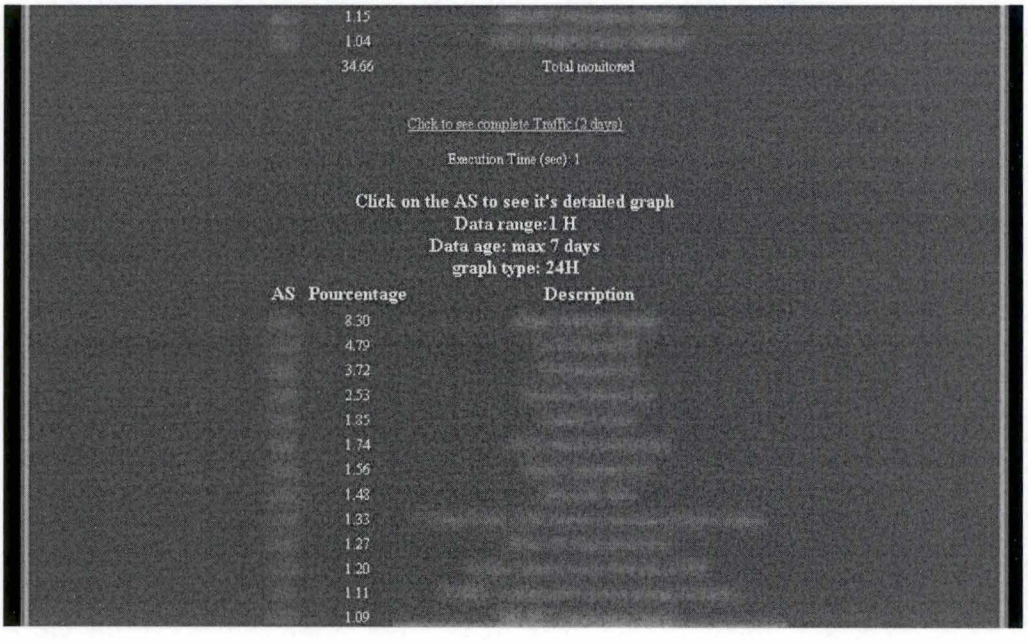

Fig. 6.3: Vue de la distribution du trafic entrant par AS (deuxième partie)

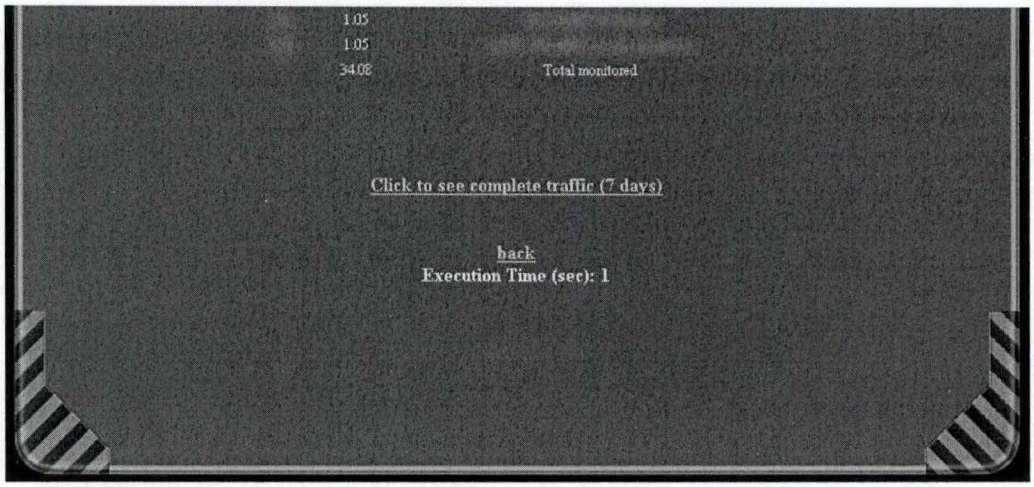

Fig. 6.4: Vue de la distribution du trafic entrant par AS (troisième partie)

Les graphiques 6.5 et 6.6 présentent le trafic réparti par port. Cette page permet de voir de manière détaillée les types de trafic les plus utilisés et de surveiller les ports les plus connus, à savoir, le port HTTP (80), FTP (20 - filetransfert), News (119), Edonkey (4662), Kazaa (1214) et Napster (6699), ainsi que le mail (25 SMTP). Ces ports sont les ports soit origine, soit destination soit origine et destination de paquets en entrée dans le réseau. La première conclusion est que 57% du trafic emprunte de manière systématique ces ports. Ce chiffre paraît important, mais cela signifie surtout que 43% du trafic est inclassable car utilisant des ports non définis spécifiquement.

Parmi ces résultats, on retrouve près de 30% de trafic pour le peer to peer. Sachant que de plus en plus d'applications peer to peer permettent de changer les ports utilisés, nous sommes certains que le trafic peer to peer représente quasiment le double. En effet, le trafic HTTP utilise le plus souvent le port 80 en port origine et le trafic FTP n'est pas un trafic aussi important que le P2P. On peut donc dire que sur le réseau Skynet, qui comprend des entreprises (PME et certaines de plus grande taille), des institutions et des particuliers, seulement 25% du trafic est de l'HTTP, ce qui est bien peu par rapport au plus de 30% identifié - et certainement plus de 50% probable - de trafic P2P. Le trafic FTP représente pour sa part à peine 1%, ainsi que le mail, et le trafic de news 3% seulement. Une remarque doit être apportée pour le trafic FTP. En effet, Skynet héberge un ensemble de sites miroirs qui sont souvent utilisés sur son réseau. Ce trafic n'est pas surveillé par notre outil qui ne montre que le trafic international.

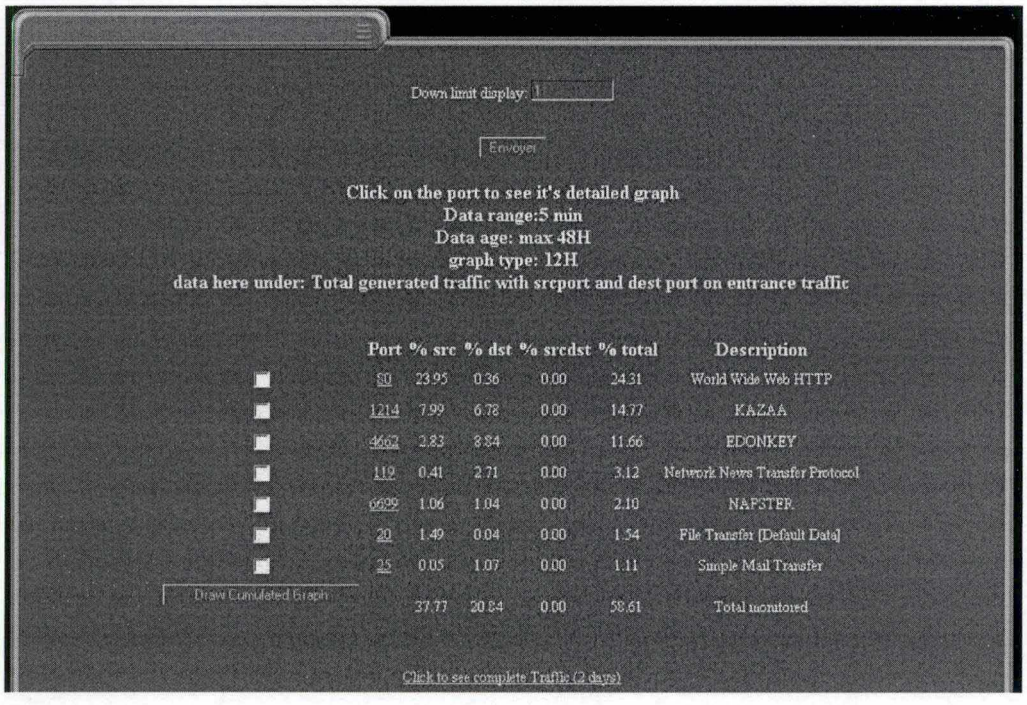

Fig. 6.5: Vue de la distribution du trafic entrant par port (première partie)

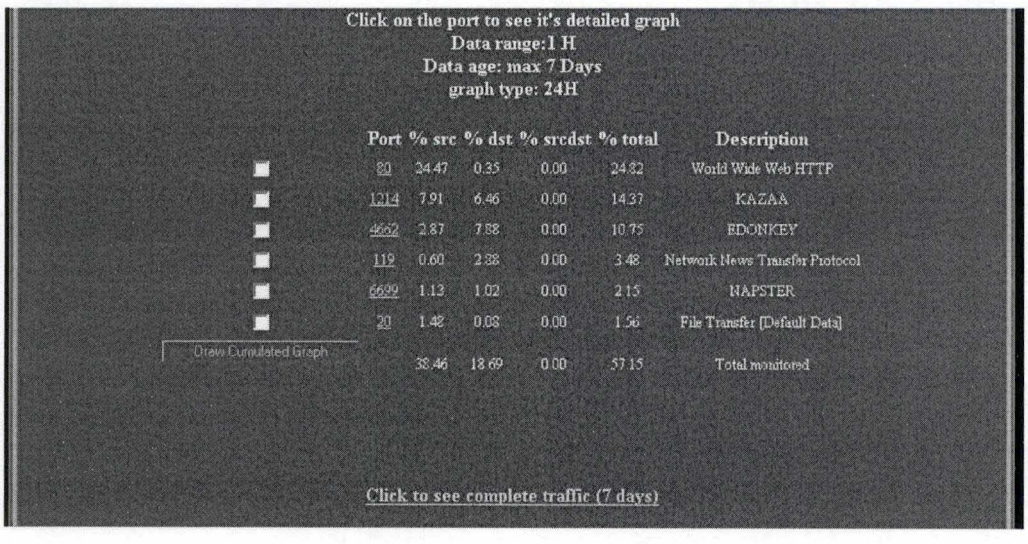

Fig. 6.6: Vue de la distribution du trafic entrant par port (deuxième partie)

Les graphiques 6.7 et 6.8 montrent le trafic entrant et sortant par peer. Les deux tracés indiquent très clairement que certains fournisseurs ont un trafic entrant beaucoup plus important que le sortant, ce qui est la preuve du trafic asymétrique de Skynet. On remarque aussi que, si les fournisseurs internationaux (les deux plus importants) envoient plus ou moins la même quantité de trafic, notre trafic sortant n'est, en revanche, pas bien réparti entre eux.

Ceci est une conséquence directe de la qualité BGP des peer. Le peer qui apporte beaucoup de trafic à Skynet et qui sert de sortie pour très peu a une qualité BGP médiocre. Normalement, on devrait voir des tracés assez uniformes si l'on suit notre théorie (si algorithme de routage par défaut, équilibre des trafics (p. 40)). Dans ce cas précis, la mauvaise qualité du fournisseur étant expliquée par un fait connu, tous les clients de ce fournisseur corrigent la qualité en utilisant les filtres BGP, mais pas Skynet. En effet, Skynet ne paie que le trafic entrant et pas le sortant : une aussi grande divergence dans la sortie du trafic n'est donc pas un problème en soi tant qu'aucun lien de sortie (d'aucun fournisseur) n'est saturé.

Les autres fournisseurs ont des comportements normaux, sachant que Skynet absorbe plus de trafic qu'il n'en produit. Le tracé en équilibre est le tracé du BNIX qui montre bien que les accords de peering établis au BNIX sont profitables équitablement aux deux parties engagées.

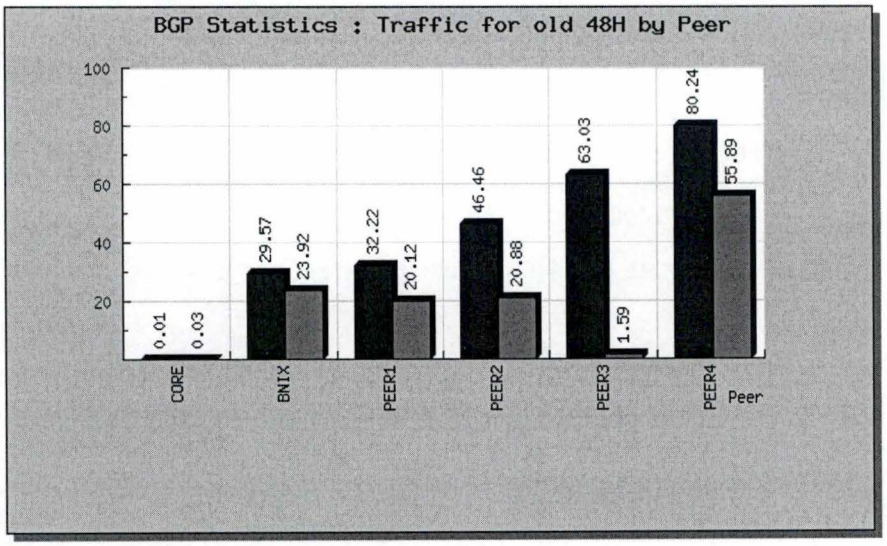

Fig. 6.7: Vue de la quantité de trafic entrant (gauche) et sortant (droite), par peer, en Mb/s (48 H)

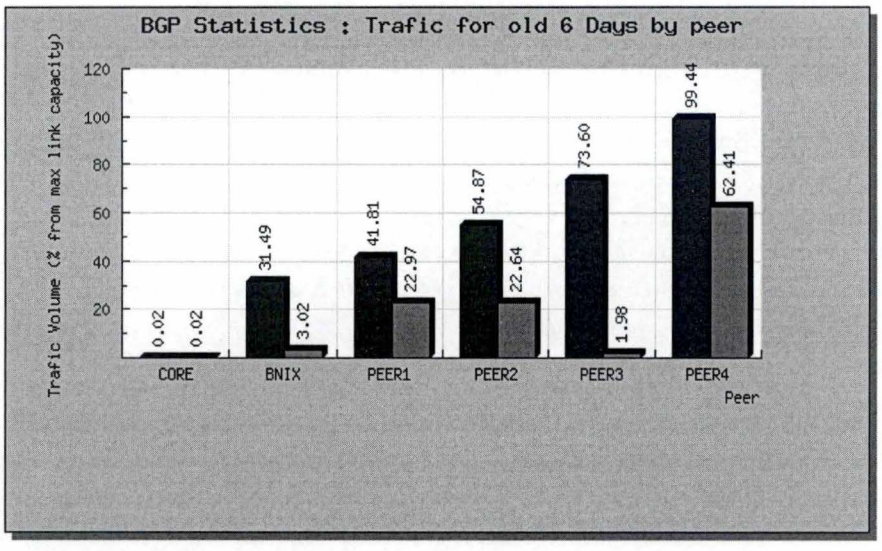

Fig. 6.8: Vue de la quantité de trafic entrant (gauche) et sortant (droite), par peer, en Mb/s (6 Jours)

L'outil BGP

Dans l'état actuel du projet, l'outil BGP n'est pas terminé, mais il permet déjà de donner un ensemble de résultats : les rapports de simulation du trafic au travers des tables des candidats. Les graphiques suivants présentent des exemples révélateurs du but recherché par l'outil ainsi que la manière dont il rend les informations afin de pouvoir prendre des décisions.

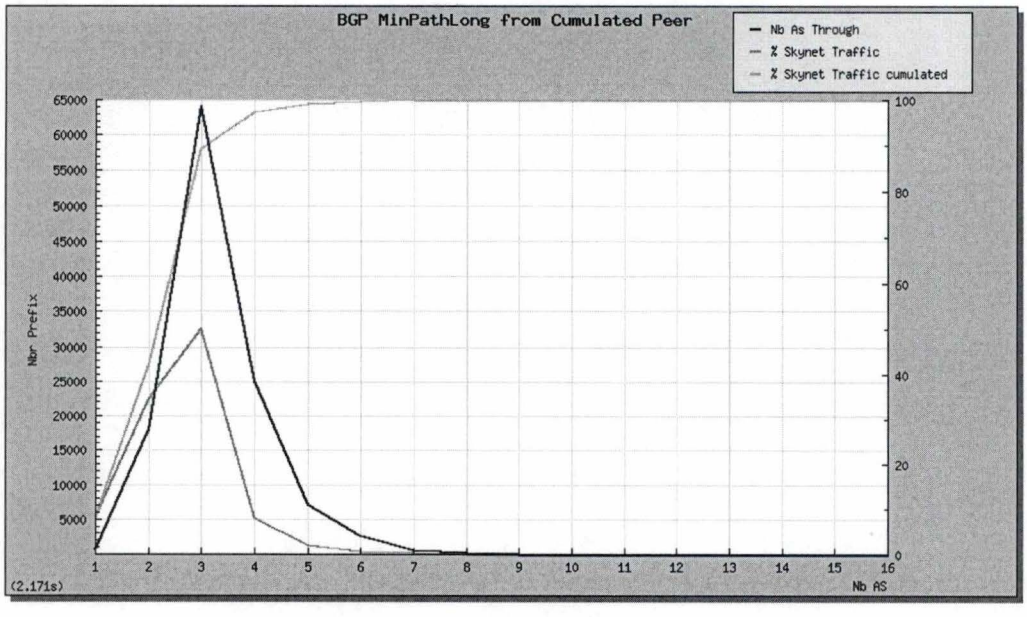

Fig. 6.9: Nombre d'AS traversés et nombre de routes annoncées (avec prepending)

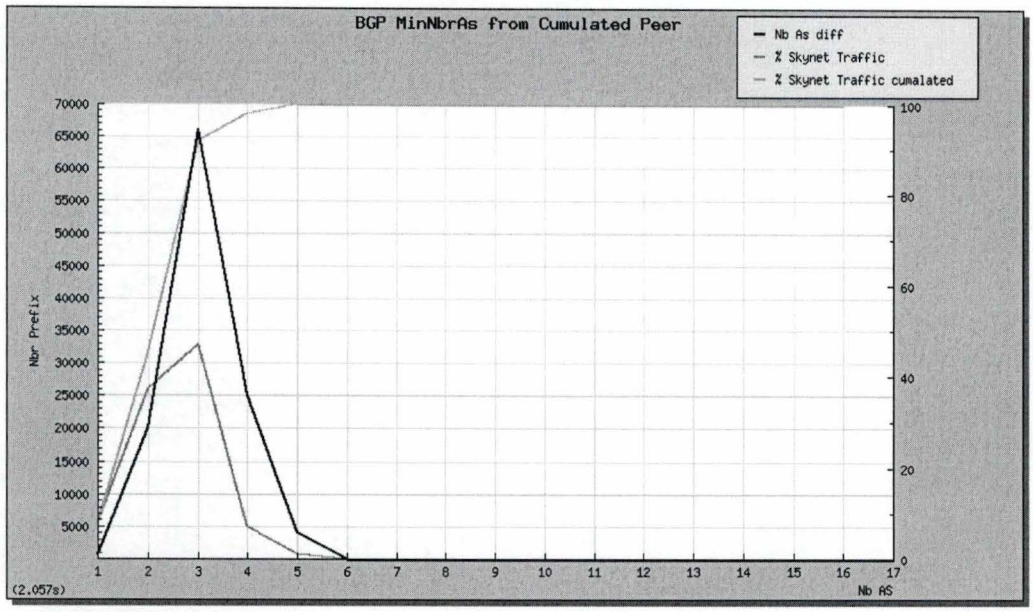

Fig. 6.10: Nombre d'AS traversés et nombre de routes annoncées (sans prepending)

Les graphiques 6.9 et 6.10, montrent l'état actuel du trafic de Skynet. Le premier permet d'observer directement qu'avant toute intervention, avec les fournisseurs actuels, près de 90% du trafic est déjà à une distance de trois sauts maximum (avec prepending !) et que l'on atteint 99% à cinq sauts, ce qui est déjà représentatif d'un bon trafic. De plus, plus de 40% du trafic est à deux sauts et près de 10% à un saut (ceci s'explique principalement par la présence de Skynet au BNIX avec, donc, des accès direct à certains réseaux). On observe aussi qu'un peu plus de 80 000 préfixes sont annoncés sur des routes de trois sauts au maximum avec près de 20 000 à deux sauts.

Certains préfixes sont annoncés avec une meilleure route de 17 sauts. D'après le simulateur, les routes de plus de dix sauts ne sont jamais utilisées, mais il est tout à fait possible que quelques paquets proviennent de ces réseaux et que l'échantillonnage fasse que l'on n'en tienne pas compte.

Le deuxième graphique offre les mêmes informations, mais sans tenir compte du prepending, c'est à dire qu'un AS apparaissant plusieurs fois dans un AS-PATH ne sera compté qu'une seule fois. Ce graphique indique donc comment serait le trafic si aucun prepending n'était utilisé. Il est intéressant de le comparer au premier afin d'estimer les pertes de qualité induites par la présence de prepending. Dans ce cas-ci, les valeurs sont à peine un peu plus élevées, ce qui laisse penser que la table avec prepending est une table d'excellente qualité, puisque ce prepending joue très peu pour les préfixes qui nous intéressent.

Il est intéressant de voir que la route maximum est de longueur 7, ce qui revient à dire que nous devrions traverser au maximum sept AS pour atteindre n'importe quelle destination.

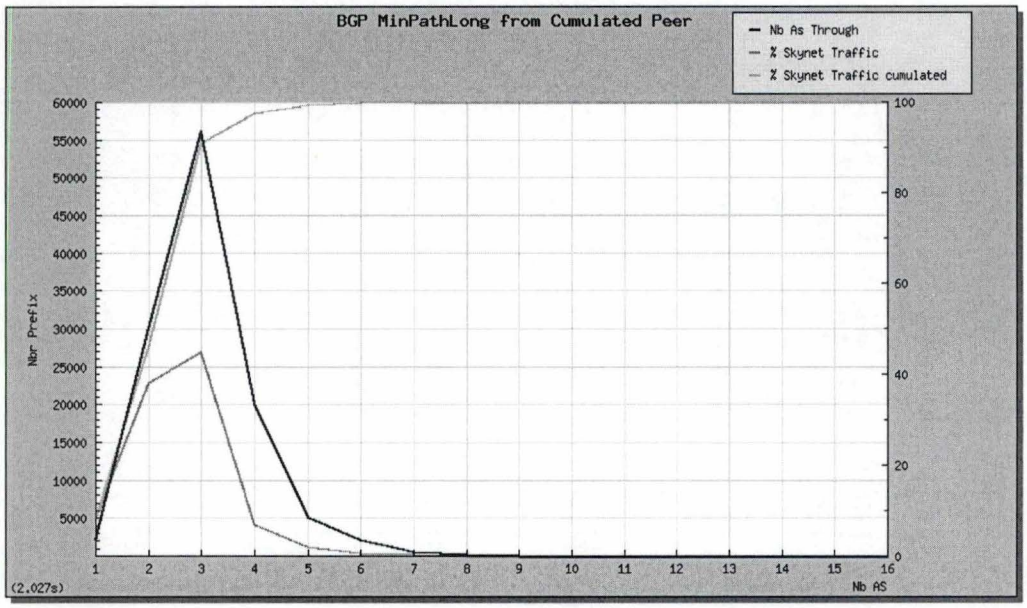

Fig. 6.11: Nombre d'AS traversés et routes annoncées (avec prepending)

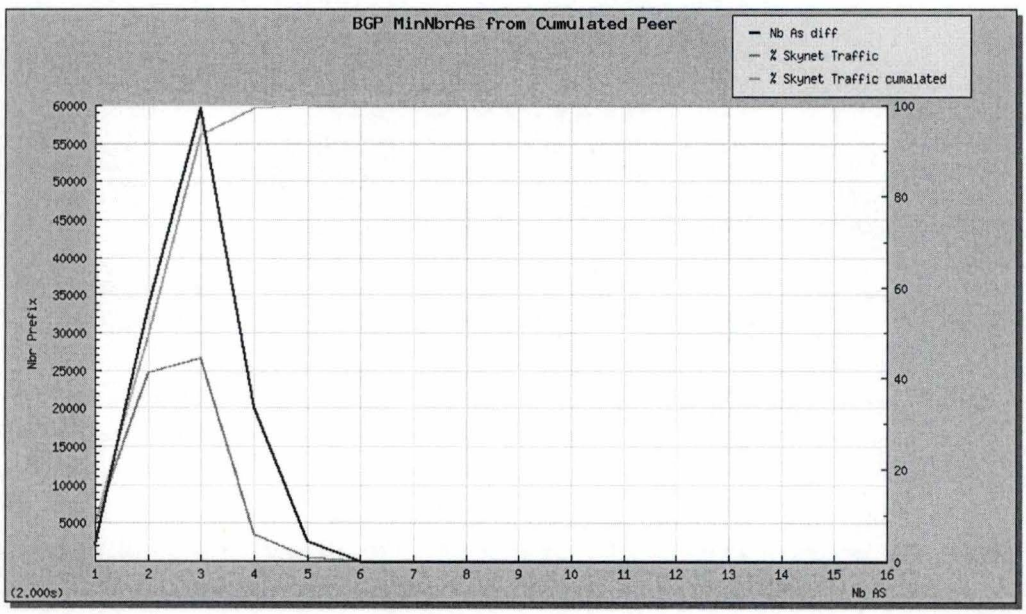

Fig. 6.12: Nombre d'AS traversés et routes annoncées (sans prepending)

Les mêmes rapports peuvent être générés pour un des candidats fournisseurs, en ajoutant sa table dans les tables sélectionnées par le simulateur. Les graphiques 6.11 et 6.12 montrent le même trafic que pour les graphiques 6.9 et 6.10, mais au travers d'une table BGP recréée à partir de la table BGP Skynet et de celle d'un candidat. On voit tout de suite que les allures des graphiques ne sont pas les mêmes : il semble que l'on ait gagné en qualité sur tous les points.

Une fois que deux rapports ont été générés, il est intéressant de reprendre les informations des deux rapports et de les comparer directement sur un graphique propre à chaque donnée. Les comparaisons étant toutes du même type, deux seulement sont proposés ici. En annexe se trouvent trois rapports complets, ainsi que les comparaisons entre les rapports 1 et 2 et entre les rapports 2 et 3.

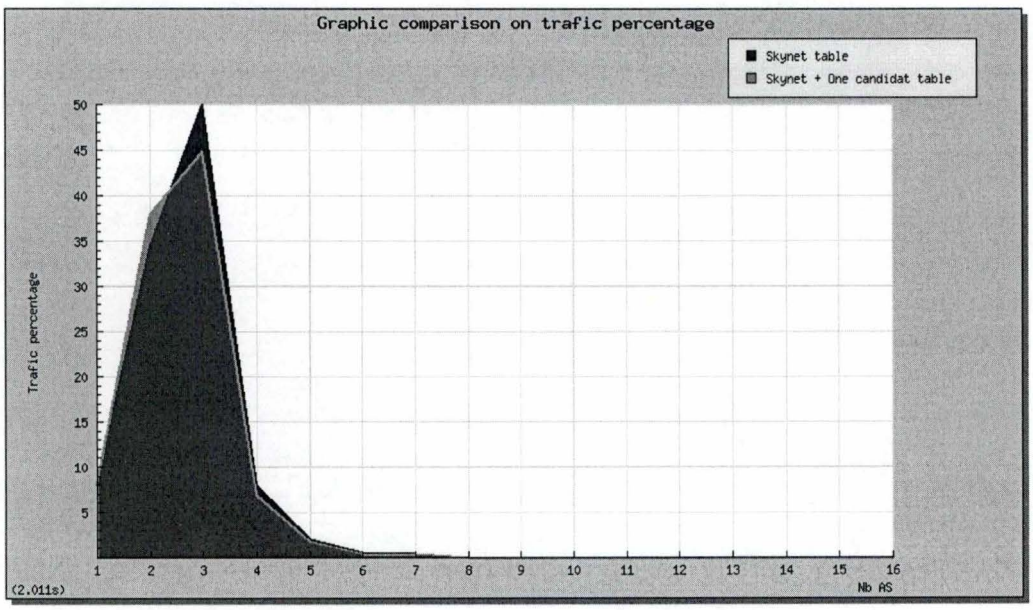

Fig. 6.13: Comparaison des pourcentages de trafic (Skynet-Skynet+1Candidat) (avec prepending)

Les graphiques des figures 6.13 et 6.14 fournissent les comparaisons entre, respectivement, les pourcentages de trafic (avec prepending) et le nombre de routes annoncées.

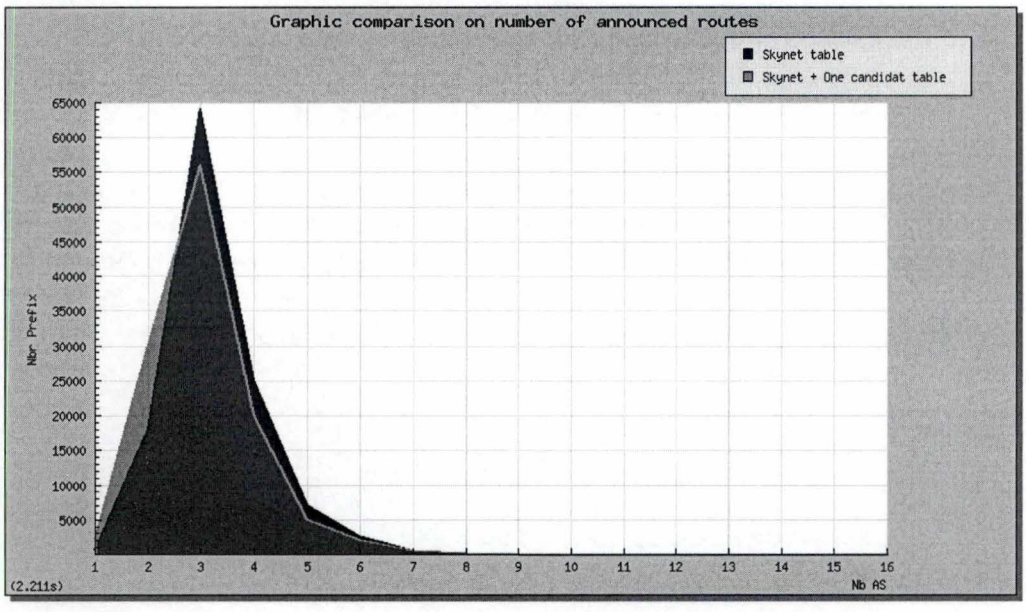

Fig. 6.14: Comparaison du nombre de routes annoncées (Skynet-Skynet+1Candidat) (avec prepending)

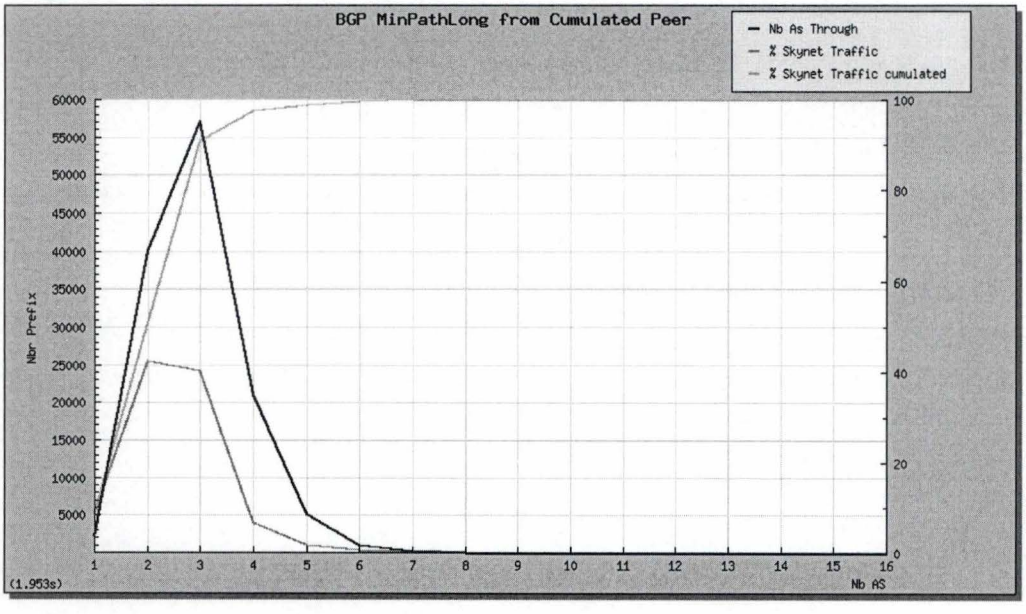

Fig. 6.15: Nombre d'AS traversés et routes annoncées (avec prepending)

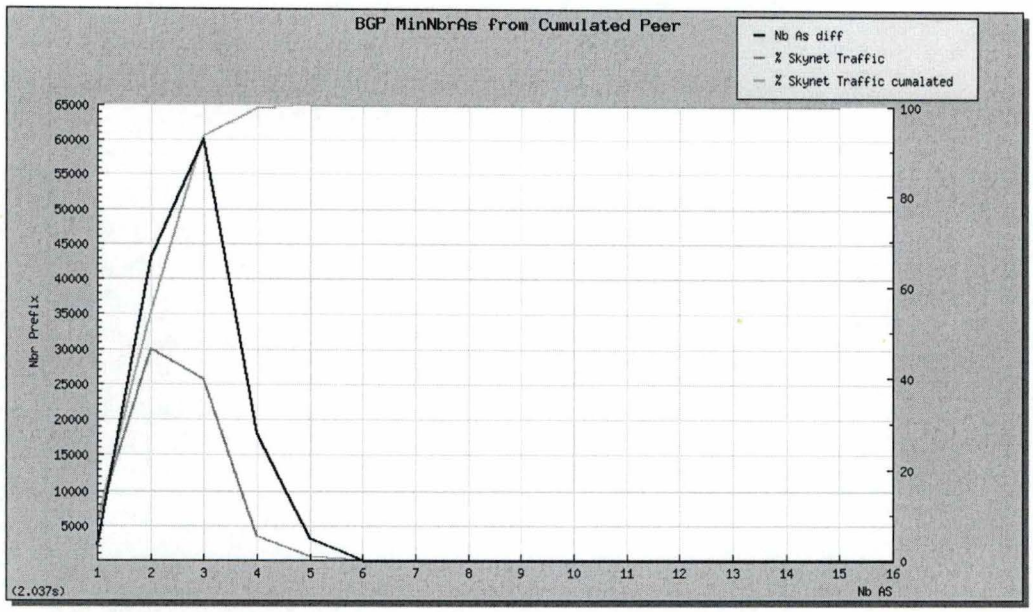

Fig. 6.16: Nombre d'AS traversés et routes annoncées (sans prepending)

Un regard plus attentif sur les valeurs de ces graphiques apprend que l'on passe de 20 000 à quelques 30 000 routes annoncées avec un AS-PATH de 2, et de 55 000 à plus de 63 000 avec un AS-PATH de 3. Ce candidat apporte donc une bonne qualité BGP supplémentaire en rapprochant Skynet de beaucoup de préfixes, mais rien ne dit que cela aura un impact sur le trafic. Or, les données concernant le trafic sont elles aussi en hausse. Près de 48% (+ 4%) de trafic (trafic cumulé) passe par des routes dont la longueur est de maximum deux sauts et l'on atteint plus de 90% (moins de 90 % pour Skynet seul) pour le trafic utilisant des routes de maximum trois sauts. On ne tiendra pas compte des valeurs au delà de dix sauts, ces valeurs étant produites par des erreurs d'arrondi lors des calculs.

Un rapport généré à partir des données de tous les candidats montrerait la meilleure table possible, représentée par les graphiques 6.15 et 6.16. Ceci n'est intéressant qu'à titre comparatif : il est plus que vraisemblable qu'aucun ISP n'établira de lien avec tous les fournisseurs présents sur le marché. On peut comparer la qualité BGP offerte en plus à Skynet par l'ajout d'un candidat avec cette qualité maximum possible. Les graphiques 6.17 et 6.18 montrent les comparaisons des pourcentages de trafic et des routes annoncées. Ces graphes donnent des valeurs encore meilleures par rapport aux valeurs des graphes précédents, ce qui est tout à fait logique. En effet, chaque fournisseur annonce ses propres routes avec les routes les plus courtes et, comme ils sont de grande taille, ils possèdent chacun quelques adresses en accès directs. Les graphes de comparaison des valeurs montrent qu'il y a encore des améliorations possibles malgré l'ajout de la table d'un candidat, mais que ces améliorations sont assez minces.

Tous ces graphiques montrent clairement que, pour augmenter la richesse BGP de Skynet, il est nécessaire de prendre le nouveau lien chez un nouveau fournisseur. L'outil permet donc de valider la théorie de départ.

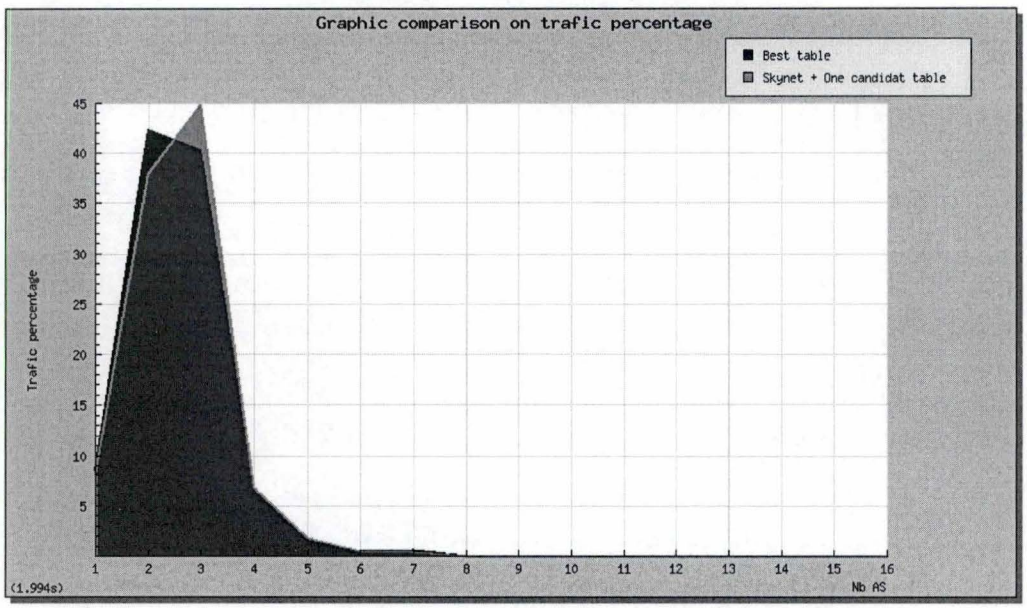

Fig. 6.17: Comparaison des pourcentages de trafic (Skynet+1candidat - Best) (avec prepending)

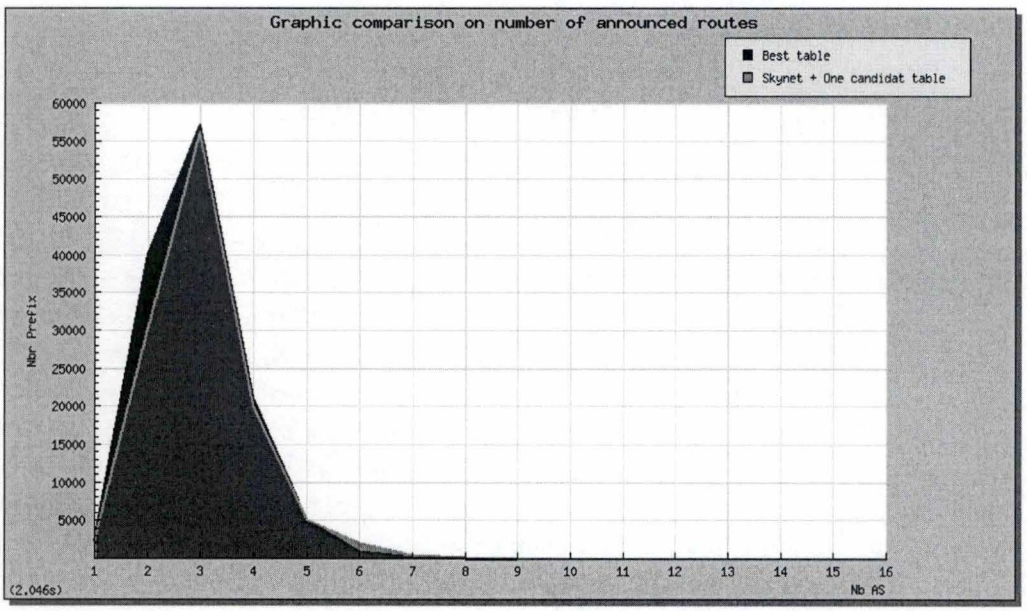

Fig. 6.18: Comparaison du nombre de routes annoncées (Skynet+1candidat - Best) (avec prepending)

6.2 Conclusions

6.2.1 Conclusions par rapport aux résultats obtenus

Le projet a été mené à bien, puisqu'une décision effective a pu être prise grâce aux rapports générés. En effet, après avoir généré l'ensemble des rapports possibles et y avoir ajouté les données de délai que nous possédions, il s'est avéré que le candidat qui offrait la meilleure qualité BGP était second dans les mesures de délai. Suite à ces excellents résultats, c'est ce candidat qui a été choisi comme nouveau fournisseur de Skynet.

L'outil de visualisation fonctionne sans problème et permet de bien consulter les chiffres souhaités : l'ensemble des données présentées montre bien la répartition du trafic sous les trois angles les plus importants, à savoir par AS, par port et par fournisseur.

Le projet n'a pas pour autant été mené à son terme. Il a pris un peu de retard dans son développement pour résoudre des problèmes de performance, plus importants que nous ne l'avions estimé. Ce retard n'a pas entraîné de lourdes conséquences pour les points clefs du projet, mais les points plus secondaires n'ont pas été achevés. En ce qui concerne la partie visualisation du trafic, il ne manque qu'un historique plus long du trafic. Pour la partie BGP, il manque encore l'automatisation de la récupération des mesures de délai ainsi que leur intégration aux différents rapports, la possibilité de consulter les données sur plus d'un mois et l'intégration automatique des graphiques comparatifs dans les rapports. Actuellement, les rapports automatiques ne se composent que des deux graphiques de base car l'intégration des graphiques de comparaison pose le problème d'avoir les données disponibles pour les comparaisons et donc, d'avoir déjà fait tourner le simulateur et d'avoir sauvé les résultats précédents.

La théorie sur la qualité BGP a quant à elle été validée par l'ensemble des données des graphiques générés par l'outil. Elle n'est cependant pas parfaite puisque bon nombre de détails peuvent être améliorés. On pourrait par exemple définir des critères plus sévères pour la mesure de délai, en pondérant par exemple cette mesure en fonction du nombre de sauts IP mesurés, ce qui donnerait une idée plus précise sur la longueur du chemin jusqu'à la destination ainsi que sur sa stabilité. On pourrait également ajouter dans l'outil la possibilité de mesurer la stabilité des tables BGP en relevant régulièrement celles-ci et en les comparant. On pourrait aussi, au niveau de l'interprétation des données, montrer plus d'éléments : par exemple le trafic minimum, maximum et moyen qui devrait entrer par un fournisseur en fonction de la variation de la table créée dans le simulateur, cette table variant avec la sélection de différents candidats. En résumé, cette théorie, qui a permis à Skynet de faire un bon choix, est une bonne base de départ qui mériterait cependant d'être développée davantage.

6.2.2 Conclusion

Ce travail propose une solution, basée sur une réflexion théorique concernant la comparaison d'ISP et l'ensemble des données qu'un ISP possède pour établir son choix, à savoir principalement ses propres données de trafic, les tables de routages des autres ISP ainsi que les mesures de délais que l'on peut effectuer chez les candidats avec leur accord.

Une fois ces données collectées, il est important de pouvoir les comparer comme si le lien

devenait effectif. Pour cela, un simulateur a été créé : sont but est de simuler l'ajout, dans la table de routage, des annonces provenant de l'établissement d'un ou plusieurs liens et de voir l'impact que cela a sur la répartition du trafic et sur la qualité de cette table.

L'étape suivante est la génération de rapports qui permettent de rendre les résultats du simulateur facilement interprétables. Cette étape peut être entièrement personnalisée : les résultats bruts étant dans une base de données, générer les rapports à partir de ces données peut être réalisé de différentes manières. Ce sont les décideurs qui doivent demander les informations selon leur méthode préférée, mais nous conseillons d'utiliser le même type de rapport que celui que nous montrons dans ce travail, à savoir un rapport basé sur, tout d'abord, les graphiques des données les plus sensibles (répartition du trafic en fonction des routes et de leur longueur, nombre d'annonces en fonction de la longueur des routes annoncées, pourcentage cumulé du trafic en fonction de la longueur des routes), le tout en prenant la peine de comparer les résultats avec prepending et ceux sans prepending, car la différence peut apporter un élément de décision final si plusieurs candidats sont à égalité.

L'ensemble de ce travail propose donc une méthode complète, testée et validée pour permettre à un ISP de sélectionner ses fournisseurs internationaux. Cette solution a été implémentée chez Skynet sa à Bruxelles et a été effectivement utilisé pour prendre des décisions. Cette solution n'est certainement pas parfaite, mais pose un premier jalon pour permettre aux ISP de posséder des outils leur permettant de toujours choisir plus efficacement leurs interconnexions sur des données toujours plus concrètes et non plus sur uniquement des arguments marketing ou le *flair* de leurs ingénieurs réseau.

Nous mettons en avant dans ce travail une formule de comparaison des ISP, un format standard de route ainsi qu'un algorithme permettant de créer un simulateur de trafic. La formule de comparaison donne de bons résultats, mais devrait certainement pouvoir être améliorée en lui permettant d'intégrer de nouveaux paramètres. Le format de route est standard dans tout notre travail, mais est lié intimement au simulateur et aux données que nous voulions voir ressortir. Ce format n'est évidemment pas un standard reconnu, mais uniquement utilisé dans le cadre de ce travail. Quant au simulateur, son algorithme est très simple, mais son écriture beaucoup moins. Du fait du temps accordé à la réalisation du projet, le simulateur n'a pu être développé de manière à le rendre vraiment utilisable sans précautions et avec différents formats de route.

Les résultats obtenus ont été assez satisfaisant pour permettre de prendre une décision, mais ils pourraient être améliorés pour permettre un choix encore plus précis.

Aujourd'hui, l'outil a poursuivi son évolution au sein de Belgacom et est toujours utilisé pour négocier les contrats de peering. Si la base de l'outil n'a pas changé (le simulateur n'a pas été modifié, le format standard non plus et les règles d'interprétation sont restées valides), certains composants ont évolué. Ainsi, le collecteur de base a été réécrit en interne, la structure de la base de données à été affinée et les calculs d'agrégation révisés.

BIBLIOGRAPHIE

[And01] Andre Broido, and kc claffy. Internet Topology : connectivity of IP graphs. *SPIE International symposium on Convergence of It and Communication*, Septembre 2001. `http://www.caida.org/outreach/papers/2001/OSD/`.

[And02] Andre Broido, Evi Nemeth, and kc claffy. Interne expansion, refinement and churn. *European Transactions on Telecommunications*, January 2002. `http://www.caida.org/outreach/papers/2002/EGR/`.

[Bel] Belnet. `http://www.belnet.be`.

[Bég] Jean Bégin. Analyse quantitative en psychologie : Distribution de poisson. `http://www.er.uqam.ca/nobel/r30574/PSY1300/C5P10.html`. Dernier accès le 29 août 2003.

[Bra02] Bradley Huffaker, Marina Fomenkov, Daniel J. Plummer, David Moore and k claffy. Distance Metrics in the Internet, 2002. `http://www.caida.org/outreach/papers/2002/Distance/`.

[CAIa] CAIDA. cflowd : Traffic Flow Analysis Tool. `http://www.caida.org/tools/measurement/cflowd/`.

[CAIb] CAIDA. *FlowScan - Network Traffic Flow Visualization and Reporting Tool.* `http://www.caida.org/tools/utilities/flowscan/`.

[Cisa] Cisco. BGP Best Path Selection Algorithm. `http://www.cisco.com/warp/public/459/25.shtml`. Accédé le 26 Septembre 2003.

[Cisb] Cisco. `http://www.cisco.com`.

[D. 92] D. Estrin and Y. Rekhter and S. Hotz. RFC 1322 : A Unified Approach to Inter-Domain Routing, Mai 1992.

[Deb] Debian. `www.debian.org`.

[IAN04] IANA. Port numbers, 02 2004. `http://www.iana.org/assignments/port-numbers`.

[Ing01] Ing-wher Chen, Wen W. Chiang, Syed Adnan and Lucas Silacci. Geographically Speaking. University of California, San Diego, Winter 2001. `http://www.caida.org/analysis/geopolitical/geo-6.ps`.

[Int93] Internet Engineering Steering Group and R. Hinden. RFC 1517 : Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR) , Septembre 1993.

[IP] IP Infusion Inc. GNU Zebra . `http://www.zebra.org`.

[J. 96] J. Hawkinson, T. Bates. RFC 1930 : Guidelines for creation, selection, and registration of an Autonomous System (AS) , Mars 1996.

[Joh99] John W. Stewart III. *BGP4 Inter-Domain Routing in the Internet.* Addison-Wesley, 1999.

[Juna] Juniper. Selecting the Best Path (The BGP Path Decision Algorithm). `http://www.juniper.net/techpubs/software/erx/erx51x/swconfig-routing-vol2/html/bgp-config10.html`. Accédé le 28 Janvier 2004.

[Junb] Juniper. `http://www.juniper.net`.

[M. 93] M. Knopper, S. Richardson. RFC 1482 : Aggregation Support in the NSFNET Policy-Based Routing Database, Juin 1993.

[Mar] Mark Fullmer. flow-tools information. `http://www.splintered.net/sw/flow-tools/`.

[O. 03] O. Bonaventure (UCL), P. Trimintzios (University of Surrey), G. Pavlou (University of Surrey), B. Quoitin (FUNDP), A. Azcorra (UC3M), M. Bagnulo (UC3M) , P. Flegkas (University of Surrey), A. Garcia-Martinez(University of Surrey), P. Georgatsos(UC3M), L. Georgiadis(Algonet), C. Jacquenet(France Telecom), L. Swinnen(FUNDP), S. Tandel(FUNDP), S. Uhlig(UCL). Internet traffic engineering. *Quality of Future Internet Services*, COST263 final report, Springer LNCS 2856 :pp. 118–179, 2003.

[Ope91] Open Source Initiative. The GNU General Public License (GPL). `http://www.opensource.org/licenses/gpl-license.php`, 1991. Accédé le 29 août 2003.

[Per] Perl. `http://www.perl.org`.

[sea] searchNetworking.com. Définition du terme peer. `http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212768,00.html`.

[Sys] Cisco Systems. Netflow. `http://www.cisco.com/en/US/tech/tk648/tk362/tk812/tech_protocol_home.html`. Accédé le 28 Janvier 2004.

[Tob] Tobi Oetiker. About RRDtool. `http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/`. Accédé le 28 Janvier 2004.

[UB] Steve Uhlig and Olivier Bonaventure. The Macroscopic Behavior of Internet Traffic : a Comparative Study.

[V. 92] V. Jacobson, R. Braden, D. Borman. RFC 1323 : TCP Extensions for High Performance, Mai 1992.

[V. 93] V. Fuller, T. Li, J. Yu, K. Varadhan. RFC 1519 : Classless Inter-Domain Routing (CIDR) : an Address Assignment and Aggregation Strategy , Septembre 1993.

[V. 98] V. Paxson, G. Almes, J. Mahdavi, M. Mathis. RFC 2330 : Framework for IP Performance Metrics, May 1998.

[Y. 93] Y. Rekhter,T. Li. RFC 1518 : An Architecture for IP Address Allocation with CIDR , Septembre 1993.

[Y. 95a] Y. Rekhter, P. Gross. RFC 1772 : Application of the Border Gateway Protocol in the Internet, Mars 1995.

[Y. 95b] Y. Rekhter,T. Li. RFC 1771 : A Border Gateway Protocol 4 (BGP-4), Mars 1995.

FUNDP
Institut d'Informatique

Rue Grandgagnage, 21
B-5000 Namur Belgique

Comment un ISP peut mieux choisir ses fournisseurs d'accès grâce à BGP et à son trafic

Annexe

Christophe Ponsen

Promoteurs : J. Ramaekers et O. Bonaventure

Mémoire présenté pour l'obtention
du grade de
Maître en informatique

Année Académique 2003-2004

Table des matières

Table des figures

Chapitre 1

3 rapports complets

1.1 Rapport 1 : Trafic Skynet

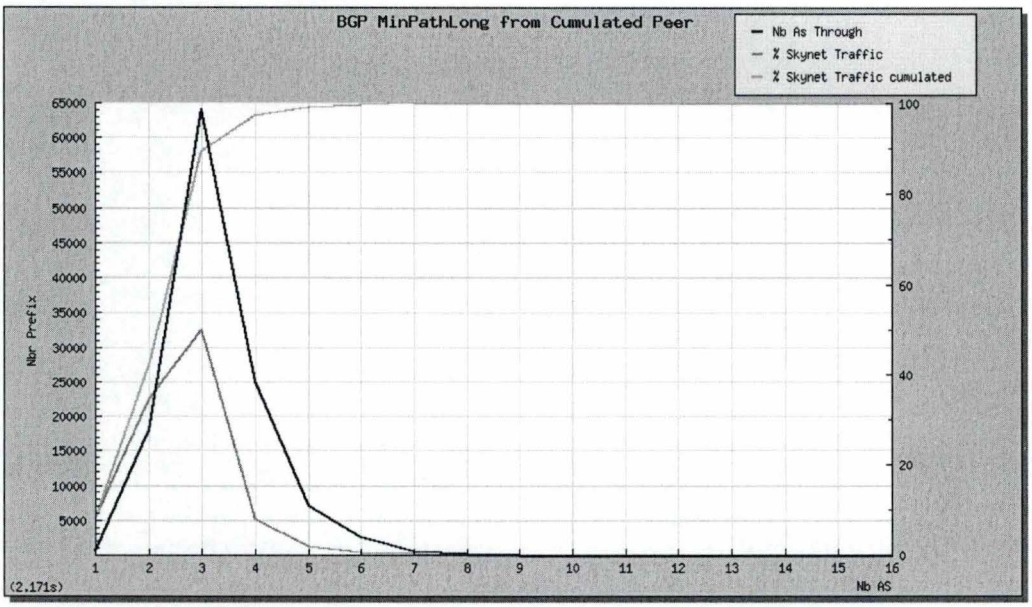

FIG. 1.1 – Nombre d'AS traversés et routes annoncées (avec prepending)

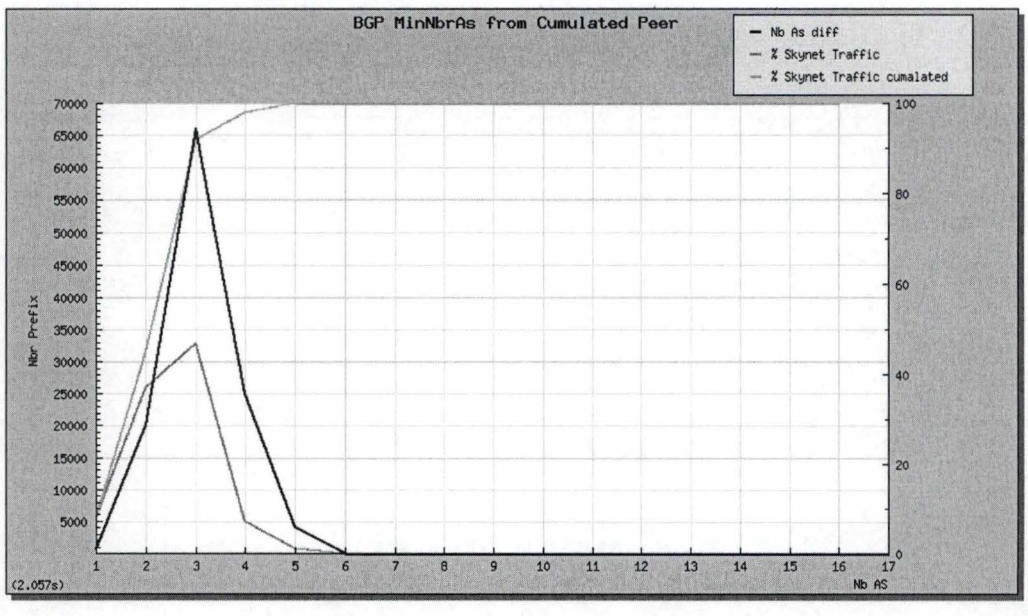

FIG. 1.2 – Nombre d'AS traversés et routes annoncées (sans prepending)

1.2 Rapport 2 : Trafic Skynet + un candidat

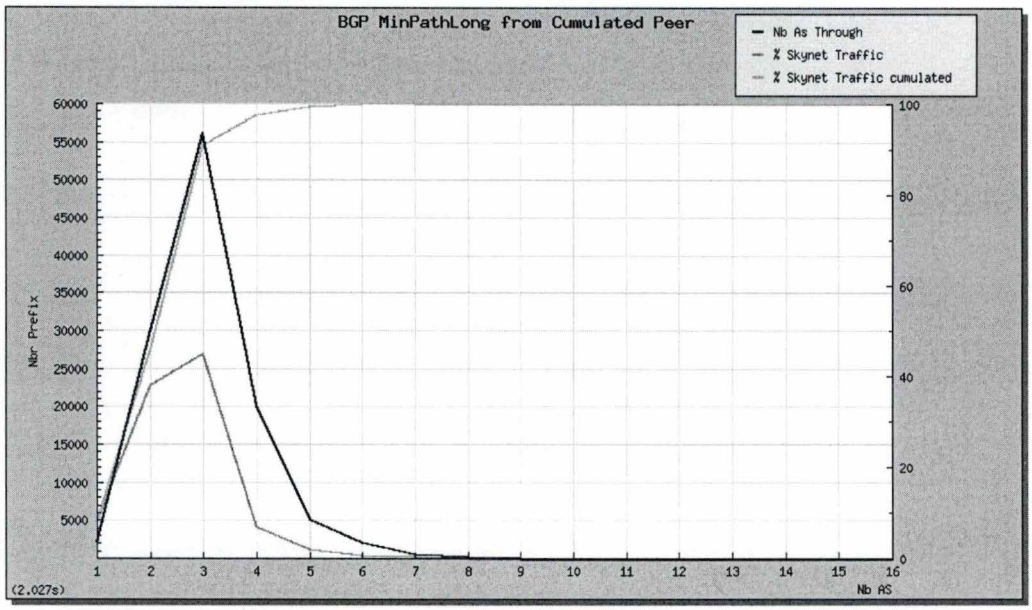

FIG. 1.3 – Nombre d'AS traversés et routes annoncées (avec prepending)

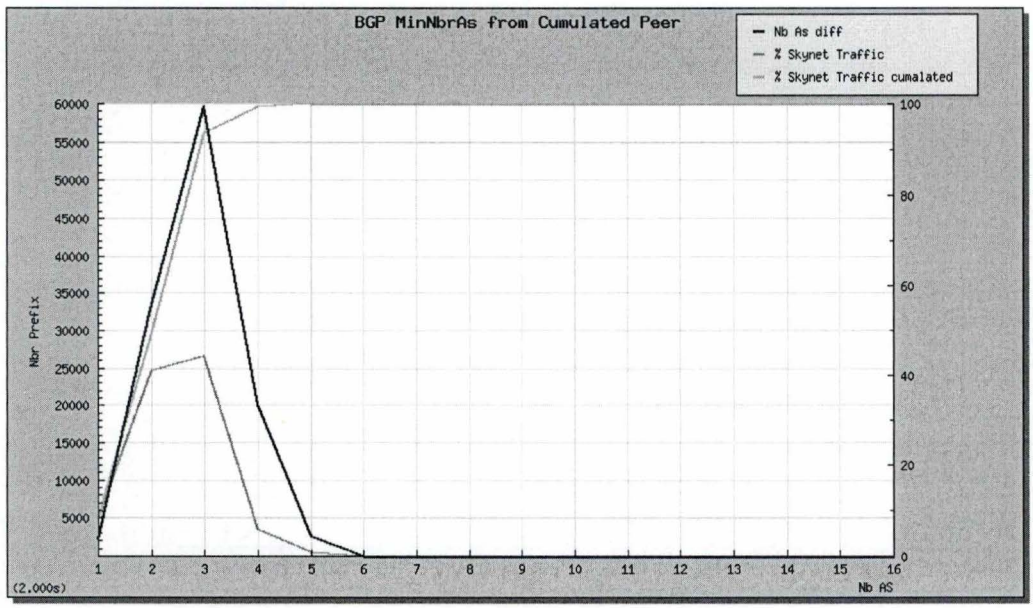

FIG. 1.4 – Nombre d'AS traversés et routes annoncées (sans prepending)

1.3 Rapport 3 : Trafic avec toutes les tables

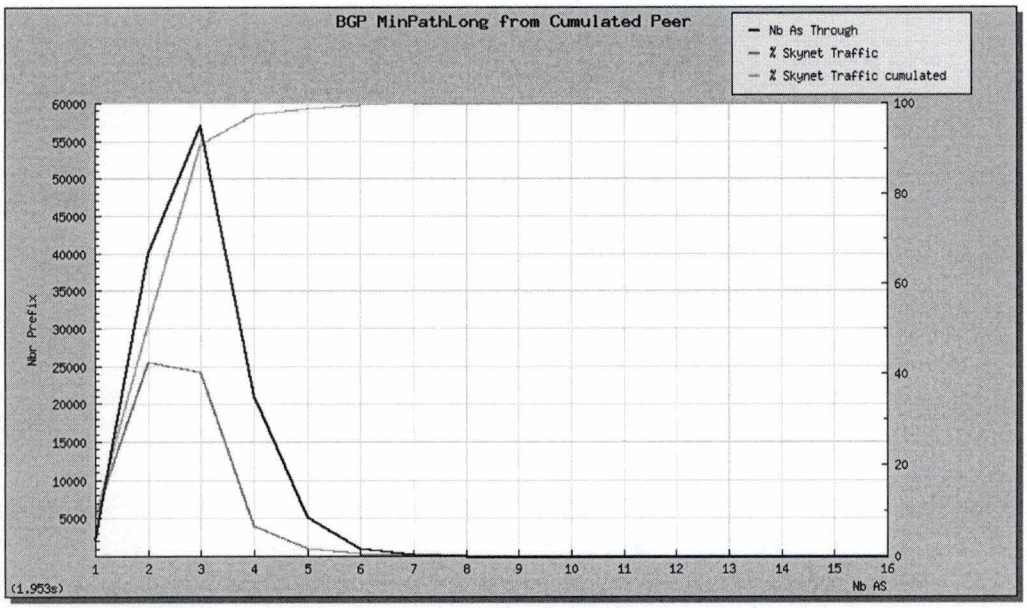

FIG. 1.5 – Nombre d'AS traversés et routes annoncées (avec prepending)

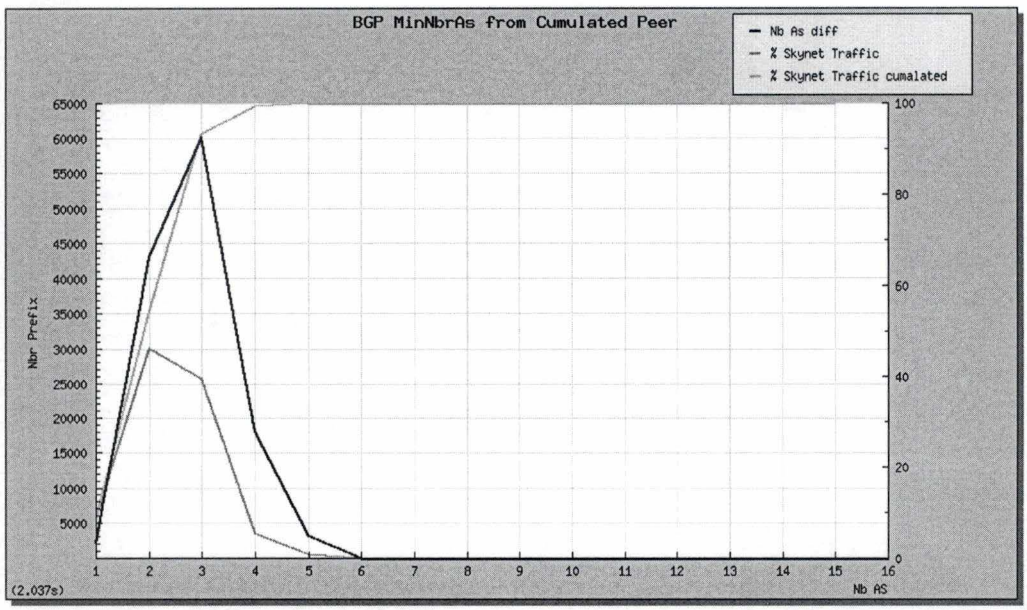

FIG. 1.6 – Nombre d'AS traversés et routes annoncées (sans prepending)

Chapitre 2

Comparaison des rapports

2.1 Skynet Vs Skynet + un candidat

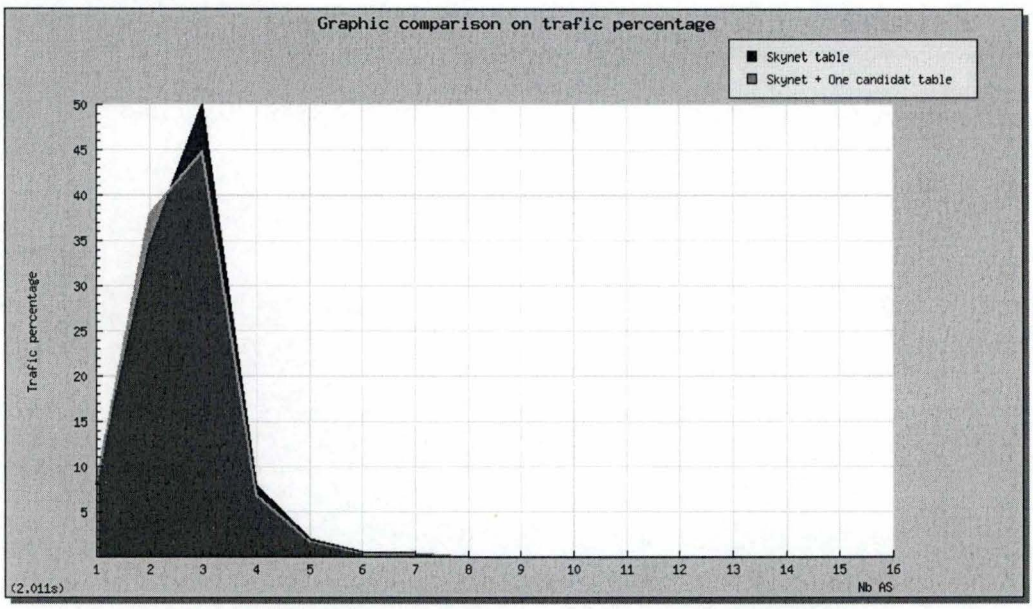

FIG. 2.1 – Comparaison des pourcentages de trafic (Skynet-Skynet+1Candidat) (avec prepending)

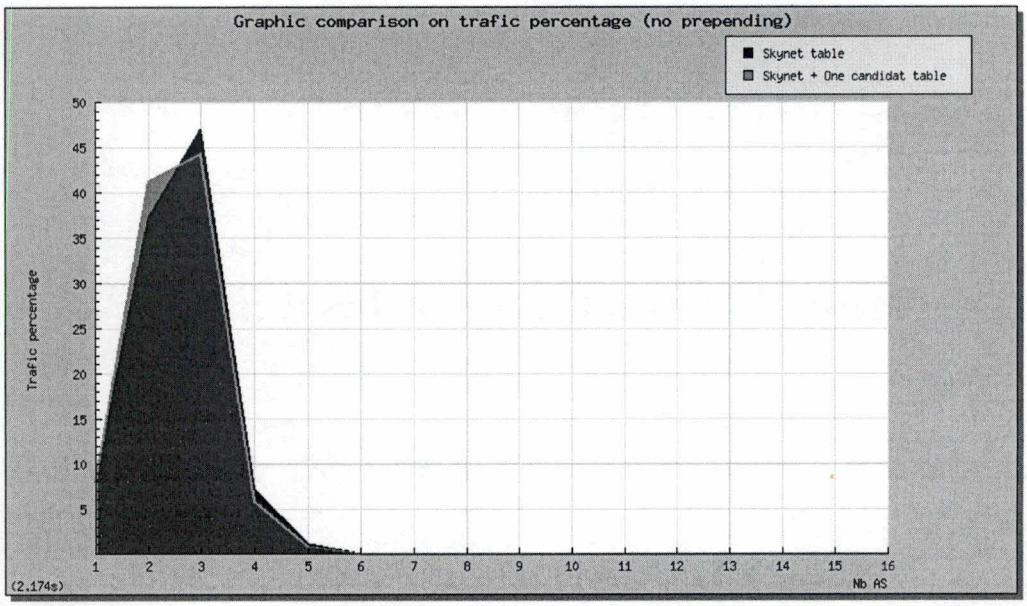

FIG. 2.2 – Comparaison des pourcentages de trafic (Skynet-Skynet+1Candidat) (sans prepending)

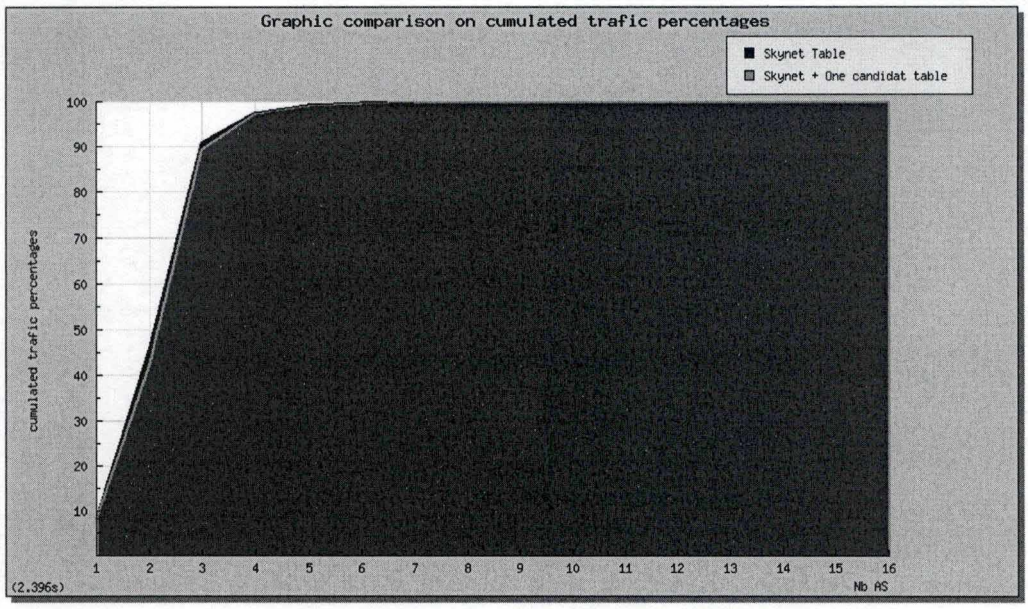

FIG. 2.3 – Comparaison des pourcentages de trafic (Skynet-Skynet+1Candidat) (avec prepending)

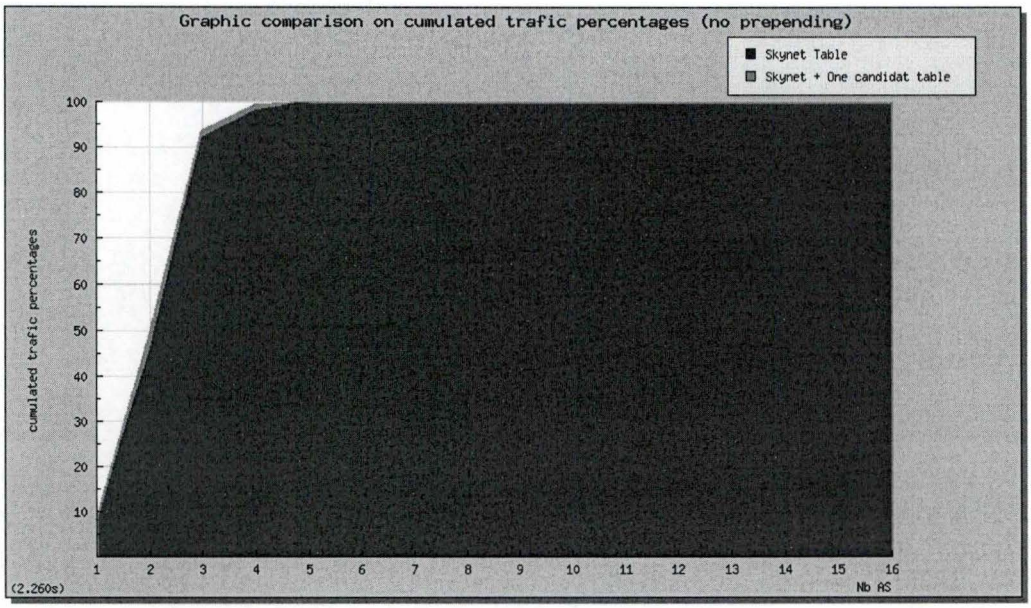

FIG. 2.4 – Comparaison des pourcentages de trafic (Skynet-Skynet+1Candidat) (sans prepending)

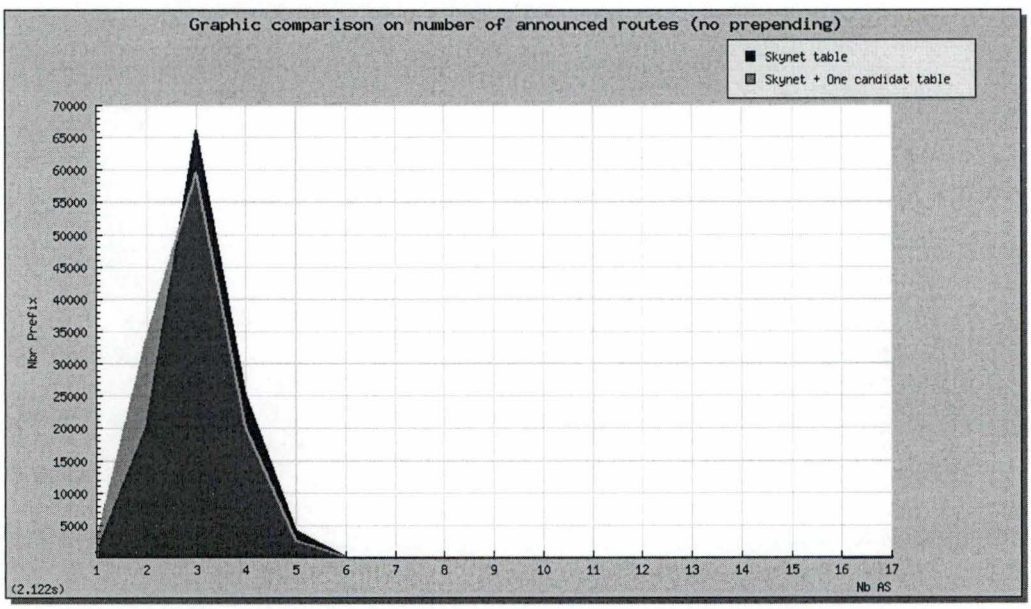

FIG. 2.5 – Comparaison du nombre de routes annoncées (Skynet-Skynet+1Candidat) (sans prepending)

2.2 Skynet + un candidat Vs toutes les tables

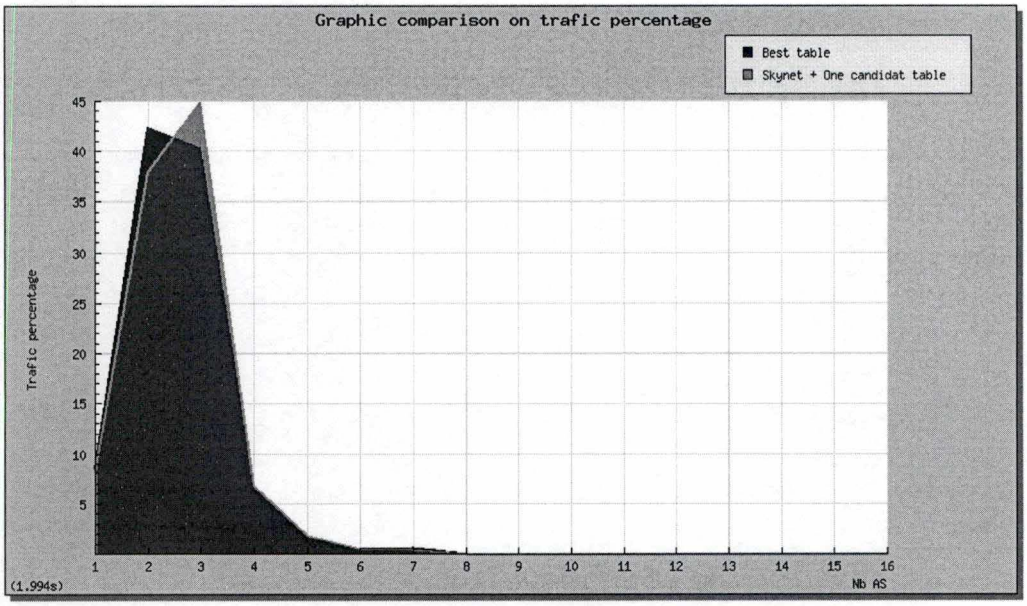

FIG. 2.6 – Comparaison des pourcentages de trafic (Skynet+1candidat - Best) (avec prepending)

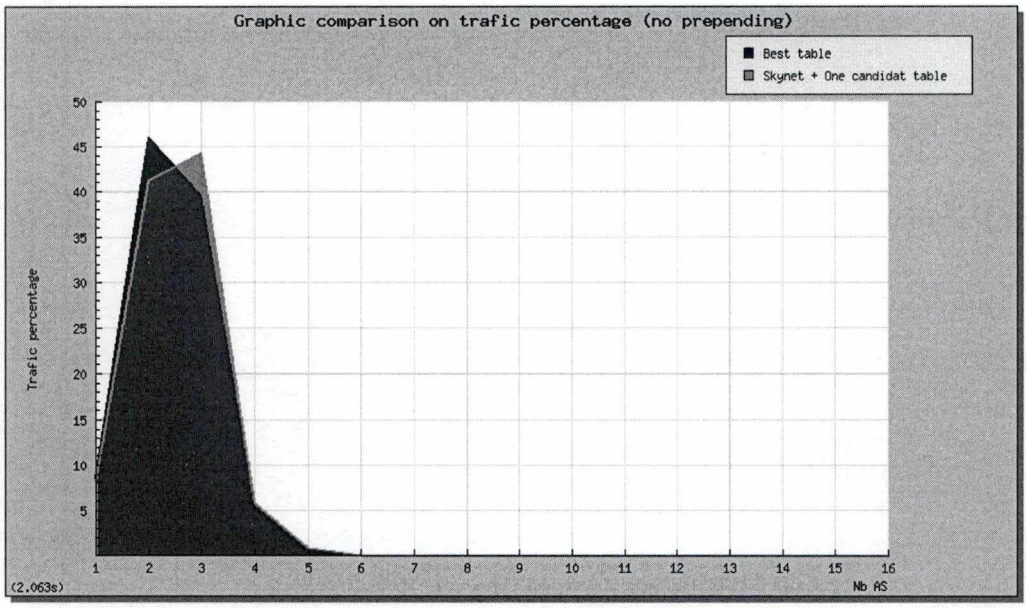

FIG. 2.7 – Comparaison des pourcentages de trafic (Skynet+1candidat - Best) (sans prepending)

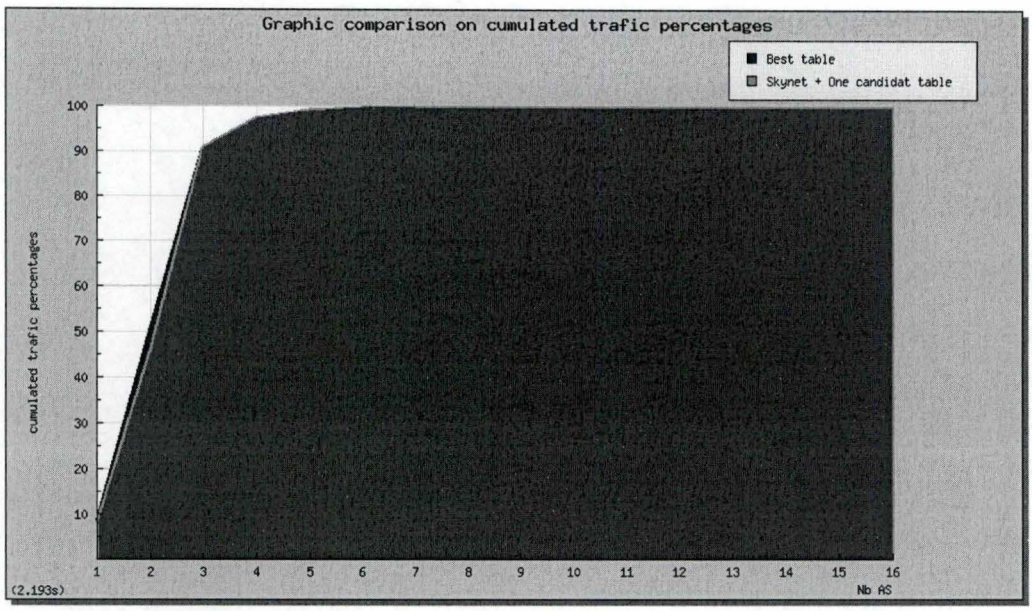

FIG. 2.8 – Comparaison des pourcentages de trafic (Skynet+1candidat - Best) (avec prepending)

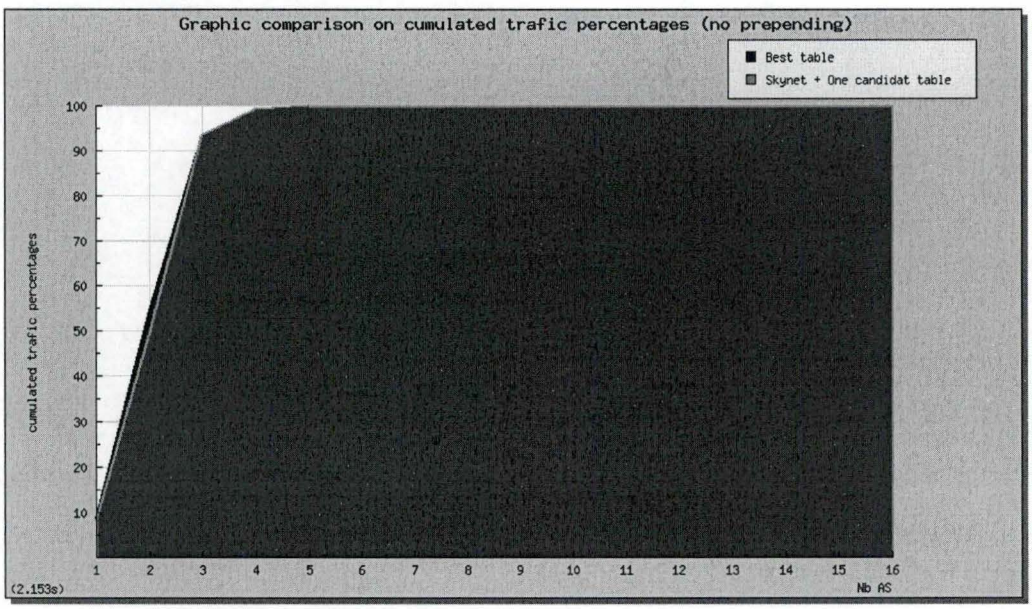

FIG. 2.9 – Comparaison des pourcentages de trafic (Skynet+1candidat - Best) (sans prepending)

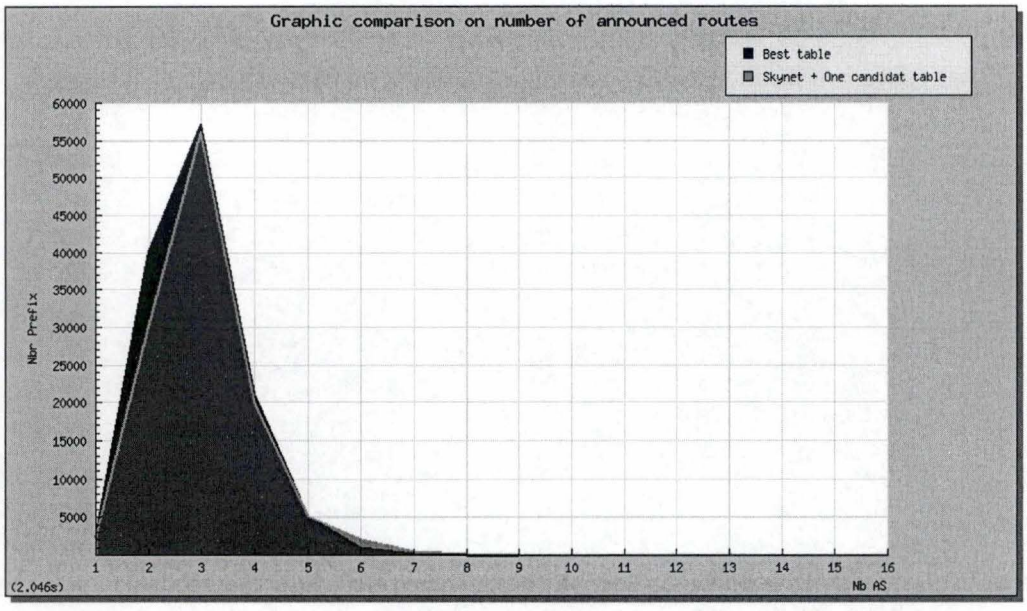

FIG. 2.10 – Comparaison du nombre de routes annoncées (Skynet+1candidat - Best) (avec prepending)

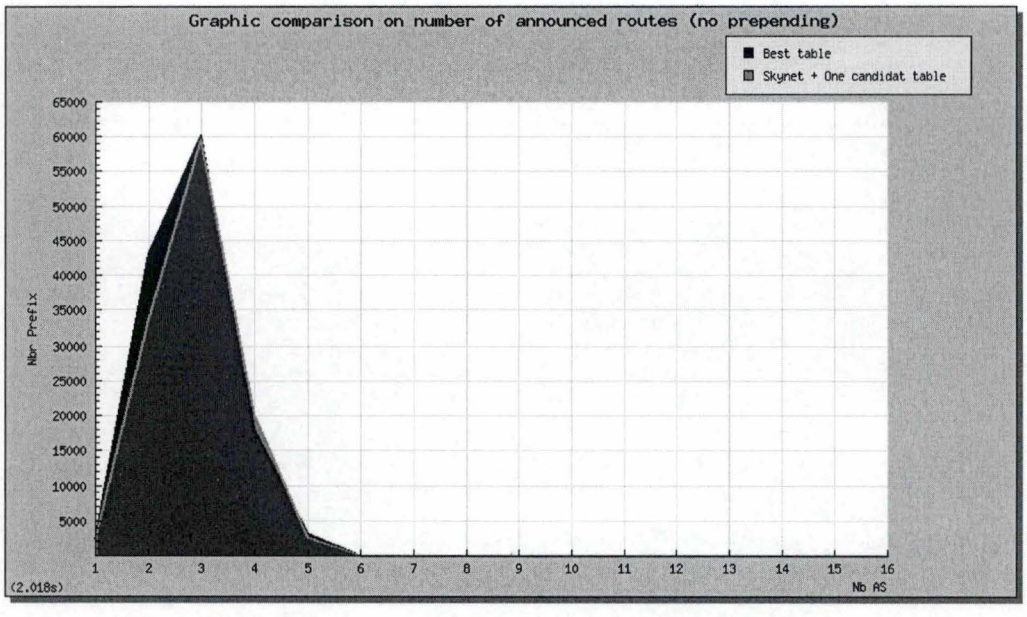

FIG. 2.11 – Comparaison du nombre de routes annoncées (Skynet+1candidat - Best) (sans prepending)

Chapitre 3

Base de données

3.1 Base de donnée complète BGP

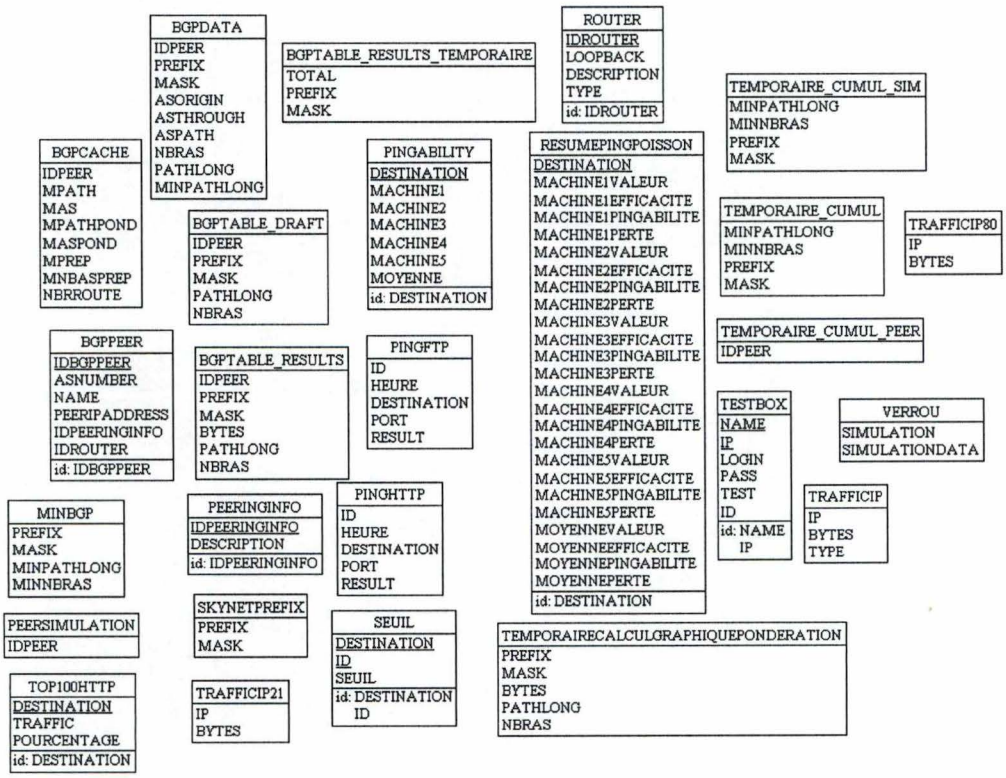

FIG. 3.1 – Ensemble des tables de la base BGP

3.2 Base de donnée complète du trafic

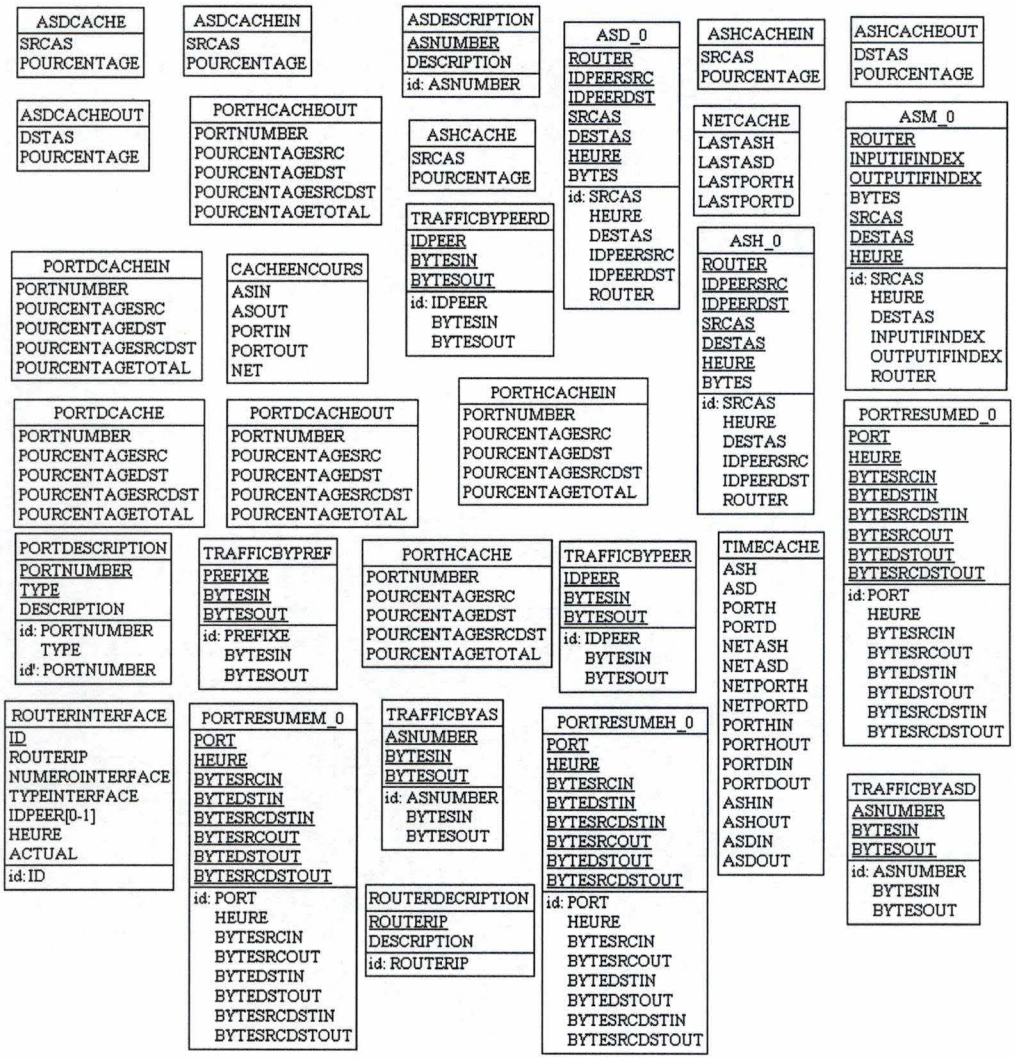

FIG. 3.2 – Ensemble des tables de la base de trafic

Chapitre 4

Code source du site WEB

Remarque : D'une manière générale, toute information contenant des données de type login, password ou permettant d'identifier un routeur ou une machine sur le réseau Skynet seront supprimée des codes sources. Si par ailleur, une telle information venait à être quand même présente dans un fichier, le lecteur ne pourra en aucun cas se servir de cette information.

4.1 Code PHP

Fichier : index.php

```
<?

require "lib/Cricket.php";

Entete2("");
print "<CENTER>";
print "<a href='bgp.php'>Sky BAT</a>";
print "<br><br>";
print "<a href='net.php'>Sky ITM</a>";
print "</center>";
Pied2("");

?>
```

Fichier : bgp.php

```
<?PHP
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Cricket.php";
require "./lib/Whois.php";
require "./lib/Network.php";

# QUERY
Entete2("Sky BAT");

$dbh=ConnectMysql();

$query = "select unix_timestamp(Now()) as timenow";
$result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
```

```
16 $row=mysql_fetch_object($result);
   $timenow = $row->timenow;
18 ?>
   <H3>Welcome on the HomePage of Sky BAT (BGP Analyses Tool)</H3>
20 <br>
   <a href="displaysim.php">Latest Simulation</a><br>
22 <br>
   <a href="controlsimul.php">New Simulation</a><br>
24 <br>
   <a href="bgpselect.php">General Bgp Informations</a><br>
26 <br>
   <br>
28 <a href="index.php">Back</a><br>

30 <?
   Pied2("");
32 mysql_close($dbh);
   ?>
```

Fichier : net.php

```
   <?PHP
 2 require "./lib/Html.php";
   require "./lib/Mysql.php";
 4 require "./lib/Cricket.php";
   require "./lib/Whois.php";
 6 require "./lib/Network.php";

 8 # QUERY
   Entete2("Sky ITM");
10
   $dbh=ConnectMysql();
12
   $query = "select unix_timestamp(Now()) as timenow";
14 $result = mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
16 $row=mysql_fetch_object($result);
   $timenow = $row->timenow;
18 $D =0;
   $H = 0;
20
   $query="select net from cacheEnCours";
22 $result = mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
24 $row = mysql_fetch_object($result);
   if($row->net == 1) {
26    print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
      flush();
28    while($row->net == 1) {
         $result = mysql_query($query)
30          or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
         $row = mysql_fetch_object($result);
32    }
      $H = 0;
34    $D = 0;
   }
36
   $query = "select  netasH,
38                   netasD,
                     netportH,
40                   netportD,
                     DATE_FORMAT(from_unixtime(netasH),'%d/%m/%y %T') as heure1,
42                   DATE_FORMAT(from_unixtime(netasD),'%d/%m/%y %T') as heure2
          from timeCache";
44 $result = mysql_query($query)
           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
46
```

```
$row=mysql_fetch_object($result);
$netportD = $row->netportD;
$netportH= $row->netportH;
$netasD = $row->netasD;
$netasH = $row->netasH;
$lastCacheH = $row->heure1;
$lastCacheD = $row->heure2;

mysql_free_result($result);

if(($timenow - $netportD) > 21600 || ($timenow - $netasD) > 21600) {
   $D = 1;
}
if(($timenow - $netasH) > 7200 || ($timenow - $netportH) > 7200) {
   $H = 1;
}
$query="select net from cacheEnCours";
$result = mysql_query($query)
   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
if($row->net == 1) {
   print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
   flush();
   while($row->net == 1) {
      $result = mysql_query($query)
         or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
   }
   $H = 0;
   $D = 0;
}
if($H ==1 || $D ==1 ) {
   $query = "update cacheEnCours set net = 1";
   $result = mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

   $asdupdate = 0;
   $asupdateunix = 0;
   $asupdate = 0;
   $asdupdateunix=0;
   $portupdate = 0;
   $portupdateunix=0;
   $portdupdate = 0;
   $portdupdateunix = 0;
   $maxtime = 0;
   $maxtimeunix = 0;
   if($H==1) {
      for($boucle=0;$boucle<48;$boucle++) {
         $query="select     DATE_FORMAT(from_unixtime(max(heure)),'%d/%m/%y %T') as heure1,
                    max(heure) as heure
               from asH_".$boucle."";
         $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
         $row=mysql_fetch_object($result);
         if($row->heure && (($asupdateunix < $row->heure) || $boucle == 0) ) {
            $asupdate = $row->heure1;
            $asupdateunix = $row->heure;
         }
         mysql_free_result($result);

         $query="select     DATE_FORMAT(from_unixtime(max(heure)),'%d/%m/%y %T') as heure1,
                    max(heure) as heure from portResumeH_".$boucle."";
         $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
         $row=mysql_fetch_object($result);
         if($row->heure && (($portupdateunix < $row->heure) || $boucle == 0) ) {
            $portupdate = $row->heure1;
```

```
114             $portupdateunix = $row->heure;
                }
116         }
        }
118     if($D == 1) {
            for($boucle=0;$boucle<7;$boucle++) {
120
                $query="select      DATE_FORMAT(from_unixtime(max(heure)),'%d/%m/%y %T') as heure1,
122                         max(heure) as heure
                        from asD_".$boucle."";
124             $result = mysql_query($query)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
126             $row=mysql_fetch_object($result);
                if($row->heure && (($asdupdateunix < $row->heure) || $boucle == 0) ) {
128                 $asdupdate = $row->heure1;
                    $asdupdateunix = $row->heure;
130             }
                mysql_free_result($result);
132
                $query="select      DATE_FORMAT(from_unixtime(max(heure)),'%d/%m/%y %T') as heure1,
134                         max(heure) as heure
                        from portResumeD_".$boucle."";
136             $result = mysql_query($query)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
138             $row=mysql_fetch_object($result);
                if($row->heure && (($portdupdateunix < $row->heure) || $boucle == 0) ) {
140                 $portdupdate = $row->heure1;
                    $portdupdateunix = $row->heure;
142             }
                mysql_free_result($result);
144         }
        }
146
        if($H == 1) {
148         $query = "update netCache
                        set lastasH=unix_timestamp('".$asupdate."'),
150                         lastportH=unix_timestamp('".$portupdate."')";
            $result = mysql_query($query)
152                         or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

154         $query = "update timeCache
                        set netasH = ".$timenow.",
156                         netportH = ".$timenow."";
            $result = mysql_query($query)
158                         or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        }
160     if($D == 1) {
            $query = "update netCache
162                     set lastasD=unix_timestamp('".$asdupdate."'),
                            lastportD=unix_timestamp('".$portdupdate."')";
164         $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
166
            $query = "update timeCache
168                     set netasD=".$timenow.",
                            netPortD=".$timenow."";
170         $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
172     }
        $query = "update cacheEnCours set net = 0";
174     $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
176 }

178 $query = "   select    DATE_FORMAT(from_unixtime(netasH),'%d/%m/%y %T') as heure1,
                    DATE_FORMAT(from_unixtime(netasD),'%d/%m/%y %T') as heure2
180         from timeCache";
```

```
$result = mysql_query($query)
182    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
184 $lastCacheD = $row->heure2;
$lastCacheH = $row->heure1;
186


188
$query = "
190    select
          DATE_FORMAT(from_unixtime(lastasH),'%d/%m/%y %T') as netasH,
192       DATE_FORMAT(from_unixtime(lastasD),'%d/%m/%y %T') as netasD,
          DATE_FORMAT(from_unixtime(lastportH),'%d/%m/%y %T') as netportH,
194       DATE_FORMAT(from_unixtime(lastportD),'%d/%m/%y %T') as netportD
       from netCache";
196 $result = mysql_query($query)
       or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
198 $row=mysql_fetch_object($result);
$netportD2 = $row->netportD;
200 $netportH2= $row->netportH;
$netasD2 = $row->netasD;
202 $netasH2 = $row->netasH;

204 mysql_free_result($result);
?>
206 <H2>Welcome on the Home Page of SkyITM</h2><br>
<center>Using Netflow data and cflowd collector</center><br>
208 <br><br>
<a href="netas2in.php"> click here to see AS monitoring (entrance traffic)</a><br>
210 <a href="netas2out.php"> click here to see AS monitoring (leaving traffic)</a><br>
<br>
212 <a href="netport2in.php"> click here to see Port monitoring (entrance traffic)</a><br>
<a href="netport2out.php"> click here to see Port monitoring (leaving traffic)</a><br>
214 <br>
<a href="drawbgppeer.php">Click here to see the Repartition of Traffic by Peer</a>
216 <br>
<br>
218 <br>
<?
220 print "Last AsH Update:".$netasH2."<br>";
print "Last PortH Update: ".$netportH2."<br>";
222 print "Last AsD Update:".$netasD2."<br>";
print "Last PortD Update: ".$netportD2."<br>";
224 print "<br>";
print "<center>Cache: H=2H, D=6H.  Last Cache: H: $lastCacheH D:$lastCacheD
226       </center><br><br>";
?>
228 <table width="100%" cellspacing="0" cellpadding="0" align="center">
<tr>
230    <td><a href="gestionrouter.php">Routers Management</a></td>
       <td><a href="topTraffic.php">Top 100 IP Traffic in (/24)</a></td>
232    <td><a href="top100TrafficFtp.php">Top 100 IP Traffic in (FTP)</a></td>
       <td><a href="top100TrafficHttp.php">Top 100 IP Traffic in (HTTP)</a></td>
234 </tr>
</table>
236 <br>
<a href="index.php">Back</a><br>
238 <?
Pied2("");
240 mysql_close($dbh);
?>
```

Fichier : router.php

```
<?
2
/*
```

```
4 Fichier contenant les fonction getSelectRouter et getSelectRouter2

6 getSelectRouterin() retourne la liste (une chaîne de caractères) des routeurs
  et de leurs interfaces pour un select du traffic entrant
8
  getSelectRouterin2() retourne la liste (un tableau) des routeurs et de
10 leurs interfaces (traffic entrant)

12 getSelectRouterout() retourne la liste (une chaîne de caractères) des routeurs
  et de leurs interfaces pour  select du traffic sortant
14
  getSelectRouterout2() retourne la liste (un tableau) des routeurs et
16 de leurs interfaces (traffic sortant)
  */
18
  function getSelectRouterin() {
20    $dbh=ConnectMysql(); //connection à la base de données

22    $queryrouter = 'select distinct routerip
                from routerinterface
24              where typeinterface ="I"
                   or typeinterface ="B"
26              order by routerip';
      $resultrouter = mysql_query($queryrouter)
28       or die ('Query failed :'.$queryrouter.'<br> message:'.mysql_error($dbh));
      $boucle = 0;
30    $boucleint = 0;
      while ($rowrouter = mysql_fetch_object($resultrouter)) {
32       //garni le tableau router[] ainsi que interface []
         $router[$boucle] = $rowrouter->routerip;
34       $queryinterface = '  select distinct idpeer
                      from routerinterface
36                    where (routerip = "'.$router[$boucle].'"
                         and typeinterface="I")
38                       or (routerip = "'.$router[$boucle].'"
                         and typeinterface = "B")';
40       $resultinterface = mysql_query($queryinterface)
            or die ('Query failed :'.$queryinterface.'<br> message:'.mysql_error($dbh));
42       while($rowinterface = mysql_fetch_object($resultinterface)) {
            $interface[$boucleint][0] = $rowinterface->idpeer;
44          $boucleint++;
         }
46       mysql_free_result($resultinterface);
         $boucle++;
48    }

50    mysql_free_result($resultrouter);

52    $boucleint=0;
      $routerselect="";
54    while($interface[$boucleint]) {
         if($boucleint == 0)
56          $routerselect.= ' idpeersrc in ('.$interface[$boucleint][0];
         else
58          $routerselect.= ','.$interface[$boucleint][0];
         $boucleint++;
60    }
      $routerselect .= ')';
62    return $routerselect;
  }
64

66 function getSelectRouterIndicein($indice) {
      $dbh=ConnectMysql(); //connection à la base de données
68
      $queryrouter = 'select distinct routerip
70                from routerinterface
```

```
                where typeinterface ="I"
72                 or typeinterface ="B"
                order by routerip';
74    $resultrouter = mysql_query($queryrouter)
         or die ('Query failed :'.$queryrouter.'<br> message:'.mysql_error($dbh));
76    $boucle = 0;
      while ($rowrouter = mysql_fetch_object($resultrouter)) {
78       //garni le tableau router[] ainsi que interface []
         $router[$boucle] = $rowrouter->routerip;
80       $queryinterface = '  select    numerointerface,
                              typeinterface
82                      from routerinterface
                        where (routerip = "'.$router[$boucle].'"
84                         and typeinterface="I")
                           or (routerip = "'.$router[$boucle].'"
86                         and typeinterface = "B")';
         $resultinterface = mysql_query($queryinterface)
88          or die ('Query failed :'.$queryinterface.'<br> message:'.mysql_error($dbh));
         $boucleint = 0;
90       while($rowinterface = mysql_fetch_object($resultinterface)) {
            $interface[$boucle][$boucleint][0] = $rowinterface->numerointerface;
92          $interface[$boucle][$boucleint][1] = $rowinterface->typeinterface;
            $boucleint++;
94       }
         mysql_free_result($resultinterface);
96       $boucle++;
      }
98
      mysql_free_result($resultrouter);
100
      $boucle=0;
102   $routerselect="";
      while($router[$boucle]){
104      $boucleint = 0;
         if($boucle==0)
106         $routerselect.= '('.$indice.'.router = "'.$router[$boucle].'"
                        and '.$indice.'.inputifindex in (';
108      else
            $routerselect.= ')) or ('.$indice.'.router = "'.$router[$boucle].'"
110                     and '.$indice.'.inputifindex in (';
         while($interface[$boucle][$boucleint]) {
112         if($boucleint == 0)
               $routerselect.= $interface[$boucle][$boucleint][0];
114         else
               $routerselect.= ','.$interface[$boucle][$boucleint][0];
116
            $boucleint++;
118      }

120      $boucle++;
      }
122   $routerselect .= '))';
      return $routerselect;
124 }

126 function getSelectRouterin2 () {

128   $dbh=ConnectMysql(); //connection à la base de données

130   $queryrouter = 'select distinct routerip
                from routerinterface
132             where typeinterface ="I"
                   or typeinterface ="B"
134             order by routerip';
      $resultrouter = mysql_query($queryrouter)
136      or die ('Query failed :'.$queryrouter.'<br> message:'.mysql_error($dbh));
      $boucle = 0;
```

```
138     while ($rowrouter = mysql_fetch_object($resultrouter)) {
            //garni le tableau router[] ainsi que interface []
140         $router[$boucle] = $rowrouter->routerip;
            $queryinterface = '  select    numerointerface,
142                              typeinterface
                        from routerinterface
144                     where (routerip = "'.$router[$boucle].'"
                           and typeinterface="I")
146                        or (routerip = "'.$router[$boucle].'"
                           and typeinterface = "B");
148         $resultinterface = mysql_query($queryinterface) '
               or die ('Query failed :'.$queryinterface.'<br> message:'.mysql_error($dbh));
150         $boucleint = 0;
            while($rowinterface = mysql_fetch_object($resultinterface)) {
152            $interface[$boucle][$boucleint][0] = $rowinterface->numerointerface;
               $interface[$boucle][$boucleint][1] = $rowinterface->typeinterface;
154            $boucleint++;
            }
156         mysql_free_result($resultinterface);
            $boucle++;
158     }

160     mysql_free_result($resultrouter);

162     $boucle=0;
        $sommeBytesTotal =0;
164     while($router[$boucle]) {
            $boucleint = 0;
166         $routerselect2[$boucle] .= 'router = "'.$router[$boucle].'"
                    and inputifindex in (';
168         while($interface[$boucle][$boucleint]) {
               if($boucleint == 0)
170               $routerselect2[$boucle].= $interface[$boucle][$boucleint][0];
               else
172               $routerselect2[$boucle].= ','.$interface[$boucle][$boucleint][0];

174            $boucleint++;
            }
176         $routerselect2[$boucle].= ')';
            $boucle++;
178     }
        return $routerselect2;
180 }

182
    function getSelectRouterout() {
184     return "idpeersrc = 5432";
    }
186 ?>
```

Fichier : netas2in.php

```
    <?PHP
 2  require "./lib/Html.php";
    require "./lib/Mysql.php";
 4  require "./lib/Cricket.php";
    require "./lib/Whois.php";
 6  require "./lib/Network.php";
    $timedebut = time();
 8  require "router.php";
    $routerselect = getSelectRouterin();
10  // Variables
    // $portlist Contient la liste des ports du hit parade
12  // $port [] [0] contient le numero du port
    // $port [] [1] contient la description du port
14  // $port [] [2] contient le total du traffic du port par router
    // $port [] [3] contient l'ip du routeur selectionné
```

```
16
   // $router[] contient la liste des routeurs dans la base
18 // $interface [numero routeur] [X] [0] contient le numéro
   // de l'interface X du [numero routeur] voir le tableau $router[]
20 // $routerselect = chaine contenant le "where" d'un select construit sur
   //              base des données de la base
22 //
   // $sommeBytesTotal = total du trafic du port courant;
24 //
   // $queryXXXX, $resultXXXXX et $rowXXXX servent de variable
26 // temporaire aux requêtes XXXX
   //
28 // $port [X] contient la liste des hit parade des ports, en ordre croissant
   //
30 //ATTENTION: Du à la présence de l'élément 0 dans le tableau,
   //on ne peut utiliser le while(port []) car le 0 est considéré comme faux !
32 //on utilisera un for each ou un for(sizeof).
   //
34 //
   //
36
   Entete2("Vue du traffic par AS");
38
   $query="select asIn from cacheEnCours";
40 $result = mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
42 $row = mysql_fetch_object($result);
   if($row->asIn == 1) {
44    print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
      flush();
46    while($row->asIn == 1) {
         $result = mysql_query($query)
48          or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
         $row = mysql_fetch_object($result);
50    }
   }
52

54 if(!isset($seuil)) {
      $seuil = 1;
56 }

58 # QUERY
   // Traffic aggrégé en 48 H (par 5 minutes)
60
   $dbh=ConnectMysql(); //connection à la base de données
62 $query = "select count(*) as total from ashCacheIn";
   $result = mysql_query($query) or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
64 '.$query.'<br>');
   $row = mysql_fetch_object($result);
66 $nombreDataCacheH = $row->total;

68 $query = "select count(*) as total from asdCacheIn";
   $result = mysql_query($query) or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
70 '.$query.'<br>');
   $row = mysql_fetch_object($result);
72 $nombreDataCacheD = $row->total;

74 $query = "select asHIn,asDIn,unix_timestamp(now()) as timenow from timeCache";
   $result = mysql_query($query)
76    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
   $row = mysql_fetch_object($result);
78 $timeCacheH = $row->asHIn;
   $timeCacheD = $row->asDIn;
80 $timeNow = $row->timenow;

82 $doCacheH = 0;
```

```
$doCacheD = 0;

if($nombreDataCacheH == 0 || ($timeNow - $timeCacheH)>=21600) {
    $doCacheH = 1;
}
if($nombreDataCacheD == 0 || ($timeNow - $timeCacheD)>=43200) {
    $doCacheD = 1;
}

$query="select * from ashCacheIn where pourcentage >".$seuil."";
$query="select * from asdCacheIn where pourcentage >".$seuil."";

$query="select asIn from cacheEnCours";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
if($row->asIn == 1) {
    print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
    flush();
    while($row->asIn == 1) {
        $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        $row = mysql_fetch_object($result);
    }
    $doCacheH = 0;
    $doCacheD = 0;
}

if($doCacheH == 1) {
    $query = "update cacheEnCours set asIn = 1";
    $result = mysql_query($query)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');

    print ("<H3>Cache under construction (5 min AGG)</H3><br>");
    flush();
    $sommeBytesTotal = 0;

    $query2='truncate table ashCacheIn';
    $result2 = mysql_query($query2)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');

    // Somme Traffic entrant
    for($boucle=0;$boucle<48;$boucle++) {
        $query = 'select sum(bytes) as total from asH_'.$boucle.' where '.$routerselect.'';
        $result = mysql_query($query)
            or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
".mysql_error($dbh)."<br>");
        $row=mysql_fetch_object($result);
        $sommeBytesTotal += $row->total;
        mysql_free_result($result);
    }

    // Récupérationde l'ensemble des données sur les as
    // Utilisation d'un tableau (indice = as)

    for($boucle=0;$boucle<48;$boucle++) {

        $query = '  select    srcas,
                        sum(bytes) as total
                FROM  asH_'.$boucle.'
                where '.$routerselect.'
                group by srcas';

        $result = mysql_query($query)
                or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
'.$query.'<br>');
        while($row=mysql_fetch_object($result)) {
```

```
150             $cle = "'".$row->srcas."'";
                $as[$cle] += $row->total;
152         }
            mysql_free_result($result);
154     }
        //print_r($as);
156     $nombreelement = count($port);

158     //Creation du tableau des totaux pour le tri
        for($boucle=0;$boucle<$nombreelement;$boucle++) {
160         $cle = "'".$boucle."'";
            if(!$as[$cle]) {
162             $as[$cle] = 0;
            }
164     }
        //Triage du tableau des résultats
166     flush();
        arsort($as,SORT_NUMERIC);
168     reset($as);
        flush();
170     $totalboucle = 0;
        while(( list($key,$value)= each($as))) {
172         $cle = str_replace("'","",$key);
            $pourcentage = ($value/$sommeBytesTotal)*100;
174         $query = "insert into ashCacheIn values (".$cle.",".$pourcentage.")";
            $result = mysql_query($query)
176                 or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
    '.$query.'<br>');
178     }
        $query = "update timeCache set asHIn = ".$timeNow."";
180     mysql_query($query)
            or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");
182     if($doCacheD == 0) {
            $query = "update cacheEnCours set asIn = 0";
184         $result = mysql_query($query)
                or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
186     }
    }
188 if($doCacheD == 1) {
        if($doCacheH == 0) {
190         $query = "update cacheEnCours set asIn = 1";
            $result = mysql_query($query)
192             or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
        }
194     print ("<H3>Cache under construction (1H AGG)</H3><br>");
        flush();
196     $sommeBytesTotal = 0;
        unset($as);
198     $query2='truncate table asdCacheIn';
        $result2 = mysql_query($query2)
200         or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
        // Somme Traffic entrant
202     for($boucle=0;$boucle<7;$boucle++) {
            $query = 'select sum(bytes) as total from asD_'.$boucle.' where '.$routerselect.'';
204         $result = mysql_query($query)
                or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
206 ".mysql_error($dbh)."<br>");
            $row=mysql_fetch_object($result);
208         $sommeBytesTotal += $row->total;
            mysql_free_result($result);
210     }

212     // Récupérationde l'ensemble des données sur les as
        // Utilisation d'un tableau (indice = as)
214
        for($boucle=0;$boucle<7;$boucle++) {
216
```

```
        $query = '  select    srcas,
218                     sum(bytes) as total
                FROM  asD_'.$boucle.'
220             where     '.$routerselect.'
                group by srcas';
222
        $result = mysql_query($query)
224             or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
    '.$query.'<br>');
226     while($row=mysql_fetch_object($result)) {
           $cle = "'".$row->srcas."'";
228        $as[$cle] += $row->total;
        }
230     mysql_free_result($result);
    }
232 $nombreelement = count($port);

234 //Creation du tableau des totaux pour le tri
    for($boucle=0;$boucle<$nombreelement;$boucle++) {
236     $cle = "'".$boucle."'";
        if(!$as[$cle]) {
238        $as[$cle] = 0;
        }
240 }
    //Triage du tableau des résultats
242 flush();
    arsort($as,SORT_NUMERIC);
244 reset($as);
    flush();
246 $totalboucle = 0;
    while((list($key,$value)= each($as))) {
248     $cle = str_replace("'","",$key);
        $pourcentage = ($value/$sommeBytesTotal)*100;
250     $query = "insert into asdCacheIn values (".$cle.",".$pourcentage.")";
        $result = mysql_query($query)
252             or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
    '.$query.'<br>');
254 }
    $query = "update timeCache set asDIn = ".$timeNow."";
256 mysql_query($query)
        or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");
258
    $query = "update cacheEnCours set asIn = 0";
260 $result = mysql_query($query)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
262 }
//Chargement de la description des ports
264 unset($as);
$query2='select asnumber,description from asdescription order by asnumber';
266 $result2 = mysql_query($query2)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
268 $boucle=0;
while($row2 = mysql_fetch_object($result2)) {
270 $asdescription[$row2->asnumber] = $row2->description;
    $boucle++;
272 }
mysql_free_result($result2);
274
//Chargement de la description des ports
276 $query="select srcas,pourcentage from ashCacheIn where pourcentage > ".$seuil."";
$result = mysql_query($query)
278 or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
$boucle=0;
280 while($row = mysql_fetch_object($result)) {
    $as[$boucle][0] = $row->srcas;
282 $as[$boucle][1] = $row->pourcentage;
    $boucle++;
```

```
284 }
    mysql_free_result($result);
286


288
    // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
290 //de 1% de traffic
    ?>
292 <form action="netas2in.php" method="post">
    <center>Down Limit Display:
294 <input type="text" name="seuil" size=10 maxlength=10 value="<?print $seuil?>"></center><br>
    <br>
296 <input type="submit" value="Envoyer">
    </form>
298 <h4>Click on the AS to see it's detailed graph<br>
    Data range:5 min<br>
300 Data age: max 48H<br>
    graph type: 12H<br>
302 data here under: Total generated traffic by AS on entrance traffic</h4><br>
    <table border="0" cellspacing="2" cellpadding="2" align="center">
304 <tr><th>AS</th><th>Pourcentage</th><th>Description</th></tr>
    <?
306     flush();
        $nombreas = count($as);
308     for($boucle=0;$boucle<$nombreas;$boucle++) {
            $cle = $as[$boucle][0];
310         $pourcentage = $as[$boucle][1];
            if(!isset($asdescription[$cle])) {
312             $asparam = "AS".$cle;
                $tmp=WhoisDescriPtionLevel3v2("$asparam");
314             if(strcmp($tmp[0],"")==0){
                    $tmp=WhoisDescriPtionLevel3v2("$cle");
316                 if(strcmp($tmp[0],"")==0){
                        $tmp[0]="unknown";
318                 }
                }
320             $requete3 = 'insert into asdescription values('.$cle.',"'.$tmp[0].'")';
                mysql_query($requete3);
322             $asdescription[$cle]=$tmp[0];
                }
324         print '
            <tr><td align="center">
326         <a href="netflow.php?srcas='.$cle.'&interval=H" target="_blank">'.$cle.'</a></td>
            <!--'.$cle.'</td>-->
328         <td align="center">';
            printf("%2.2f",$pourcentage);
330         $totalboucle += $pourcentage;
            print'
332         </td>
            <td align="center">'.$asdescription[$cle].'</td></tr>';
334         flush();
        }
336     print'
        <tr><td align="center"> </td>
338         <td align="center">';
        printf("%2.2f",$totalboucle);
340     print '
            </td>
342         <td align="center">Total monitored</td>
            </tr>
344     </table><br><br>
        ';
346     print '<a href="netflow.php?interval=T&version=1" target="_blank">
                Click to see complete Traffic (2 days)</a><br><br>';
348 // Affichage du résultat de la requête ci dessus avec sélection sur les AS ayant plus
    //de 1% de traffic
350
```

```
$timefin=time();
$timetotal = $timefin-$timedebut;
print 'Execution Time (sec): ';
print $timetotal."<br>";

/// Traffic 7 jours aggrégé par heure
$sommeBytesTotal = 0;
unset($as);
unset($sommeBytesTotal);
$totalboucle = 0;
//Chargement de la description des ports
$query="select srcas,pourcentage from asdCacheIn where pourcentage > ".$seuil."";
$result = mysql_query($query) or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: %%@
'.$query2.'<br>');
$boucle=0;
while($row = mysql_fetch_object($result)) {
    $as[$boucle][0] = $row->srcas;
    $as[$boucle][1] = $row->pourcentage;
    $boucle++;
}
mysql_free_result($result);


// Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
//de 1% de traffic
?>
<h4>Click on the AS to see it's detailed graph<br>
Data range:1 H<br>
Data age: max 7 days<br>
graph type: 24H<br>
<table border="0" cellspacing="2" cellpadding="2" align="center">
<tr><th>AS</th><th>Pourcentage</th><th>Description</th></tr>
<?
    flush();
    $nombreas = count($as);
    for($boucle=0;$boucle<$nombreas;$boucle++) {
        $cle = $as[$boucle][0];
        $pourcentage = $as[$boucle][1];
        if(!isset($asdescription[$cle])) {
            $asparam = "AS".$cle;
            $tmp=WhoisDescriPtionLevel3v2("$asparam");
            if(strcmp($tmp[0],"")==0){
                $tmp=WhoisDescriPtionLevel3v2("$cle");
                if(strcmp($tmp[0],"")==0){
                    $tmp[0]="unknown";
                }
            }
            $requete3 = 'insert into asdescription values('.$cle.',"'.$tmp[0].'")';
            mysql_query($requete3);
            $asdescription[$cle]=$tmp[0];
        }
        print '
        <tr><td align="center">
        <a href="netflow.php?srcas='.$cle.'&interval=H" target="_blank">'.$cle.'</a></td>
        <!--'.$cle.'</td>-->
        <td align="center">';
        printf("%2.2f",$pourcentage);
        $totalboucle += $pourcentage;
        print'
        </td>
        <td align="center">'.$asdescription[$cle].'</td></tr>';
        flush();
    }
    print'
    <tr><td align="center"> </td>
        <td align="center">';
```

```
418     printf("%2.2f",$totalboucle);
        print '
420        </td>
           <td align="center">Total monitored</td>
422        </tr>
        </table><br><br>
424     ';
    print '<br><br><a href="netflow.php?interval=T&version=2" target="_blank">
426        Click to see complete traffic (7 days)</a><br>';
    print '<br><br><a href="net.php">back</a><br>';
428

430 # FIN QUERY
    mysql_close($dbh); // Closing connection
432 $timefin=time();
    $timetotal = $timefin-$timedebut;
434 print 'Execution Time (sec): ';
    print $timetotal;
436 Pied2("");
    ?>
```

Fichier : netas2out.php

```
 2 <?PHP
   require "./lib/Html.php";
 4 require "./lib/Mysql.php";
   require "./lib/Cricket.php";
 6 require "./lib/Whois.php";
   require "./lib/Network.php";
 8 $timedebut = time();
   $MYSQL_U="flowtools";
10 $MYSQL_P="netflow";
   $MYSQL_D="flowtools";
12 $MYSQL_H="localhost";
   require "router.php";
14
   // Variables
16 // $portlist Contient la liste des ports du hit parade
   // $port [] [0] contient le numero du port
18 // $port [] [1] contient la description du port
   // $port [] [2] contient le total du traffic du port par router
20 // $port [] [3] contient l'ip du routeur selectionné

22 // $router[] contient la liste des routeurs dans la base
   // $interface [numero routeur] [X] [0] contient le numéro de
24 // l'interface X du [numero routeur] voir le tableau $router[]
   // $routerselect = chaine contenant le "where" d'un select
26 // construit sur abse des données de la base
   //
28 // $sommeBytesTotal = total du traffic du port courant;
   //
30 // $queryXXXX, $resultXXXXX et $rowXXXX servent de variable temporaire aux requêtes XXXX
   //
32 // $port [X] contient la liste des hit parade des ports, en ordre croissant
   //
34 // ATTENTION: Du à la présence de l'élément 0 dans le tableau,
   // on ne peut utiliser le while(port []) car le 0 est considéré comme faux !
36 //     on utilisera un for each ou un for(sizeof).
   //
38 //
   //
40
   $dbh=ConnectMysql(); //connection à la base de données
42

44 Entete2("Vue du traffic par AS");
```

```
$query="select asOut from cacheEnCours";
$result = mysql_query($query)
   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
if($row->asOut == 1) {
   print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
   flush();
   while($row->asOut == 1) {
      $result = mysql_query($query)
         or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
   }
   $doCacheH = 0;
   $doCacheD = 0;
}

if(!isset($seuil)) {
   $seuil = 1;
}

# QUERY
// Traffic aggrégé en 48 H (par 5 minutes)

$query = "select count(*) as total from ashCacheOut";
$result = mysql_query($query)
   or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$nombreDataCacheH = $row->total;

$query = "select count(*) as total from asdCacheOut";
$result = mysql_query($query)
   or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$nombreDataCacheD = $row->total;

$query = "select asHOut,asDOut,unix_timestamp(now()) as timenow from timeCache";
$result = mysql_query($query)
   or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$timeCacheH = $row->asHOut;
$timeCacheD = $row->asDOut;
$timeNow = $row->timenow;

$doCacheH = 0;
$doCacheD = 0;

if($nombreDataCacheH == 0 || ($timeNow - $timeCacheH)>=21600) {
   $doCacheH = 1;
}
if($nombreDataCacheD == 0 || ($timeNow - $timeCacheD)>=43200) {
   $doCacheD = 1;
}

$query="select * from ashCacheOut where pourcentage >".$seuil."";
$query="select * from asdCacheOut where pourcentage >".$seuil."";
$query="select asOut from cacheEnCours";

$result = mysql_query($query)
   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
if($row->asOut == 1) {
   print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
   flush();
   while($row->asOut == 1) {
      $result = mysql_query($query)
         or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
```

```
112         $row = mysql_fetch_object($result);
        }
114     $doCacheH = 0;
        $doCacheD = 0;
116 }

118 if($doCacheH == 1) {
        $query = "update cacheEnCours set asOut = 1";
120     $result = mysql_query($query)
           or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
122     print ("<H3>Cache under construction (5 min AGG)</H3><br>");
        flush();
124     $sommeBytesTotal = 0;

126     $query2='truncate table ashCacheOut';
        $result2 = mysql_query($query2)
128        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');

130     // Somme Traffic entrant
        for($boucle=0;$boucle<48;$boucle++) {
132        $query = 'select sum(bytes) as total from asH_'.$boucle.' where srcas = 5432';
           $result = mysql_query($query)
134           or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
    ".mysql_error($dbh)."<br>");
136        $row=mysql_fetch_object($result);
           $sommeBytesTotal += $row->total;
138        mysql_free_result($result);
        }
140     // Récupérationde l'ensemble des données sur les as
        // Utilisation d'un tableau (indice = as)
142
        for($boucle=0;$boucle<48;$boucle++) {
144
           $query = '  select    destas,
146                       sum(bytes) as total
                   FROM asH_'.$boucle.'
148                where srcas = 5432
                   group by destas';
150
           $result = mysql_query($query) or die ('query get list as failed: %%@
152 '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
           while($row=mysql_fetch_object($result)) {
154           $cle = "'".$row->destas."'";
              $as[$cle] += $row->total;
156        }
           mysql_free_result($result);
158     }
        //print_r($as);
160     $nombreelement = count($port);

162     //Creation du tableau des totaux pour le tri
        for($boucle=0;$boucle<$nombreelement;$boucle++) {
164        $cle = "'".$boucle."'";
           if(!$as[$cle]) {
166           $as[$cle] = 0;
           }
168     }
        //Triage du tableau des résultats
170     flush();
        arsort($as,SORT_NUMERIC);
172     reset($as);
        flush();
174     $totalboucle = 0;
           while((list($key,$value)= each($as))) {
176        $cle = str_replace("'","",$key);
           $pourcentage = ($value/$sommeBytesTotal)*100;
178        $query = "insert into ashCacheOut values (".$cle.",".$pourcentage.")";
```

```
        $result = mysql_query($query) or die ('query get list as failed: %%@
180 '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
    }
182 $query = "update timeCache set asHOut = ".$timeNow."";
    mysql_query($query)
184     or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");

186 if($doCacheD == 0) {
        $query = "update cacheEnCours set asOut = 0";
188     $result = mysql_query($query)
            or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
190 }
}
192 if($doCacheD == 1) {
    if($doCacheH == 0) {
194     $query = "update cacheEnCours set asOut = 1";
        $result = mysql_query($query)
196         or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
    }
198 print ("<H3>Cache under construction (1H AGG)</H3><br>");
    flush();
200 $sommeBytesTotal = 0;
    unset($as);
202 $query2='truncate table asdCacheOut';
    $result2 = mysql_query($query2)
204     or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
    // Somme Traffic entrant
206 for($boucle=0;$boucle<7;$boucle++) {
        $query = 'select sum(bytes) as total from asD_'.$boucle.' where srcas = 5432';
208     $result = mysql_query($query)
            or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
210 ".mysql_error($dbh)."<br>");
        $row=mysql_fetch_object($result);
212     $sommeBytesTotal += $row->total;
        mysql_free_result($result);
214 }

216 // Récupérationde l'ensemble des données sur les as
    // Utilisation d'un tableau (indice = as)
218
    for($boucle=0;$boucle<7;$boucle++) {
220
        $query = '  select    destas,
222                     sum(bytes) as total
                FROM asD_'.$boucle.'
224             where srcas = 5432
                group by destas';
226
        $result = mysql_query($query)
228         or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
        while($row=mysql_fetch_object($result)) {
230         $cle = "'".$row->destas."'";
            $as[$cle] += $row->total;
232     }
        mysql_free_result($result);
234 }
    //print_r($as);
236 $nombreelement = count($port);

238 //Creation du tableau des totaux pour le tri
    for($boucle=0;$boucle<$nombreelement;$boucle++) {
240     $cle = "'".$boucle."'";
        if(!$as[$cle]) {
242         $as[$cle] = 0;
        }
244 }
    //Triage du tableau des résultats
```

```
246     flush();
        arsort($as,SORT_NUMERIC);
248     reset($as);
        flush();
250     $totalboucle = 0;
           while((list($key,$value)= each($as))) {
252        $cle = str_replace("'","",$key);
           $pourcentage = ($value/$sommeBytesTotal)*100;
254        $query = "insert into asdCacheOut values (".$cle.",".$pourcentage.")";
           $result = mysql_query($query)
256           or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
        }
258     $query = "update timeCache set asDOut = ".$timeNow."";
        mysql_query($query)
260        or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");

262     $query = "update cacheEnCours set asOut = 0";
        $result = mysql_query($query)
264           or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
        }
266 //Chargement de la description des ports
    unset($as);
268 $query2='select asnumber,description from asdescription order by asnumber';
    $result2 = mysql_query($query2)
270     or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
    $boucle=0;
272 while($row2 = mysql_fetch_object($result2)) {
        $asdescription[$row2->asnumber] = $row2->description;
274     $boucle++;
    }
276 mysql_free_result($result2);

278 $query="select dstas,pourcentage from ashCacheOut where pourcentage > ".$seuil."";
    $result = mysql_query($query)
280     or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
    $boucle=0;
282 while($row = mysql_fetch_object($result)) {
        $as[$boucle][0] = $row->dstas;
284     $as[$boucle][1] = $row->pourcentage;
        $boucle++;
286 }
    mysql_free_result($result);
288


290
    // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
292 //de 1% de traffic
    ?>
294 <form action="netas2out.php" method="post">
    <center>Down limit display:
296 <input type="text" name="seuil" size=10 maxlength=10 value="<?print $seuil?>"></center><br>
    <br>
298 <input type="submit" value="Envoyer">
    </form>
300 <h4>Click on the AS to see it's detailed graph<br>
    Data range:5 min<br>
302 Data age: max 48H<br>
    graph type: 12H<br>
304 data here under: Total generated traffic to AS on leaving traffic</h4><br>
    <table border="0" cellspacing="2" cellpadding="2" align="center">
306 <tr><th>AS</th><th>Pourcentage</th><th>Description</th></tr>
    <?
308     flush();
        $nombreas = count($as);
310     for($boucle=0;$boucle<$nombreas;$boucle++) {
           $cle = $as[$boucle][0];
312        $pourcentage = $as[$boucle][1];
```

```
        if(!isset($asdescription[$cle])) {
314         //print $asdescription[$cle]."<br>";
            $asparam = "AS".$cle;
316         $tmp=WhoisDescriPtionLevel3v2("$asparam");
            if(strcmp($tmp[0],"")==0){
318             $tmp=WhoisDescriPtionLevel3v2("$cle");
                if(strcmp($tmp[0],"")==0){
320                 $tmp[0]="unknown";
                }
322         }
            $requete3 = 'insert into asdescription values('.$cle.',"'.$tmp[0].'")';
324         mysql_query($requete3);
            $asdescription[$cle]=$tmp[0];
326     }
        print '
328     <tr><td align="center">
        <a href="netflow.php?srcas='.$cle.'&interval=H" target="_blank">'.$cle.'</a></td>
330     <!--'.$cle.'</td>-->
        <td align="center">';
332     printf("%2.2f",$pourcentage);
        $totalboucle += $pourcentage;
334     print'
        </td>
336     <td align="center">'.$asdescription[$cle].'</td></tr>';
        flush();
338 }
    print'
340 <tr><td align="center"> </td>
      <td align="center">';
342 printf("%2.2f",$totalboucle);
    print '
344     </td>
        <td align="center">Total monitored</td>
346     </tr>
    </table><br><br>
348 ';
    print '<a href="netflow.php?interval=T&version=1" target="_blank">
350     Click to see complete Traffic (2 days)</a><br><br>';
// Affichage du résultat de la requête ci dessus avec sélection sur les AS ayant plus
352 //de 1% de traffic
//mysql_close($dbh); // Closing connection
354 $timefin=time();
$timetotal = $timefin-$timedebut;
356 print 'Execution Time (sec): ';
print $timetotal."<br>";
358
/// Traffic 7 jours aggrégé par heure
360 $sommeBytesTotal = 0;
unset($as);
362 unset($sommeBytesTotal);
$totalboucle = 0;
364 //Chargement de la description des ports
$query="select dstas,pourcentage from asdCacheOut where pourcentage > ".$seuil."";
366 $result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
368 $boucle=0;
while($row = mysql_fetch_object($result)) {
370     $as[$boucle][0] = $row->dstas;
        $as[$boucle][1] = $row->pourcentage;
372     $boucle++;
}
374 mysql_free_result($result);

376

378 // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
//de 1% de traffic
```

```
?>
<h4>Click on the AS to see it's detailed graph<br>
Data range:1 H<br>
Data age: max 7 days<br>
graph type: 24H<br>
<table border="0" cellspacing="2" cellpadding="2" align="center">
<tr><th>AS</th><th>Pourcentage</th><th>Description</th></tr>
<?
    flush();
    //for($boucle=0;$boucleport<$nombreelement;$boucleport++){
    $nombreas = count($as);
    for($boucle=0;$boucle<$nombreas;$boucle++) {
        $cle = $as[$boucle][0];
        $pourcentage = $as[$boucle][1];
        if(!isset($asdescription[$cle])) {
            //print $asdescription[$cle]."<br>";
            $asparam = "AS".$cle;
            $tmp=WhoisDescriPtionLevel3v2("$asparam");
            if(strcmp($tmp[0],"")==0){
                $tmp=WhoisDescriPtionLevel3v2("$cle");
                if(strcmp($tmp[0],"")==0){
                    $tmp[0]="unknown";
                }
            }
            $requete3 = 'insert into asdescription values('.$cle.',"'.$tmp[0].'")';
            mysql_query($requete3);
            $asdescription[$cle]=$tmp[0];
        }
        print '
        <tr><td align="center">
        <a href="netflow.php?srcas='.$cle.'&interval=H" target="_blank">'.$cle.'</a></td>
        <!--'.$cle.'</td>-->
        <td align="center">';
        printf("%2.2f",$pourcentage);
        $totalboucle += $pourcentage;
        print'
        </td>
        <td align="center">'.$asdescription[$cle].'</td></tr>';
        flush();
    }
    print'
    <tr><td align="center"> </td>
        <td align="center">';
    printf("%2.2f",$totalboucle);
    print '
        </td>
        <td align="center">Total monitored</td>
        </tr>
    </table><br><br>
    ';
print '<br><br><a href="netflow.php?interval=T&version=2" target="_blank">
    Click to see complete traffic (7 days)</a><br>';
print '<br><br><a href="net.php">back</a><br>';

# FIN QUERY
mysql_close($dbh); // Closing connection
$timefin=time();
$timetotal = $timefin-$timedebut;
print 'Execution Time (sec): ';
print $timetotal;
Pied2("");
?>
```

Fichier : netflow.php

```
<?php
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Whois.php";
require "./lib/Network.php";
require "router.php";

require ("./jpgraph-1.8/src/jpgraph.php");
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");

$routerin = getSelectRouterin();
$routerout = getSelectRouterout();


# QUERY
$dbh=ConnectMysql();
$mintableH = 0;
$mintableD = 0;
$minheureH = 0;
$minheureD = 0;




switch ($interval) {
   case 'H':
      for($boucle=0;$boucle<48;$boucle++) {
         $query = "select min(heure) as heure from asH_".$boucle."";
         $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
         $row = mysql_fetch_object($result);
         if(($boucle ==0 || !($minheureH)) && $row->heure)  {
            $minheureH = $row->heure;
            $mintableH=$boucle;
         } elseif($row->heure) {
            if(($row->heure<$minheureH) && $row->heure) {
               $minheureH = $row->heure;
               $mintableH = $boucle;
            }
         }
      }

      $ConvertMBits=8/300;

      for($boucle=0;$boucle<48;$boucle++) {
         $table = ($mintableH+$boucle)%48;
         $query = "  select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
                        sum(bytes)/1000 as rs
                  FROM asH_".$table."
                  where srcas in (".$srcas.")
                  group by heure
                  order by heure";
         $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
                        sum(bytes)/1000 as rs
                     FROM asH_".$table."
                  where destas in (".$srcas.")
                  group by heure
                  order by heure";

         $result = mysql_query($query)
              or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

```

```
            while ($row = mysql_fetch_object($result)) {
70              $cle = ($row->heure-$minheureH)/300;
                $data[$cle]=$row->rs*$ConvertMBits;
72              $ydata[$cle]=$row->d;
            }
74
            $result = mysql_query($query2)
76              or die("Query failed<br>Query: ".$query2."<br>".mysql_error($dbh)."<br>");
            while ($row = mysql_fetch_object($result)) {
78              $cle = ($row->heure-$minheureH)/300;
                    $data2[$cle]=$row->rs*$ConvertMBits;
80          }
        }
82      break;

84  case 'D':
        for($boucle=0;$boucle<7;$boucle++) {
86          $query = "select min(heure) as heure from asD_".$boucle."";
            $result = mysql_query($query)
88              or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
            $row = mysql_fetch_object($result);
90          if(($boucle==0 || !($minheureD)) && $row->heure)  {
                $minheureD = $row->heure;
92              $mintableD=$boucle;
            } elseif ($row->heure) {
94              if(($row->heure < $minheureD) && $row->heure) {
                    $minheureD = $row->heure;
96                  $mintableD = $boucle;
                }
98          }
        }
100     for($boucle=0;$boucle<7;$boucle++) {
            $table = ($mintableD+$boucle)%7;
102         $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
104                     sum(bytes)/1000 as rs
                  FROM asD_".$table."
106               where srcAs in (".$srcas.")
                  group by heure order by heure";
108         $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
110                     sum(bytes)/1000 as rs
                    FROM asD_".$table."
112               where destAs in (".$srcas.")
                        group by heure
114               order by heure";
            $ConvertMBits=8/3600;
116         $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
118
            while ($row = mysql_fetch_object($result)) {
120             $cle = ($row->heure-$minheureD)/3600;
                $data[$cle]=$row->rs*$ConvertMBits;
122             $ydata[$cle]=$row->d;
            }
124
            $result = mysql_query($query2)
126                     or die("Query failed<br>Query: ".$query2."<br>".mysql_error($dbh)."<br>");
            $i=0;
128
            while ($row = mysql_fetch_object($result)) {
130             $cle = ($row->heure-$minheureD)/3600;
                    $data2[$cle]=$row->rs*$ConvertMBits;
132             }
        }
134     break;
```

```
136     case 'B':
            for($boucle=0;$boucle<7;$boucle++) {
138                 $query = "select min(heure) as heure from asD_".$boucle."";
                    $result = mysql_query($query)
140                         or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
                    $row = mysql_fetch_object($result);
142                 if(($boucle==0 || !($minheureD)) && $row->heure)  {
                            $minheureD = $row->heure;
144                         $mintableD=$boucle;
                    } elseif ($row->heure) {
146                         if(($row->heure < $minheureD) && $row->heure) {
                            $minheureD = $row->heure;
148                         $mintableD = $boucle;
                            }
150                 }
            }
152
        $query="select asorigin from BgpCheck.BGPDATA where aspath like '$srcas %' group by asorigin";
154     $result = mysql_query($query)
           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
156     $asListe="";
        $asListe.=$srcas;
158     while ($row = mysql_fetch_object($result)) {
           $asListe.=",".$row->asorigin;
160     }

162        for($boucle=0;$boucle<7;$boucle++) {
                   $table = ($mintableD+$boucle)%7;
164                $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                            heure,sum(bytes)/1000 as rs
166                       FROM asD_".$table."
                          where srcAs in (".$asListe.")
168                       group by heure
                          order by heure";
170                $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                            heure,
172                         sum(bytes)/1000 as rs
                                FROM asD_".$table."
174                       where destAs in (".$asListe.")
                          group by heure order by heure";
176                $ConvertMBits=8/3600;
                   $result = mysql_query($query)
178                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

180                 while ($row = mysql_fetch_object($result)) {
                          $cle = ($row->heure-$minheureD)/3600;
182                         $data[$cle]=$row->rs*$ConvertMBits;
                            $ydata[$cle]=$row->d;
184                }

186                $result = mysql_query($query2)
                   or die("Query failed<br>Query: ".$query2."<br>".mysql_error($dbh)."<br>");
188            $i=0;

190                while ($row = mysql_fetch_object($result)) {
                          $cle = ($row->heure-$minheureD)/3600;
192                        $data2[$cle]=$row->rs*$ConvertMBits;
               }
194        }
       break;
196
    case 'T':
198    switch($version) {
          case '1':
200          for($boucle=0;$boucle<48;$boucle++) {
                $query = "select min(heure) as heure from asH_".$boucle."";
202             $result = mysql_query($query)
```

```
                                or die("Query failed<br>Query: %%@
204 ".$query."<br>".mysql_error($dbh)."<br>");
                    $row = mysql_fetch_object($result);
206                 if( ($boucle ==0 || !($minheureH)) && $row->heure)  {
                        $minheureH = $row->heure;
208                     $mintableH=$boucle;
                    } elseif ($row->heure) {
210                     if(($row->heure<$minheureH) && $row->heure) {
                            $minheureH = $row->heure;
212                         $mintableH = $boucle;
                        }
214                 }
                }
216             for($boucle=0;$boucle<48;$boucle++) {
                    $table = ($mintableH+$boucle)%48;
218                 $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                                heure,
220                             sum(bytes)/1000 as rs
                            FROM asH_".$table."
222                         where ".$routerin."
                            group by heure
224                         order by heure ";
                    $ConvertMBits=8/300;
226                 $result = mysql_query($query)
                                or die("Query failed<br>Query: %%@
228 ".$query."<br>".mysql_error($dbh)."<br>");

230                 while ($row = mysql_fetch_object($result)) {
                        $cle = ($row->heure-$minheureH)/300;
232                     $data[$cle]=$row->rs*$ConvertMBits;
                        $ydata[$cle] =$row->d;
234                 }

236                 $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                                heure,sum(bytes)/1000 as rs
238                         FROM asH_".$table."
                            where ".$routerout."
240                         group by heure
                            order by heure ";
242                 $result = mysql_query($query2)
                                or die("Query failed<br>Query: %%@
244 ".$query2."<br>".mysql_error($dbh)."<br>");
                    while ($row = mysql_fetch_object($result)) {
246                     $cle = ($row->heure-$minheureH)/300;
                            $data2[$cle]=$row->rs*$ConvertMBits;
248                 }
                }
250             break;

252         case '2':
                for($boucle=0;$boucle<7;$boucle++) {
254                 $query = "select min(heure) as heure from asD_".$boucle."";
                    $result = mysql_query($query)
256                             or die("Query failed<br>Query: %%@
  ".$query."<br>".mysql_error($dbh)."<br>");
258                 $row = mysql_fetch_object($result);
                    if(($boucle==0 || !($minheureD)) && $row->heure)  {
260                     $minheureD = $row->heure;
                        $mintableD=$boucle;
262                 } elseif ($row->heure) {
                        if(($row->heure<$minheureD) && $row->heure) {
264                         $minheureD = $row->heure;
                            $mintableD = $boucle;
266                     }
                    }
268             }
                for($boucle=0;$boucle<7;$boucle++) {
```

```
270                 $table = ($mintableD+$boucle)%7;
                    $query = "   select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
272                             heure,sum(bytes)/1000 as rs
                        FROM asD_".$table."
274                     where ".$routerin."
                        group by heure
276                     order by heure";
                    $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
278                             heure,
                                sum(bytes)/1000 as rs
280                        FROM asD_".$table."
                        where ".$routerout."
282                     group by heure
                        order by heure";
284                 $ConvertMBits=8/3600;
                    $result = mysql_query($query)
286                                 or die("Query failed<br>Query: %%@
    ".$query."<br>".mysql_error($dbh)."<br>");
288
                    while ($row = mysql_fetch_object($result)) {
290                     $cle = ($row->heure-$minheureD)/3600;
                        $data[$cle]=$row->rs*$ConvertMBits;
292                     $ydata[$cle]=$row->d;
                    }
294
                    $result = mysql_query($query2)
296                                 or die("Query failed<br>Query: %%@
    ".$query2."<br>".mysql_error($dbh)."<br>");
298                 $i=0;

300                 while ($row = mysql_fetch_object($result)) {
                        $cle = ($row->heure-$minheureD)/3600;
302                         $data2[$cle]=$row->rs*$ConvertMBits;
                    }
304             }
                break;
306         }
    }
308
    # FIN QUERY
310 mysql_free_result($result); // Free result
    mysql_close($dbh); // Closing connection
312 /*print $minheureH."<br>";
    print $mintableH."<br>";
314 print $minheureD."<br>";
    print $mintableD."<br>";
316
    print "Data:";
318 print_r($data);
    print "<br> data2";
320 print_r($data2);
    print "<br>Ydata:";
322 print_r($ydata);
    */
324 //Create the graph
    $graph = new Graph(900,500);
326 $graph -> SetScale("textlin");
    // Set the margins
328 $graph ->img->SetMargin(80,80,40,120);
    if($interval=='T') {
330     $asData=" ALL AS";
    }
332 else
    {
334     $As="AS".$srcas;
        $tmp=WhoisDescriPtionLevel3v2("$As");
336     $asData=$srcas." (".$tmp[0].")";
```

```
}

//Titles and layout stuff
$graph ->title->Set("AS :".$asData."");
$graph ->xaxis->title->Set("Time");
$graph ->xaxis->SetTickLabels("Netflow");
$graph ->xgrid->Show(true,false);
$graph ->xaxis->SetTextTickInterval(22);
$graph->xaxis->SetTickLabels($ydata);
$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
$graph ->yaxis->title->Set("Mbit/s");
$graph ->yaxis->scale->ticks->SupressFirst();
$graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_HOR);
$graph ->legend->Pos(.5,.1,"center","top");
$graph ->ygrid->Show(true,false);

//Create linear graph for weight
$lineplot = new LinePlot($data);
$lineplot ->SetColor("blue");
$lineplot ->mark->SetColor("blue");
$lineplot ->SetWeight("2");
$lineplot ->SetLegend("Mbit/s TO 5432");

$lineplot2 = new LinePlot($data2);
$lineplot2 ->SetColor("red");
$lineplot2 ->mark->SetColor("red");
$lineplot2 ->SetWeight("2");
$lineplot2 ->SetLegend("Mbit/s FROM 5432");


//Draw the graphs
$graph->Add($lineplot);
$graph->Add($lineplot2);
$graph->Stroke();


?>
```

Fichier : netport2in.php

```
<?PHP
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Cricket.php";
require "./lib/Whois.php";
require "./lib/Network.php";
$timedebut = time();
Entete2("Vue du traffic par Port");

// Variables
// $portlist Contient la liste des ports du hit parade
// $port [] [0] contient le numero du port
// $port [] [1] contient la description du port
// $port [] [2] contient le total du traffic du port par router
// $port [] [3] contient l'ip du routeur selectionné

// $router[] contient la liste des routeurs dans la base
// $interface [numero routeur] [X] [0] contient le numéro de
// l'interface X du [numero routeur]
// voir le tableau $router[]
// $routerselect = chaine contenant le "where" d'un select
// construit sur base des données de la base
//
// $sommeBytesTotal = total du traffic du port courant;
```

```
//
// $queryXXXX, $resultXXXXX et $rowXXXX servent de variable temporaire
// aux requêtes XXXX
//
// $port [X] contient la liste des hit parade des ports, en ordre croissant
// ATTENTION: Du à la présence de l'élément 0 dans le tableau,
// on ne peut utiliser le while(port []) car le 0 est considéré comme faux !
//    on utilisera un for each ou un for(sizeof).
//
//
//
if(!isset($seuil)) {
    $seuil = 1;
}
$dbh=ConnectMysql(); //connection à la base de données

$query = "select count(*) as total from porthCacheIn";
$result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$nombreDataCacheH = $row->total;

$query = "select count(*) as total from portdCacheIn";
$result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$nombreDataCacheD = $row->total;

$query = "select portHIn,portDIn,unix_timestamp(now()) as timenow from timeCache";
$result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$timeCacheH = $row->portHIn;
$timeCacheD = $row->portDIn;
$timeNow = $row->timenow;

$doCacheH = 0;
$doCacheD = 0;

if($nombreDataCacheH == 0 || ($timeNow - $timeCacheH)>=21600) {
    $doCacheH = 1;
}
if($nombreDataCacheD == 0 || ($timeNow - $timeCacheD)>=43200) {
    $doCacheD = 1;
}

$query="select portIn from cacheEnCours";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
if($row->portIn == 1) {
    print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
    flush();
    while($row->portIn == 1) {
        $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        $row = mysql_fetch_object($result);
    }
    $doCacheH = 0;
    $doCacheD = 0;
}

if($doCacheH == 1) {
    $query = "update cacheEnCours set portIn = 1";
    $result = mysql_query($query)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
```

```
92      print ("<H3>Cache under construction (5 min AGG)</H3><br>");
        flush();
94      $sommeBytesTotal = 0;

96      $query2='truncate table porthCacheIn';
        $result2 = mysql_query($query2)
98         or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');

100
        // Somme Traffic entrant
102
        for($boucle=0;$boucle<48;$boucle++) {
104        $query = 'select sum(bytesrcout+bytesrcdstout) as total from portResumeH_'.$boucle.'';
           $result = mysql_query($query)
106           or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
    ".mysql_error($dbh)."<br>");
108        $row=mysql_fetch_object($result);
           $sommeBytesTotal += $row->total;
110        mysql_free_result($result);
        }
112
        // Récupérationde l'ensemble des données sur les ports
114     // Utilisation d'un tableau (indice = port)

116     for($boucle=0;$boucle<48;$boucle++) {

118        $query = 'select port,';
           $query.= 'sum(bytesrcout) as srcin,';
120        $query.= 'sum(bytedstout) as dstin,';
           $query.= 'sum(bytesrcdstout) as srcdstin ';
122        $query.= 'FROM portResumeH_'.$boucle;
           $query.= ' group by port';
124        $query.= ' order by port';

126        $result = mysql_query($query) or die ('query get list as failed: %%@
    '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
128        while($row=mysql_fetch_object($result)) {
              $port[$row->port][0] += $row->srcin;
130           $port[$row->port][1] += $row->dstin;
              $port[$row->port][2] += $row->srcdstin;
132           $port[$row->port][3] += $row->srcin+$row->dstin+$row->srcdstin;
           }
134        mysql_free_result($result);
        }
136
        $nombreelement = count($port);
138
        //Creation du tableau des totaux pour le tri
140     for($boucle=0;$boucle<$nombreelement;$boucle++) {
           $cle = "'".$boucle."'";
142        if($port[$boucle][3]) {
              $total[$cle] = $port[$boucle][3];
144        }
           else {
146           $total[$cle] = 0;
           }
148     }
        //Triage du tableau des résultats
150     flush();
        arsort($total,SORT_NUMERIC);
152     reset($total);
        flush();
154
        while((list($key,$value)= each($total))) {
156        $key = str_replace("'","",$key);
           $pourcentagesrc = ($port[$key][0]/$sommeBytesTotal)*100;
158        $pourcentagedst = ($port[$key][1]/$sommeBytesTotal)*100;
```

```
        $pourcentagesrcdst = ($port[$key][2]/$sommeBytesTotal)*100;
160     $pourcentagetotal = ($port[$key][3]/$sommeBytesTotal)*100;
        $query = "insert into porthCacheIn values(".$key.",".
162                 $pourcentagesrc.",".$pourcentagedst.",".
                    $pourcentagesrcdst.",".$pourcentagetotal.")";
164     $result = mysql_query($query) or die ('query get list as failed: %%@
  '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
166   }
    $query = "update timeCache set portHIn = ".$timeNow."";
168 mysql_query($query)
      or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");
170
    if($doCacheD == 0) {
172   $query = "update cacheEnCours set portIn = 0";
      $result = mysql_query($query)
174     or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
    }
176 }

178 if($doCacheD == 1) {
    if($doCacheH == 0) {
180   $query = "update cacheEnCours set portIn = 1";
      $result = mysql_query($query)
182     or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
    }
184
    unset($port);
186 print ("<H3>Cache under construction (1H AGG)</H3><br>");
    flush();
188 $sommeBytesTotal = 0;
    unset($port);
190 $query2='truncate table portdCacheIn';
    $result2 = mysql_query($query2)
192   or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');

194 // Somme Traffic entrant

196 for($boucle=0;$boucle<7;$boucle++) {
      $query = 'select sum(bytesrcout+bytesrcdstout) as total from portResumeD_'.$boucle.'';
198   $result = mysql_query($query)
        or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
200 ".mysql_error($dbh)."<br>");
      $row=mysql_fetch_object($result);
202   $sommeBytesTotal += $row->total;
      mysql_free_result($result);
204 }

206 // Récupérationde l'ensemble des données sur les ports
    // Utilisation d'un tableau (indice = port)
208
    for($boucle=0;$boucle<7;$boucle++) {
210
      $query = 'select port,';
212   $query.= 'sum(bytesrcout) as srcin,';
      $query.= 'sum(bytedstout) as dstin,';
214   $query.= 'sum(bytesrcdstout) as srcdstin ';
      $query.= 'FROM portResumeD_'.$boucle;
216   $query.= ' group by port';
      $query.= ' order by port';
218
      $result = mysql_query($query) or die ('query get list as failed: %%@
220 '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
      while($row=mysql_fetch_object($result)) {
222     $port[$row->port][0] += $row->srcin;
        $port[$row->port][1] += $row->dstin;
224     $port[$row->port][2] += $row->srcdstin;
        $port[$row->port][3] += $row->srcin+$row->dstin+$row->srcdstin;
```

```
226         }
            mysql_free_result($result);
228     }
        $nombreelement = count($port);
230
        //Creation du tableau des totaux pour le tri
232     for($boucle=0;$boucle<$nombreelement;$boucle++) {
            $cle = "'".$boucle."'";
234         if($port[$boucle][3]) {
                $total[$cle] = $port[$boucle][3];
236         }
            else {
238             $total[$cle] = 0;
            }
240     }
        //Triage du tableau des résultats
242     flush();
        arsort($total,SORT_NUMERIC);
244     reset($total);
        flush();
246
        while((list($key,$value)= each($total))) {
248         $key = str_replace("'","",$key);
            $pourcentagesrc = ($port[$key][0]/$sommeBytesTotal)*100;
250         $pourcentagedst = ($port[$key][1]/$sommeBytesTotal)*100;
            $pourcentagesrcdst = ($port[$key][2]/$sommeBytesTotal)*100;
252         $pourcentagetotal = ($port[$key][3]/$sommeBytesTotal)*100;
            $query = "insert into portdCacheIn values(".$key.",".
254                     $pourcentagesrc.",".$pourcentagedst.",".
                        $pourcentagesrcdst.",".$pourcentagetotal.")";
256         $result = mysql_query($query) or die ('query get list as failed: %%@
    '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
258     }
        $query = "update timeCache set portDIn = ".$timeNow."";
260     mysql_query($query)
            or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");
262
        $query = "update cacheEnCours set portIn = 0";
264     $result = mysql_query($query)
            or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
266 }

268 //Chargement de la description des ports
    $query2='select number,description from PortDescription where type="tcp" order by number';
270 $result2 = mysql_query($query2)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
272 $boucle=0;
    while($row2 = mysql_fetch_object($result2)) {
274     $portdescription[$row2->number] = $row2->description;
        $boucle++;
276 }
    mysql_free_result($result2);
278
    unset($port);
280
    $query="select      number,
282             pourcentagesrc,
                pourcentagedst,
284             pourcentagesrcdst,
                pourcentagetotal
286         from porthCacheIn
            where pourcentagetotal > ".$seuil."";
288 $result = mysql_query($query)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
290 $boucle=0;
    while($row = mysql_fetch_object($result)) {
292     $port[$boucle][0] = $row->number;
```

```
    $port[$boucle][1] = $row->pourcentagesrc;
294     $port[$boucle][2] = $row->pourcentagedst;
    $port[$boucle][3] = $row->pourcentagesrcdst;
296     $port[$boucle][4] = $row->pourcentagetotal;
    $boucle++;
298 }
  mysql_free_result($result);
300


302
  // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
304 //de 1% de traffic
  ?>
306 <form action="netport2in.php" method="post">
  <center>Down limit display:
308 <input type="text" name="seuil" size=10 maxlength=10 value="<?print $seuil?>">
  </center><br>
310 <br>
  <input type="submit" value="Envoyer">
312 </form>
  <h4>Click on the port to see it's detailed graph<br>
314 Data range:5 min<br>
  Data age: max 48H<br>
316 graph type: 12H<br>
  data here under: Total generated traffic with srcport and dest port
318    on entrance traffic</h4><br>
  <form method="post" action="netflowportaggin.php">
320 <table border="0" cellspacing="2" cellpadding="2" align="center">
  <tr><th> </th><th>Port</th>
322    <th>% src</th><th>% dst</th>
    <th>% srcdst</th><th>% total</th>
324    <th>Description</th></tr>
  <?
326    flush();
    $boucle =0;
328    for($boucle2=0;$boucle2<4;$boucle2++) {
       $totalboucle[$boucle2] = 0;
330    }
    $nombreport = count($port);
332    for($boucle=0;$boucle<$nombreport;$boucle++) {
       $numeroport = $port[$boucle][0];
334       $pourcentagesrc= $port[$boucle][1];
       $pourcentagedst= $port[$boucle][2];
336       $pourcentagesrcdst= $port[$boucle][3];
       $pourcentagetotal=  $port[$boucle][4];
338       print '
       <tr>
340       <td align = "center">
          <input type="checkbox" name= "srcport[]" value=" '.$numeroport.'">
342          <input type="hidden"  name="interval" value="H">
       </td>
344       <td align="center">
          <a href="netflowport.php?srcport='.$numeroport.'
346                   &description='.$portdescription[$numeroport].'
                   &interval=H" target="_blank">'.$numeroport.'</a></td>
348       <td align="center">';
       printf("%2.2f",$pourcentagesrc);
350       $totalboucle[0] += $pourcentagesrc;
       print'
352       </td>
       <td align="center">';
354       printf("%2.2f",$pourcentagedst);
       $totalboucle[1] += $pourcentagedst;
356       print'
       </td>
358       <td align="center">';
       printf("%2.2f",$pourcentagesrcdst);
```

```
360         $totalboucle[2] += $pourcentagesrcdst;
            print '
362         </td>
            <td align="center">';
364         printf("%2.2f",$pourcentagetotal);
            $totalboucle[3] += $pourcentagetotal;
366         print '
            </td>
368         <td align="center">'.$portdescription[$numeroport]. '</td></tr>';
            flush();
370      }
         print '
372      <tr>
            <td align="center">
374            <input type="submit" value="Draw Cumulated Graph">
               </form>
376         </td>
            <td align="center"> </td>
378         <td align="center">';
         printf("%2.2f",$totalboucle[0]);
380      print '
            </td>
382         <td align="center">';
         printf("%2.2f",$totalboucle[1]);
384      print '
            </td>
386         <td align="center">';
         printf("%2.2f",$totalboucle[2]);
388      print '
            </td>
390         <td align="center">';
         printf("%2.2f",$totalboucle[3]);
392      print '</td>
            <td align="center">Total monitored</td>
394         </tr>
         </table><br><br>
396      ';
         print '<a href="netflowport.php?interval=T&version=1" target="_blank">
398         Click to see complete Traffic (2 days)</a><br><br>';
   // Affichage du résultat de la requête ci dessus avec sélection sur les AS ayant plus
400 //de 1% de traffic

402 $timefin=time();
   $timetotal = $timefin-$timedebut;
404 print 'Execution Time (sec): ';
   print $timetotal."<br>";
406
   /// Traffic 7 jours aggrégé par heure
408 $sommeBytesTotal = 0;
   unset($port);
410 unset($total);

412 $query="select     number,
                pourcentagesrc,
414             pourcentagedst,
                pourcentagesrcdst,
416             pourcentagetotal
         from portdCacheIn
418      where pourcentagetotal > ".$seuil."";
   $result = mysql_query($query)
420    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
   $boucle=0;
422 while($row = mysql_fetch_object($result)) {
      $port[$boucle][0] = $row->number;
424   $port[$boucle][1] = $row->pourcentagesrc;
      $port[$boucle][2] = $row->pourcentagedst;
426   $port[$boucle][3] = $row->pourcentagesrcdst;
```

```
    $port[$boucle][4] = $row->pourcentagetotal;
428    $boucle++;
   }
430 mysql_free_result($result);

432

434 // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
   //de 1% de traffic
436 ?>
   <h4>Click on the port to see it's detailed graph<br>
438 Data range:1 H<br>
   Data age: max 7 Days<br>
440 graph type: 24H<br>
   <form method="post" action="netflowportaggin.php">
442 <table border="0" cellspacing="2" cellpadding="2" align="center">
   <tr><th> </th><th>Port</th><th>% src</th><th>% dst</th><th>% srcdst</th><th>% %%@
444 total</th><th>Description</th></tr>
   <?
446    flush();
       //for($boucle=0;$boucleport<$nombreelement;$boucleport++){
448    $boucle =0;
       for($boucle2=0;$boucle2<4;$boucle2++) {
450       $totalboucle[$boucle2] = 0;
       }
452    $nombreport = count($port);
       for($boucle=0;$boucle<$nombreport;$boucle++) {
454       $numeroport = $port[$boucle][0];
          $pourcentagesrc= $port[$boucle][1];
456       $pourcentagedst= $port[$boucle][2];
          $pourcentagesrcdst= $port[$boucle][3];
458       $pourcentagetotal=  $port[$boucle][4];
          print '
460       <tr>
          <td align = "center">
462          <input type="checkbox" name= "srcport[]" value="'.$numeroport.'">
             <input type="hidden" name="interval" value="D">
464       </td>
          <td align="center">
466       <a href="netflowport.php?srcport='.$numeroport.'
                &descrition='.$portdescription[$numeroport].'
468             &interval=H" target="_blank">'.$numeroport.'</a></td>
          <td align="center">';
470       printf("%2.2f",$pourcentagesrc);
          $totalboucle[0] += $pourcentagesrc;
472       print'
          </td>
474       <td align="center">';
          printf("%2.2f",$pourcentagedst);
476       $totalboucle[1] += $pourcentagedst;
          print'
478       </td>
          <td align="center">';
480       printf("%2.2f",$pourcentagesrcdst);
          $totalboucle[2] += $pourcentagesrcdst;
482       print'
          </td>
484       <td align="center">';
          printf("%2.2f",$pourcentagetotal);
486       $totalboucle[3] += $pourcentagetotal;
          print'
488       </td>
          <td align="center">'.$portdescription[$numeroport].'</td></tr>';
490       flush();
       }
492    print'
       <tr>
```

```
494         <td align="center">
               <input type="submit" value="Draw Cumulated Graph">
496            </form>
            </td>
498         <td align="center"> </td>
            <td align="center">';
500      printf("%2.2f",$totalboucle[0]);
         print '
502         </td>
            <td align="center">';
504      printf("%2.2f",$totalboucle[1]);
         print '
506         </td>
            <td align="center">';
508      printf("%2.2f",$totalboucle[2]);
         print '
510         </td>
            <td align="center">';
512      printf("%2.2f",$totalboucle[3]);
         print '</td>
514         <td align="center">Total monitored</td>
            </tr>
516      </table><br><br>
         ';
518   print '<br><br><a href="netflowport.php?interval=T
                  &version=2" target="_blank">
520               Click to see complete traffic (7 days)</a><br>';
      print '<br><br><a href="net.php">back</a><br>';
522

524   # FIN QUERY
      mysql_close($dbh); // Closing connection
526   $timefin=time();
      $timetotal = $timefin-$timedebut;
528   print 'Execution Time (sec): ';
      print $timetotal;
530   Pied2("");
      ?>
```

Fichier : netport2out.php

```
      <?PHP
 2    require "./lib/Html.php";
      require "./lib/Mysql.php";
 4    require "./lib/Cricket.php";
      require "./lib/Whois.php";
 6    require "./lib/Network.php";
      $timedebut = time();
 8    Entete2("Vue du traffic par Port");
      $MYSQL_U="flowtools";
10    $MYSQL_P="netflow";
      $MYSQL_D="flowtools";
12    $MYSQL_H="localhost";

14
      // Variables
16    // $portlist Contient la liste des ports du hit parade
      // $port [] [0] contient le numero du port
18    // $port [] [1] contient la description du port
      // $port [] [2] contient le total du traffic du port par router
20    // $port [] [3] contient l'ip du routeur selectionné

22    // $router[] contient la liste des routeurs dans la base
      // $interface [numero routeur] [X] [0] contient le numéro
24    // de l'interface X du [numero routeur]
      // voir le tableau $router[]
26    // $routerselect = chaine contenant le "where" d'un select construit
```

```
// sur base des données de la base
//
// $sommeBytesTotal = total du traffic du port courant;
//
// $queryXXXX, $resultXXXXX et $rowXXXX servent de variable
// temporaire aux requêtes XXXX
//
// $port [X] contient la liste des hit parade des ports, en ordre croissant
// ATTENTION: Du à la présence de l'élément 0 dans le tableau,
// on ne peut utiliser le while(port []) car le 0 est considéré comme faux !
// on utilisera un for each ou un for(sizeof).
//
//
//

if(!isset($seuil)) {
    $seuil = 1;
}
$dbh=ConnectMysql(); //connection à la base de données

$query = "select count(*) as total from porthCacheOut";
$result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$nombreDataCacheH = $row->total;

$query = "select count(*) as total from portdCacheOut";
$result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$nombreDataCacheD = $row->total;

$query = "select portHOut,portDOut,unix_timestamp(now()) as timenow from timeCache";
$result = mysql_query($query)
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
$row = mysql_fetch_object($result);
$timeCacheH = $row->portHOut;
$timeCacheD = $row->portDOut;
$timeNow = $row->timenow;

$doCacheH = 0;
$doCacheD = 0;

if($nombreDataCacheH == 0 || ($timeNow - $timeCacheH)>=21600) {
    $doCacheH = 1;
}
if($nombreDataCacheD == 0 || ($timeNow - $timeCacheD)>=43200) {
    $doCacheD = 1;
}

$query="select portOut from cacheEnCours";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
if($row->portOut == 1) {
    print "<H3>Please Wait, Cache construction already in action ! </H3><br>";
    flush();
    while($row->portOut == 1) {
        $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        $row = mysql_fetch_object($result);
    }
    $doCacheH = 0;
    $doCacheD = 0;
}

if($doCacheH) {
```

```
94
    $query = "update cacheEnCours set portOut = 1";
96  $result = mysql_query($query)
        or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
98
    print ("<H3>Cache under construction (5 min AGG)</H3><br>");
100 flush();
    $sommeBytesTotal = 0;
102
    $query2='truncate table porthCacheOut';
104 $result2 = mysql_query($query2)
       or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
106

108 // Somme Traffic entrant

110 for($boucle=0;$boucle<48;$boucle++) {
       $query = 'select sum(bytesrcin+bytesrcdstin) as total from portResumeH_'.$boucle.'';
112    $result = mysql_query($query)
           or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
114 ".mysql_error($dbh)."<br>");
       $row=mysql_fetch_object($result);
116    $sommeBytesTotal += $row->total;
       mysql_free_result($result);
118 }

120 // Récupérationde l'ensemble des données sur les ports
    // Utilisation d'un tableau (indice = port)
122
    for($boucle=0;$boucle<48;$boucle++) {
124
       $query = 'select port,';
126    $query.= 'sum(bytesrcin) as srcout,';
       $query.= 'sum(bytedstin) as dstout,';
128    $query.= 'sum(bytesrcdstin) as srcdstout ';
       $query.= 'FROM portResumeH_'.$boucle;
130    $query.= ' group by port';
       $query.= ' order by port';
132
       $result = mysql_query($query)
134       or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
       while($row=mysql_fetch_object($result)) {
136       $port[$row->port][0] += $row->srcout;
          $port[$row->port][1] += $row->dstout;
138       $port[$row->port][2] += $row->srcdstout;
          $port[$row->port][3] += $row->srcout+$row->dstout+$row->srcdstout;
140    }
       mysql_free_result($result);
142 }

144 $nombreelement = count($port);

146 //Creation du tableau des totaux pour le tri
    for($boucle=0;$boucle<$nombreelement;$boucle++) {
148    $cle = "'".$boucle."'";
       if($port[$boucle][3]) {
150       $total[$cle] = $port[$boucle][3];
       }
152    else {
          $total[$cle] = 0;
154    }
    }
156 //Triage du tableau des résultats
    flush();
158 arsort($total,SORT_NUMERIC);
    reset($total);
160 flush();
```

```
162     while((list($key,$value)= each($total))) {
            $key = str_replace("'","",$key);
164         $pourcentagesrc = ($port[$key][0]/$sommeBytesTotal)*100;
            $pourcentagedst = ($port[$key][1]/$sommeBytesTotal)*100;
166         $pourcentagesrcdst = ($port[$key][2]/$sommeBytesTotal)*100;
            $pourcentagetotal = ($port[$key][3]/$sommeBytesTotal)*100;
168         $query = "insert into porthCacheOut values(".$key.",".
                        $pourcentagesrc.",".$pourcentagedst.",".
170                     $pourcentagesrcdst.",".$pourcentagetotal.")";
            $result = mysql_query($query)
172             or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
        }
174     $query = "update timeCache set portHOut = ".$timeNow."";
        mysql_query($query)
176         or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");

178     if(!$doCacheD) {
            $query = "update cacheEnCours set portOut = 0";
180         $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
182     }
    }
184
    if($doCacheD) {
186     if(!$doCacheH) {
            $query = "update cacheEnCours set portOut = 1";
188         $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
190     }
        unset($port);
192     print ("<H3>Cache under construction (1H AGG)</H3><br>");
        flush();
194     $sommeBytesTotal = 0;
        unset($port);
196     $query2='truncate table portdCacheOut';
        $result2 = mysql_query($query2)
198         or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');

200     // Somme Traffic entrant

202     for($boucle=0;$boucle<7;$boucle++) {
            $query = 'select sum(bytesrcin+bytesrcdstin) as total from portResumeD_'.$boucle.'';
204         $result = mysql_query($query)
                or die ("Query sum bytes failed. <br> Query: ".$query."<br> Reason: %%@
206 ".mysql_error($dbh)."<br>");
            $row=mysql_fetch_object($result);
208         $sommeBytesTotal += $row->total;
            mysql_free_result($result);
210     }

212     // Récupérationde l'ensemble des données sur les ports
        // Utilisation d'un tableau (indice = port)
214
        for($boucle=0;$boucle<7;$boucle++) {
216
            $query = 'select port,';
218         $query.= 'sum(bytesrcin) as srcout,';
            $query.= 'sum(bytedstin) as dstout,';
220         $query.= 'sum(bytesrcdstin) as srcdstout ';
            $query.= 'FROM portResumeD_'.$boucle;
222         $query.= ' group by port';
            $query.= ' order by port';
224
            $result = mysql_query($query)
226             or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
            while($row=mysql_fetch_object($result)) {
```

```
228             $port[$row->port][0] += $row->srcout;
                $port[$row->port][1] += $row->dstout;
230             $port[$row->port][2] += $row->srcdstout;
                $port[$row->port][3] += $row->srcout+$row->dstout+$row->srcdstout;
232         }
            mysql_free_result($result);
234     }
        $nombreelement = count($port);
236
        //Creation du tableau des totaux pour le tri
238     for($boucle=0;$boucle<$nombreelement;$boucle++) {
            $cle = "'".$boucle."'";
240         if($port[$boucle][3]) {
                $total[$cle] = $port[$boucle][3];
242         }
            else {
244             $total[$cle] = 0;
            }
246     }
        //Triage du tableau des résultats
248     flush();
        arsort($total,SORT_NUMERIC);
250     reset($total);
        flush();
252
        while((list($key,$value)= each($total))) {
254         $key = str_replace("'","",$key);
            $pourcentagesrc = ($port[$key][0]/$sommeBytesTotal)*100;
256         $pourcentagedst = ($port[$key][1]/$sommeBytesTotal)*100;
            $pourcentagesrcdst = ($port[$key][2]/$sommeBytesTotal)*100;
258         $pourcentagetotal = ($port[$key][3]/$sommeBytesTotal)*100;
            $query = "insert into portdCacheOut values(".$key.",".
260                     $pourcentagesrc.",".$pourcentagedst.",".
                        $pourcentagesrcdst.",".$pourcentagetotal.")";
262         $result = mysql_query($query)
                or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
264     }
        $query = "update timeCache set portDOut = ".$timeNow."";
266     mysql_query($query)
            or die ("Query :".$query." failed.<br> Error: ".mysql_error($dbh)."<br>");
268
        $query = "update cacheEnCours set portOut = 0";
270     $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
272 }

274 //Chargement de la description des ports
    $query2='select number,description from PortDescription where type="tcp" order by number';
276 $result2 = mysql_query($query2)
        or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
278 $boucle=0;
    while($row2 = mysql_fetch_object($result2)) {
280     $portdescription[$row2->number] = $row2->description;
        $boucle++;
282 }
    mysql_free_result($result2);
284
    unset($port);
286
    $query="select number,
288             pourcentagesrc,
                pourcentagedst,
290             pourcentagesrcdst,
                pourcentagetotal
292         from porthCacheOut
            where pourcentagetotal > ".$seuil."";
294 $result = mysql_query($query)
```

```
    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query.'<br>');
296 $boucle=0;
  while($row = mysql_fetch_object($result)) {
298     $port[$boucle][0] = $row->number;
        $port[$boucle][1] = $row->pourcentagesrc;
300     $port[$boucle][2] = $row->pourcentagedst;
        $port[$boucle][3] = $row->pourcentagesrcdst;
302     $port[$boucle][4] = $row->pourcentagetotal;
        $boucle++;
304 }
  mysql_free_result($result);
306


308
  // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
310 //de 1% de traffic
  ?>
312 <form action="netport2out.php" method="post">
  <center>Down limit display:
314 <input type="text" name="seuil" size=10 maxlength=10 value="<?print $seuil?>"></center><br>
  <br>
316 <input type="submit" value="Envoyer">
  </form>
318 <h4>Click on the port to see it's detailed graph<br>
  Data range:5 min<br>
320 Data age: max 48H<br>
  graph type: 12H<br>
322 data here under: Total generated traffic with srcport and dest port on leaving traffic</h4><br>
  <form method="post" action="netflowportaggout.php">
324 <table border="0" cellspacing="2" cellpadding="2" align="center">
  <tr><th> </th><th>Port</th>
326     <th>% src</th><th>% dst</th><th>% srcdst</th>
        <th>% total</th><th>Description</th></tr>
328 <?
        flush();
330     //for($boucle=0;$boucleport<$nombreelement;$boucleport++){
        $boucle =0;
332     for($boucle2=0;$boucle2<4;$boucle2++) {
           $totalboucle[$boucle2] = 0;
334     }
        $nombreport = count($port);
336     for($boucle=0;$boucle<$nombreport;$boucle++) {
           $numeroport = $port[$boucle][0];
338        $pourcentagesrc= $port[$boucle][1];
           $pourcentagedst= $port[$boucle][2];
340        $pourcentagesrcdst= $port[$boucle][3];
           $pourcentagetotal=  $port[$boucle][4];
342        print '
           <tr>
344        <td align = "center">
              <input type="checkbox" name= "srcport[]" value=" '.$numeroport.'">
346           <input type="hidden"  name="interval" value="H">
           </td>
348        <td align="center">
              <a href="netflowportout.php?srcport='.$numeroport.'
350                   &description='.$portdescription[$numeroport].'
                     &interval=H" target="_blank">'.$numeroport.'</a></td>
352        <td align="center">';
           printf("%2.2f",$pourcentagesrc);
354        $totalboucle[0] += $pourcentagesrc;
           print'
356        </td>
           <td align="center">';
358        printf("%2.2f",$pourcentagedst);
           $totalboucle[1] += $pourcentagedst;
360        print'
           </td>
```

```
362         <td align="center">';
            printf("%2.2f",$pourcentagesrcdst);
364         $totalboucle[2] += $pourcentagesrcdst;
            print '
366         </td>
            <td align="center">';
368         printf("%2.2f",$pourcentagetotal);
            $totalboucle[3] += $pourcentagetotal;
370         print '
            </td>
372         <td align="center">'.$portdescription[$numeroport]. '</td></tr>';
            flush();
374      }
         print '
376      <tr>
            <td align="center">
378            <input type="submit" value="Draw Cumulated Graph">
               </form>
380         </td>
            <td align="center"> </td>
382         <td align="center">';
         printf("%2.2f",$totalboucle[0]);
384      print '
            </td>
386         <td align="center">';
         printf("%2.2f",$totalboucle[1]);
388      print '
            </td>
390         <td align="center">';
         printf("%2.2f",$totalboucle[2]);
392      print '
            </td>
394         <td align="center">';
         printf("%2.2f",$totalboucle[3]);
396      print '</td>
            <td align="center">Total monitored</td>
398         </tr>
         </table><br><br>
400      ';
         print '<a href="netflowportin.php?interval=1&version=1"
402           target="_blank">Click to see complete Traffic (2 days)</a><br><br>';
   // Affichage du résultat de la requête ci dessus avec sélection sur les AS ayant plus
404 //de 1% de traffic

406 $timefin=time();
   $timetotal = $timefin-$timedebut;
408 print 'Execution Time (sec): ';
   print $timetotal."<br>";
410
   /// Traffic 7 jours aggrégé par heure
412 $sommeBytesTotal = 0;
   unset($port);
414 unset($total);

416 $query="select number,
                pourcentagesrc,
418             pourcentagedst,
                pourcentagesrcdst,
420             pourcentagetotal
         from portdCacheOut
422      where pourcentagetotal > ".$seuil."";
   $result = mysql_query($query)
424    or die ('query get list as failed: '.mysql_error($dbh).'<br>Query: '.$query2.'<br>');
   $boucle=0;
426 while($row = mysql_fetch_object($result)) {
      $port[$boucle][0] = $row->number;
428   $port[$boucle][1] = $row->pourcentagesrc;
```

```
    $port[$boucle][2] = $row->pourcentagedst;
430     $port[$boucle][3] = $row->pourcentagesrcdst;
    $port[$boucle][4] = $row->pourcentagetotal;
432     $boucle++;
    }
434 mysql_free_result($result);

436

438 // Affichage du résultat de la erquête ci dessus avec sélection sur les AS ayant plus
    //de 1% de traffic
440 ?>
    <h4>Click on the port to see it's detailed graph<br>
442 Data range:1 H<br>
    Data age: max 7 Days<br>
444 graph type: 24H<br>
    <form method="post" action="netflowportaggout.php">
446 <table border="0" cellspacing="2" cellpadding="2" align="center">
    <tr><th> </th><th>Port</th>
448     <th>% src</th><th>% dst</th><th>% srcdst</th>
    <th>% total</th><th>Description</th></tr>
450 <?
    flush();
452     //for($boucle=0;$boucleport<$nombreelement;$boucleport++){
    $boucle =0;
454     for($boucle2=0;$boucle2<4;$boucle2++) {
        $totalboucle[$boucle2] = 0;
456     }
    $nombreport = count($port);
458     for($boucle=0;$boucle<$nombreport;$boucle++) {
        $numeroport = $port[$boucle][0];
460         $pourcentagesrc= $port[$boucle][1];
        $pourcentagedst= $port[$boucle][2];
462         $pourcentagesrcdst= $port[$boucle][3];
        $pourcentagetotal=  $port[$boucle][4];
464         print '
        <tr>
466         <td align = "center">
            <input type="checkbox" name= "srcport[]" value="'.$numeroport.'">
468         <input type="hidden" name="interval" value="D">
        </td>
470         <td align="center">
        <a href="netflowportout.php?srcport='.$numeroport.'
472             &description='.$portdescription[$numeroport].'
            &interval=H" target="_blank">'.$numeroport.'</a></td>
474         <td align="center">';
        printf("%2.2f",$pourcentagesrc);
476         $totalboucle[0] += $pourcentagesrc;
        print'
478         </td>
        <td align="center">';
480         printf("%2.2f",$pourcentagedst);
        $totalboucle[1] += $pourcentagedst;
482         print'
        </td>
484         <td align="center">';
        printf("%2.2f",$pourcentagesrcdst);
486         $totalboucle[2] += $pourcentagesrcdst;
        print'
488         </td>
        <td align="center">';
490         printf("%2.2f",$pourcentagetotal);
        $totalboucle[3] += $pourcentagetotal;
492         print'
        </td>
494         <td align="center">'.$portdescription[$numeroport].'</td></tr>';
        flush();
```

```
496     }
        print '
498     <tr>
           <td align="center">
500           <input type="submit" value="Draw Cumulated Graph">
              </form>
502        </td>
           <td align="center"> </td>
504        <td align="center">';
        printf("%2.2f",$totalboucle[0]);
506     print '
           </td>
508        <td align="center">';
        printf("%2.2f",$totalboucle[1]);
510     print '
           </td>
512        <td align="center">';
        printf("%2.2f",$totalboucle[2]);
514     print '
           </td>
516        <td align="center">';
        printf("%2.2f",$totalboucle[3]);
518     print '</td>
           <td align="center">Total monitored</td>
520        </tr>
        </table><br><br>
522     ';
    print '<br><br><a href="netflowportout.php?interval=T&version=2"
524         target="_blank">Click to see complete traffic (7 days)</a><br>';
    print '<br><br><a href="net.php">back</a><br>';
526

528 # FIN QUERY
    mysql_close($dbh); // Closing connection
530 $timefin=time();
    $timetotal = $timefin-$timedebut;
532 print 'Execution Time (sec): ';
    print $timetotal;
534 Pied2("");
    ?>
```

Fichier : netflowport.php

```
 2 <?php
   require "./lib/Html.php";
 4 require "./lib/Mysql.php";
   require "./lib/Whois.php";
 6 require "./lib/Network.php";
   require "router.php";
 8
   require ("./jpgraph-1.8/src/jpgraph.php");
10 require ("./jpgraph-1.8/src/jpgraph_line.php");
   require ("./jpgraph-1.8/src/jpgraph_bar.php");
12 require ("./jpgraph-1.8/src/jpgraph_log.php");

14
   $dbh=ConnectMysql();
16 $minheureH=0;
   $minheureD=0;
18 $mintableH=0;
   $mintableD=0;
20
   # QUERY
22 $routerselectin = getSelectRouterin();
   $routerselectout = getSelectRouterout();
24 switch ($interval) {
```

```
case 'H':
    for($boucle=0;$boucle<48;$boucle++) {
        $query = "select min(heure) as heure from portResumeH_".$boucle."";
        $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
      if(($boucle==0 || !($minheureH)) && $row->heure)  {
       $minheureH = $row->heure;
       $mintableH = $boucle;
      }
      elseif($row->heure) {
       if(($row->heure < $minheureH) && $row->heure) {
          $minheureH = $row->heure;
          $mintableH = $boucle;
       }
      }
    }
    $ConvertMBits=8/300;
    for($boucle=0;$boucle<48;$boucle++) {
        $table = ($mintableH+$boucle)%48;
        $query = "  select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                      heure,
                      sum(bytesrcin+bytedstin+bytesrcdstin)/1000 as rs
                FROM portResumeH_".$table."
                where port in (".$srcport.")
                group by heure
                order by heure";
        $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        while ($row = mysql_fetch_object($result)) {
            $cle = ($row->heure-$minheureH)/300;
            $data[$cle]=$row->rs*$ConvertMBits;
            $ydata[$cle]=$row->d;
        }

        $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                      heure,
                      sum(bytesrcout+bytedstout+bytesrcdstout)/1000 as rs
                FROM portResumeH_".$table."
                where port in (".$srcport.")
                group by heure
                order by heure";

        $result2 = mysql_query($query2)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        while ($row = mysql_fetch_object($result2)) {
             $cle = ($row->heure-$minheureH)/300;
           $data2[$cle]+=$row->rs*$ConvertMBits;
        }
    }

    break;
case 'D':
    for($boucle=0;$boucle<7;$boucle++) {
        $query = "select min(heure) as heure from portResumeD_".$boucle."";
        $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
      if(($boucle==0 || !($minheureD)) && $row->heure)  {
       $minheureD = $row->heure;
       $mintableD=$boucle;
      }
      elseif ($row->heure) {
       if($row->heure < $minheureD && $row->heure) {
          $minheureD = $row->heure;
          $mintableD = $boucle;
       }
```

```
92          }
        }
94      $ConvertMBits=8/3600;
        for($boucle=0;$boucle<7;$boucle++) {
96          $table = ($mintableD+$boucle)%7;
            $query = "  select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
98                          heure,
                            sum(bytesrcin+bytedstin+bytesrcdstin)/1000 as rs
100                 FROM portResumeD_".$table."
                    where port in (".$srcport.")
102                 group by heure
                    order by heure";
104         $result = mysql_query($query)
               or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
106         while ($row = mysql_fetch_object($result)) {
               $cle = ($row->heure-$minheureD)/3600;
108            $data[$cle]=$row->rs*$ConvertMBits;
               $ydata[$cle]=$row->d;
110         }

112         $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                            heure,
114                         sum(bytesrcout+bytedstout+bytesrcdstout)/1000 as rs
                    FROM portResumeD_".$table."
116                 where port in (".$srcport.")
                    group by heure
118                 order by heure";

120         $result2 = mysql_query($query2)
               or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
122         while ($row = mysql_fetch_object($result2)) {
                $cle = ($row->heure-$minheureD)/3600;
124             $data2[$cle]+=$row->rs*$ConvertMBits;
            }
126     }

128     break;

130 case 'T':
        switch($version) {
132     case '1':
            for($boucle=0;$boucle<48;$boucle++) {
134             $query = "select min(heure) as heure from portResumeH_".$boucle."";
                $result = mysql_query($query)
136                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
              $row = mysql_fetch_object($result);
138           if( ($boucle ==0 || !($minheureH)) && $row->heure)  {
               $minheureH = $row->heure;
140            $mintableH=$boucle;
              }
142           elseif ($row->heure) {
               if( ($row->heure<$minheureH) && $row->heure) {
144               $minheureH = $row->heure;
                  $mintableH = $boucle;
146            }
              }
148         }

150         $ConvertMBits=8/300;
            for($boucle=0;$boucle<48;$boucle++) {
152             $table = ($mintableH+$boucle)%48;
                $query = "  select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
154                             heure,
                                sum(bytesrcin+bytesrcdstin)/1000 as rs
156                     FROM portResumeH_".$table."
                        group by heure
158                     order by heure";
```

```
            $result = mysql_query($query)
160            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
            while ($row = mysql_fetch_object($result)) {
162            $cle = ($row->heure-$minheureH)/300;
               $data[$cle]=$row->rs*$ConvertMBits;
164            $ydata[$cle]=$row->d;
            }
166
            $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
168                        heure,
                           sum(bytesrcout+bytesrcdstout)/1000 as rs
170                FROM portResumeH_".$table."
                   group by heure
172                order by heure";

174         $result2 = mysql_query($query2)
               or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
176         while ($row = mysql_fetch_object($result2)) {
                $cle = ($row->heure-$minheureH)/300;
178            $data2[$cle]+=$row->rs*$ConvertMBits;
            }
180      }

182      break;

184   case '2' :
         for($boucle=0;$boucle<7;$boucle++) {
186         $query = "select min(heure) as heure from portResumeD_".$boucle."";
            $result = mysql_query($query)
188            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
            $row = mysql_fetch_object($result);
190         if(($boucle==0 || !($minheureD)) && $row->heure)  {
               $minheureD = $row->heure;
192            $mintableD=$boucle;
            }
194         elseif ($row->heure) {
               if($row->heure < $minheureD && $row->heure) {
196               $minheureD = $row->heure;
                  $mintableD = $boucle;
198            }
            }
200      }

202      $ConvertMBits=8/3600;
         for($boucle=0;$boucle<7;$boucle++) {
204         $table = ($mintableD+$boucle)%7;
            $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
206                        heure,
                           sum(bytesrcin+bytesrcdstin)/1000 as rs
208               FROM portResumeD_".$table."
                  group by heure
210               order by heure";
            $result = mysql_query($query)
212            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
            while ($row = mysql_fetch_object($result)) {
214            $cle = ($row->heure-$minheureD)/3600;
               $data[$cle]=$row->rs*$ConvertMBits;
216            $ydata[$cle]=$row->d;
            }
218
            $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
220                        heure,
                           sum(bytesrcout+bytesrcdstout)/1000 as rs
222                FROM portResumeD_".$table."
                   group by heure
224                order by heure";
```

```
226             $result2 = mysql_query($query2)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
228             while ($row = mysql_fetch_object($result2)) {
                        $cle = ($row->heure-$minheureD)/3600;
230                 $data2[$cle]+=$row->rs*$ConvertMBits;
                }
232         }

234         break;
    }
236
    break;
238 }

240 # FIN QUERY
    mysql_free_result($result); // Free result
242 mysql_close($dbh); // Closing connection
    /*
244 print $minheureH."<br>";
    print $mintableH."<br>";
246 print $minheureD."<br>";
    print $mintableD."<br>";
248
    print "Data:";
250 print_r($data);
    print "<br><br> data2";
252 print_r($data2);
    print "<br><br>Ydata:";
254 print_r($ydata);
    exit();
256
    */
258 //Create the graph
    $graph = new Graph(900,500);
260 $graph -> SetScale("textlin");
    #$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
262 // Set the margins
    $graph ->img->SetMargin(80,80,40,120);
264 if($interval=='T') {
        $port=" ALL PORT";
266 }
    else
268 {
        $port=$srcport;
270 }

272
    //Titles and layout stuff
274 $graph ->title->Set("PORT :".$port."");
    $graph ->xaxis->title->Set("Time");
276 $graph ->xaxis->SetTickLabels("Netflow");
    $graph ->xgrid->Show(true,false);
278 $graph ->xaxis->SetTextTickInterval(22);
    $graph->xaxis->SetTickLabels($ydata);
280 $graph->xaxis->SetLabelAngle(90);
    $graph ->yaxis->SetColor("blue");
282 $graph ->yaxis->SetWeight("1");
    $graph ->yaxis->title->Set("Mbit/s");
284 $graph ->yaxis->scale->ticks->SupressFirst();
    $graph ->SetShadow();
286 $graph ->legend->SetLayout(LEGEND_HOR);
    $graph ->legend->Pos(.5,.1,"center","top");
288 $graph ->ygrid->Show(true,false);

290 //Create linear graph for weight
    $lineplot = new LinePlot($data);
292 $lineplot ->SetColor("red");
```

```
//$lineplot ->SetFillColor("blue");
$lineplot ->mark->SetColor("red");
$lineplot ->SetWeight("2");
$lineplot ->SetLegend("Mbit/s FROM 5432");

$lineplot2 = new LinePlot($data2);
$lineplot2 ->SetColor("blue");
//$lineplot2 ->SetFillColor("red");
$lineplot2 ->mark->SetColor("blue");
$lineplot2 ->SetWeight("2");
$lineplot2 ->SetLegend("Mbit/s TO 5432");


//Draw the graphs
$graph->Add($lineplot);
$graph->Add($lineplot2);
$graph->Stroke();


?>
```

Fichier : netflowportin.php

```
<?php
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Whois.php";
require "./lib/Network.php";
require "router.php";

require ("./jpgraph-1.8/src/jpgraph.php");
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");

$dbh=ConnectMysql();
$minheureH=0;
$minheureD=0;
$mintableH=0;
$mintableD=0;

# QUERY
$routerselectin = getSelectRouterin();
$routerselectout = getSelectRouterout();
switch ($interval) {
case 'H':
    for($boucle=0;$boucle<48;$boucle++) {
        $query = "select min(heure) as heure from portResumeH_".$boucle."";
        $result = mysql_query($query)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
      if(($boucle==0 || !($minheureH)) && $row->heure)  {
       $minheureH = $row->heure;
       $mintableH = $boucle;
      }
      elseif($row->heure) {
       if(($row->heure < $minheureH) && $row->heure) {
          $minheureH = $row->heure;
          $mintableH = $boucle;
       }
      }
    }
    $ConvertMBits=8/300;
    for($boucle=0;$boucle<48;$boucle++) {
        $table = ($mintableH+$boucle)%48;
        $query = "  select DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
```

```
                heure,
46              sum(bytesrcin+bytedstin+bytesrcdstin)/1000 as rs
            FROM portResumeH_".$table."
48          where port in (".$srcport.")
            group by heure order by heure";
50      $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
52      while ($row = mysql_fetch_object($result)) {
            $cle = ($row->heure-$minheureH)/300;
54          $data[$cle]=$row->rs*$ConvertMBits;
            $ydata[$cle]=$row->d;
56      }

58      $query2 = "select DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                    heure,
60                  sum(bytesrcout+bytedstout+bytesrcdstout)/1000 as rs
            FROM portResumeH_".$table."
62          where port in (".$srcport.")
            group by heure order by heure";
64
        $result2 = mysql_query($query2)
66          or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        while ($row = mysql_fetch_object($result2)) {
68          $cle = ($row->heure-$minheureH)/300;
            $data2[$cle]+=$row->rs*$ConvertMBits;
70      }
    }
72
    break;
74 case 'D':
    for($boucle=0;$boucle<7;$boucle++) {
76      $query = "select min(heure) as heure from portResumeD_".$boucle."";
        $result = mysql_query($query)
78                  or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
80    if(($boucle==0 || !($minheureD)) && $row->heure)  {
      $minheureD = $row->heure;
82    $mintableD=$boucle;
      }
84    elseif ($row->heure) {
      if($row->heure < $minheureD && $row->heure) {
86        $minheureD = $row->heure;
          $mintableD = $boucle;
88    }
      }
90  }
    $ConvertMBits=8/3600;
92  for($boucle=0;$boucle<7;$boucle++) {
        $table = ($mintableD+$boucle)%7;
94      $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                    heure,
96                  sum(bytesrcin+bytedstin+bytesrcdstin)/1000 as rs
            FROM portResumeD_".$table."
98          where port in (".$srcport.")
            group by heure order by heure";
100     $result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
102     while ($row = mysql_fetch_object($result)) {
            $cle = ($row->heure-$minheureD)/3600;
104         $data[$cle]=$row->rs*$ConvertMBits;
            $ydata[$cle]=$row->d;
106     }

108     $query2 = " select  DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                    heure,sum(bytesrcout+bytedstout+bytesrcdstout)/1000 as rs
110         FROM portResumeD_".$table."
            where port in (".$srcport.")
```

```
112                 group by heure order by heure";

114         $result2 = mysql_query($query2)
               or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
116         while ($row = mysql_fetch_object($result2)) {
                $cle = ($row->heure-$minheureD)/3600;
118             $data2[$cle]+=$row->rs*$ConvertMBits;
            }
120     }

122     break;

124 case 'T':
        switch($version) {
126     case '1':
            for($boucle=0;$boucle<48;$boucle++) {
128             $query = "select min(heure) as heure from portResumeH_".$boucle."";
                $result = mysql_query($query)
130                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
                $row = mysql_fetch_object($result);
132             if( ($boucle ==0 || !($minheureH)) && $row->heure)  {
                   $minheureH = $row->heure;
134                $mintableH=$boucle;
                }
136             elseif ($row->heure) {
                   if( ($row->heure<$minheureH) && $row->heure) {
138                   $minheureH = $row->heure;
                      $mintableH = $boucle;
140                }
                }
142         }

144         $ConvertMBits=8/300;
            for($boucle=0;$boucle<48;$boucle++) {
146             $table = ($mintableH+$boucle)%48;
                $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
148                            heure,
                               sum(bytesrcin+bytesrcdstin)/1000 as rs
150                    FROM portResumeH_".$table."
                       group by heure
152                    order by heure";
                $result = mysql_query($query)
154                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
                while ($row = mysql_fetch_object($result)) {
156                $cle = ($row->heure-$minheureH)/300;
                   $data[$cle]=$row->rs*$ConvertMBits;
158                $ydata[$cle]=$row->d;
                }
160
                $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
162                            heure,sum(bytesrcout+bytesrcdstout)/1000 as rs
                       FROM portResumeH_".$table."
164                    group by heure
                       order by heure";
166
                $result2 = mysql_query($query2)
168                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
                while ($row = mysql_fetch_object($result2)) {
170                $cle = ($row->heure-$minheureH)/300;
                   $data2[$cle]+=$row->rs*$ConvertMBits;
172             }
            }
174         break;

176     case'2' :   for($boucle=0;$boucle<7;$boucle++) {
                    $query = "select min(heure) as heure from portResumeD_".$boucle."";
178                 $result = mysql_query($query)
```

```
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
180             $row = mysql_fetch_object($result);
                if(($boucle==0 || !($minheureD)) && $row->heure)  {
182                 $minheureD = $row->heure;
                    $mintableD=$boucle;
184             }
                elseif ($row->heure) {
186                 if($row->heure < $minheureD && $row->heure) {
                        $minheureD = $row->heure;
188                     $mintableD = $boucle;
                    }
190             }
            }
192
            $ConvertMBits=8/3600;
194         for($boucle=0;$boucle<7;$boucle++) {
                $table = ($mintableD+$boucle)%7;
196             $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                                heure,sum(bytesrcin+bytesrcdstin)/1000 as rs
198                         FROM portResumeD_".$table."
                            group by heure
200                         order by heure";
                $result = mysql_query($query)
202                 or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
                while ($row = mysql_fetch_object($result)) {
204                 $cle = ($row->heure-$minheureD)/3600;
                    $data[$cle]=$row->rs*$ConvertMBits;
206                 $ydata[$cle]=$row->d;
                }
208
                $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
210                             heure,
                                sum(bytesrcout+bytesrcdstout)/1000 as rs
212                         FROM portResumeD_".$table."
                            group by heure
214                         order by heure";

216             $result2 = mysql_query($query2)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
218             while ($row = mysql_fetch_object($result2)) {
                    $cle = ($row->heure-$minheureD)/3600;
220                 $data2[$cle]+=$row->rs*$ConvertMBits;
                }
222         }
            break;
224     }
        break;
226 }

228 # FIN QUERY
    mysql_free_result($result); // Free result
230 mysql_close($dbh); // Closing connection

232 //Create the graph
    $graph = new Graph(900,500);
234 $graph -> SetScale("textlin");
    #$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
236 // Set the margins
    $graph ->img->SetMargin(80,80,40,120);
238 if($interval=='T') {
        $port=" ALL PORT";
240 }
    else
242 {
        $port=$srcport;
244 }
```

```
246
    //Titles and layout stuff
248 $graph ->title->Set("PORT :".$port."");
    $graph ->xaxis->title->Set("Time");
250 $graph ->xaxis->SetTickLabels("Netflow");
    $graph ->xgrid->Show(true,false);
252 $graph ->xaxis->SetTextTickInterval(22);
    $graph->xaxis->SetTickLabels($ydata);
254 $graph->xaxis->SetLabelAngle(90);
    $graph ->yaxis->SetColor("blue");
256 $graph ->yaxis->SetWeight("1");
    $graph ->yaxis->title->Set("Mbit/s");
258 $graph ->yaxis->scale->ticks->SupressFirst();
    $graph ->SetShadow();
260 $graph ->legend->SetLayout(LEGEND_HOR);
    $graph ->legend->Pos(.5,.1,"center","top");
262 $graph ->ygrid->Show(true,false);

264 //Create linear graph for weight
    $lineplot = new LinePlot($data);
266 $lineplot ->SetColor("red");
    //$lineplot ->SetFillColor("blue");
268 $lineplot ->mark->SetColor("red");
    $lineplot ->SetWeight("2");
270 $lineplot ->SetLegend("Mbit/s FROM 5432");

272 $lineplot2 = new LinePlot($data2);
    $lineplot2 ->SetColor("blue");
274 //$lineplot2 ->SetFillColor("red");
    $lineplot2 ->mark->SetColor("blue");
276 $lineplot2 ->SetWeight("2");
    $lineplot2 ->SetLegend("Mbit/s TO 5432");
278

280 //Draw the graphs
    $graph->Add($lineplot);
282 $graph->Add($lineplot2);
    $graph->Stroke();
284

286 ?>
```

Fichier : netflowportout.php

```
 2 <?php
   require "./lib/Html.php";
 4 require "./lib/Mysql.php";
   require "./lib/Whois.php";
 6 require "./lib/Network.php";
   require "router.php";
 8
   require ("./jpgraph-1.8/src/jpgraph.php");
10 require ("./jpgraph-1.8/src/jpgraph_line.php");
   require ("./jpgraph-1.8/src/jpgraph_bar.php");
12 require ("./jpgraph-1.8/src/jpgraph_log.php");

14 $dbh=ConnectMysql();
   $minheureH=0;
16 $minheureD=0;
   $mintableH=0;
18 $mintableD=0;

20 # QUERY
   $routerselectin = getSelectRouterin();
22 $routerselectout = getSelectRouterout();
   switch ($interval) {
```

```
case 'H':
    for($boucle=0;$boucle<48;$boucle++) {
        $query = "select min(heure) as heure from portResumeH_".$boucle."";
        $result = mysql_query($query)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
      if(($boucle==0 || !($minheureH)) && $row->heure)  {
       $minheureH = $row->heure;
       $mintableH = $boucle;
      }
      elseif($row->heure) {
       if(($row->heure < $minheureH) && $row->heure) {
          $minheureH = $row->heure;
          $mintableH = $boucle;
       }
      }
    }
    $ConvertMBits=8/300;
    for($boucle=0;$boucle<48;$boucle++) {
        $table = ($mintableH+$boucle)%48;
        $query = "  select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
                        sum(bytesrcin+bytedstin+bytesrcdstin)/1000 as rs
                FROM portResumeH_".$table."
                where port in (".$srcport.")
                group by heure
                order by heure";
        $result = mysql_query($query)
           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        while ($row = mysql_fetch_object($result)) {
           $cle = ($row->heure-$minheureH)/300;
           $data[$cle]=$row->rs*$ConvertMBits;
           $ydata[$cle]=$row->d;
        }

        $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
                        sum(bytesrcout+bytedstout+bytesrcdstout)/1000 as rs
                FROM portResumeH_".$table."
                where port in (".$srcport.")
                group by heure
                order by heure";

        $result2 = mysql_query($query2)
           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
        while ($row = mysql_fetch_object($result2)) {
             $cle = ($row->heure-$minheureH)/300;
           $data2[$cle]+=$row->rs*$ConvertMBits;
        }
    }

    break;
case 'D':
    for($boucle=0;$boucle<7;$boucle++) {
        $query = "select min(heure) as heure from portResumeD_".$boucle."";
        $result = mysql_query($query)
           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
      $row = mysql_fetch_object($result);
      if(($boucle==0 || !($minheureD)) && $row->heure)  {
       $minheureD = $row->heure;
       $mintableD=$boucle;
      }
      elseif ($row->heure) {
       if($row->heure < $minheureD && $row->heure) {
          $minheureD = $row->heure;
          $mintableD = $boucle;
       }
```

```
        }
92      }
        $ConvertMBits=8/3600;
94      for($boucle=0;$boucle<7;$boucle++) {
           $table = ($mintableD+$boucle)%7;
96         $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
98                      sum(bytesrcin+bytedstin+bytesrcdstin)/1000 as rs
                   FROM portResumeD_".$table."
100                where port in (".$srcport.")
                   group by heure
102                order by heure";
           $result = mysql_query($query)
104           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
           while ($row = mysql_fetch_object($result)) {
106           $cle = ($row->heure-$minheureD)/3600;
              $data[$cle]=$row->rs*$ConvertMBits;
108           $ydata[$cle]=$row->d;
           }
110
           $query2 = " select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
112                     heure,
                        sum(bytesrcout+bytedstout+bytesrcdstout)/1000 as rs
114                FROM portResumeD_".$table."
                   where port in (".$srcport.")
116                group by heure
                   order by heure";
118
           $result2 = mysql_query($query2)
120           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
           while ($row = mysql_fetch_object($result2)) {
122             $cle = ($row->heure-$minheureD)/3600;
               $data2[$cle]+=$row->rs*$ConvertMBits;
124        }
        }
126
        break;
128
    case 'T':
130     switch($version) {
           case '1':
132           for($boucle=0;$boucle<48;$boucle++) {
                 $query = "select min(heure) as heure from portResumeH_".$boucle."";
134              $result = mysql_query($query)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
136            $row = mysql_fetch_object($result);
               if( ($boucle ==0 || !($minheureH)) && $row->heure)  {
138             $minheureH = $row->heure;
                $mintableH=$boucle;
140            }
               elseif ($row->heure) {
142             if( ($row->heure<$minheureH) && $row->heure) {
                   $minheureH = $row->heure;
144                $mintableH = $boucle;
               }
146            }
           }
148
           $ConvertMBits=8/300;
150        for($boucle=0;$boucle<48;$boucle++) {
              $table = ($mintableH+$boucle)%48;
152           $query = "  select   DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                        heure,
154                     sum(bytesrcin+bytesrcdstin)/1000 as rs
                   FROM portResumeH_".$table."
156                group by heure
                   order by heure";
```

```
158             $result = mysql_query($query)
                   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
160             while ($row = mysql_fetch_object($result)) {
                   $cle = ($row->heure-$minheureH)/300;
162                $data[$cle]=$row->rs*$ConvertMBits;
                   $ydata[$cle]=$row->d;
164             }

166             $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                            heure,
168                         sum(bytesrcout+bytesrcdstout)/1000 as rs
                      FROM portResumeH_".$table."
170                   group by heure
                      order by heure";
172
                $result2 = mysql_query($query2)
174                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
                while ($row = mysql_fetch_object($result2)) {
176                   $cle = ($row->heure-$minheureH)/300;
                   $data2[$cle]+=$row->rs*$ConvertMBits;
178             }
            }
180
            break;
182
        case '2' :
184         for($boucle=0;$boucle<7;$boucle++) {
               $query = "select min(heure) as heure from portResumeD_".$boucle."";
186            $result = mysql_query($query)
                   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
188           $row = mysql_fetch_object($result);
              if(($boucle==0 || !($minheureD)) && $row->heure)  {
190            $minheureD = $row->heure;
               $mintableD=$boucle;
192           }
              elseif ($row->heure) {
194            if($row->heure < $minheureD && $row->heure) {
                  $minheureD = $row->heure;
196               $mintableD = $boucle;
               }
198           }
            }
200
            $ConvertMBits=8/3600;
202         for($boucle=0;$boucle<7;$boucle++) {
               $table = ($mintableD+$boucle)%7;
204            $query = "  select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                            heure,
206                         sum(bytesrcin+bytesrcdstin)/1000 as rs
                      FROM portResumeD_".$table."
208                   group by heure
                      order by heure";
210            $result = mysql_query($query)
                   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
212            while ($row = mysql_fetch_object($result)) {
                   $cle = ($row->heure-$minheureD)/3600;
214                $data[$cle]=$row->rs*$ConvertMBits;
                   $ydata[$cle]=$row->d;
216            }

218            $query2 = " select    DATE_FORMAT(from_unixtime(heure),'%m/%d/%y %T') as d,
                            heure,
220                         sum(bytesrcout+bytesrcdstout)/1000 as rs
                      FROM portResumeD_".$table."
222                   group by heure
                      order by heure";
224
```

```
            $result2 = mysql_query($query2)
226             or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
            while ($row = mysql_fetch_object($result2)) {
228             $cle = ($row->heure-$minheureD)/3600;
                $data2[$cle]+=$row->rs*$ConvertMBits;
230         }
        }
232
        break;
234 }

236 break;
}
238
# FIN QUERY
240 mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection
242 /*
print $minheureH."<br>";
244 print $mintableH."<br>";
print $minheureD."<br>";
246 print $mintableD."<br>";

248 print "Data:";
print_r($data);
250 print "<br><br> data2";
print_r($data2);
252 print "<br><br>Ydata:";
print_r($ydata);
254 exit();

256 */
//Create the graph
258 $graph = new Graph(900,500);
$graph -> SetScale("textlin");
260 #$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
// Set the margins
262 $graph ->img->SetMargin(80,80,40,120);
if($interval=='T') {
264     $port=" ALL PORT";
}
266 else
{
268     $port=$srcport;
}
270

272 //Titles and layout stuff
$graph ->title->Set("PORT :".$port."");
274 $graph ->xaxis->title->Set("Time");
$graph ->xaxis->SetTickLabels("Netflow");
276 $graph ->xgrid->Show(true,false);
$graph ->xaxis->SetTextTickInterval(22);
278 $graph->xaxis->SetTickLabels($ydata);
$graph->xaxis->SetLabelAngle(90);
280 $graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
282 $graph ->yaxis->title->Set("Mbit/s");
$graph ->yaxis->scale->ticks->SupressFirst();
284 $graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_HOR);
286 $graph ->legend->Pos(.5,.1,"center","top");
$graph ->ygrid->Show(true,false);
288
//Create linear graph for weight
290 $lineplot = new LinePlot($data);
$lineplot ->SetColor("red");
```

```
292 //$lineplot ->SetFillColor("blue");
    $lineplot ->mark->SetColor("red");
294 $lineplot ->SetWeight("2");
    $lineplot ->SetLegend("Mbit/s FROM 5432");
296
    $lineplot2 = new LinePlot($data2);
298 $lineplot2 ->SetColor("blue");
    //$lineplot2 ->SetFillColor("red");
300 $lineplot2 ->mark->SetColor("blue");
    $lineplot2 ->SetWeight("2");
302 $lineplot2 ->SetLegend("Mbit/s TO 5432");

304
    //Draw the graphs
306 $graph->Add($lineplot);
    $graph->Add($lineplot2);
308 $graph->Stroke();

310
    ?>
```

Fichier : drawbgppeer.php

```
 2 <?PHP
   require "./lib/Html.php";
 4 require "./lib/Mysql.php";
   require "./lib/Cricket.php";
 6

 8 Entete2("Graphiques Analyse BGP ");

10 print "<center>Traffic repartition by Peer</center><br>";
   print "
12 <br>
   Calcul du traffic en cours<br>
14 ";
   flush();
16
   //Calcul du traffic by peer
18 exec("/home/cponsen/mysql/calcRealTraf.pl");

20 print "
   Calcul terminer
22 <br>
   ";
24 print '
   <img src="drawbgppeerD.php"><br>
26 <br><br>
   <img src="drawbgppeerS.php">
28 <br>
   <br>
30 <a href="net.php">Back</a><br>
   ';
32 Pied2("");
   ?>
```

Fichier : drawbgppeerD.php

```
 2 <?php
   require "./lib/Html.php";
 4 require "./lib/Mysql.php";
   require "./lib/Whois.php";
 6 require "./lib/Network.php";

 8 require ("./jpgraph-1.8/src/jpgraph.php");
```

```
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");

$dbh = connectMysql();
$query = "select idBgpPeer,Name from BgpPeer order by idBgpPeer";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
while($row = mysql_fetch_object($result)) {
    $asName[$row->idBgpPeer]=$row->Name;
}
$asName[0] = "BNIX";
$asName[5432] = "Skynet Core";
mysql_free_result($result);
mysql_close($dbh);


$User=$PHP_AUTH_USER;
$MYSQL_U="pdevemy";
$MYSQL_P="digital";
$MYSQL_D="flowtools";
$MYSQL_H="localhost";

$COLORJPGRAPH = file("color.txt");
$NBRCOLOR = count($COLORJPGRAPH);

# QUERY
$dbh=ConnectMysql();

$boucle = 0;

$query = "select idpeer,bytesIn,bytesOut from trafficByPeerD order by bytesIn";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$tailletableau = 0;
while ($row = mysql_fetch_object($result)) {
    $datain[] = (($row->bytesIn/169200)*8)/1000;
    $dataout[] = (($row->bytesOut/169200)*8)/1000;
    $ydata[] = $asName[$row->idpeer];
    $tailletableau++;
}
/*
print_r($datain);
print '<br>';
print '<br>';
print_r($dataout);
print '<br>';print '<br>';
print_r($ydata);print '<br>';
print ($tailletableau);
*/

# FIN QUERY
mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection


//Create the graph
$graph = new Graph(600,350);
$graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
// Set the margins
$graph ->img->SetMargin(80,80,40,120);
//Titles and layout stuff
//$graph ->title->Set("FROM AS".$srcas."");
$graph ->title->Set("BGP Statistics : Traffic for old 48H by Peer");
$graph ->xaxis->title->Set("Peer");
//$graph ->xaxis->SetTickLabels("XXX");
```

```
76 $graph ->xgrid->Show(true, false);
   $graph ->xaxis->SetTextTickInterval(1);
78 $graph->xaxis->SetTickLabels($ydata);
   $graph->xaxis->SetLabelAngle(90);
80 $graph ->yaxis->SetColor("blue");
   $graph ->yaxis->SetWeight("1");
82 $graph ->yaxis->title->Set("Traffic Volume (Mb/s)");
   $graph ->yaxis->scale->ticks->SupressFirst();
84 $graph ->SetShadow();
   $graph ->legend->SetLayout(LEGEND_HOR);
86 $graph ->legend->Pos(.05,.90,"right","bottom");
   $graph ->ygrid->Show(true, false);
88 $graph->yaxis->scale->SetGrace(20);

90 //Create linear graph for weight
   //for($boucle=0;$boucle<$tailletableau;$boucle++) {
92
       $barplot1 = new BarPlot($datain);
94     $barplot1->SetFillColor(trim($COLORJPGRAPH[2%$NBRCOLOR]));
       $barplot1->value->Show();
96     $barplot1->value->SetAngle(90);
       $barplot1->SetValuePos('top');
98     $barplot1->SetShadow();
       $barplot2 = new BarPlot($dataout);
100    $barplot2->SetFillColor(trim($COLORJPGRAPH[5%$NBRCOLOR]));
       $barplot2->value->Show();
102    $barplot2->value->SetAngle(90);
       $barplot2->SetShadow();
104    $barplot2->SetValuePos('top');
       $aggplot = new GroupBarPlot(array($barplot1,$barplot2));
106    $aggplot->SetLegend($ydata);
       $graph->Add($aggplot);
108    //$graph->Add($barplot1);
       //$graph->Add($barplot2);
110 //}

112 //Draw the graphs
   $graph->Stroke();
114

116 ?>
```

Fichier : drawbgppeerS.php

```
2  <?php
   require "./lib/Html.php";
4  require "./lib/Mysql.php";
   require "./lib/Whois.php";
6  require "./lib/Network.php";

8  require ("./jpgraph-1.8/src/jpgraph.php");
   require ("./jpgraph-1.8/src/jpgraph_line.php");
10 require ("./jpgraph-1.8/src/jpgraph_bar.php");
   require ("./jpgraph-1.8/src/jpgraph_log.php");
12
   $User=$PHP_AUTH_USER;
14 $MYSQL_U="pdevemy";
   $MYSQL_P="digital";
16 $MYSQL_D="BgpCheck";
   $MYSQL_H="localhost";
18
   $dbh = connectMysql();
20 $query = "select idBgpPeer,Name from BgpPeer order by idBgpPeer";
   $result = mysql_query($query)
22    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   while($row = mysql_fetch_object($result)) {
```

```
24      $asName[$row->idBgpPeer]=$row->Name;
    }
26  $asName[0] = "BNIX";
    $asName[5432] = "Skynet Core";
28  mysql_free_result($result);
    mysql_close($dbh);
30

32  $User=$PHP_AUTH_USER;
    $MYSQL_U="pdevemy";
34  $MYSQL_P="digital";
    $MYSQL_D="flowtools";
36  $MYSQL_H="localhost";

38  $COLORJPGRAPH = file("color.txt");
    $NBRCOLOR = count($COLORJPGRAPH);
40
    # QUERY
42  $dbh=ConnectMysql();

44  $boucle = 0;

46  $query = "select idpeer,bytesIn,bytesOut from trafficByPeer order by bytesIn";
    $result = mysql_query($query)
48      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
    $tailletableau = 0;
50  while ($row = mysql_fetch_object($result)) {
        $datain[] = (($row->bytesIn/518400)*8)/1000;
52      $dataout[] = (($row->bytesOut/518400)*8)/1000;
        $ydata[] = $asName[$row->idpeer];
54      $tailletableau++;
    }
56  /*
    print_r($datain);
58  print '<br>';
    print '<br>';
60  print_r($dataout);
    print '<br>';print '<br>';
62  print_r($ydata);print '<br>';
    print ($tailletableau);
64  */

66  # FIN QUERY
    mysql_free_result($result); // Free result
68  mysql_close($dbh); // Closing connection

70
    //Create the graph
72  $graph = new Graph(600,350);
    $graph -> SetScale("textlin");
74  #$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
    // Set the margins
76  $graph ->img->SetMargin(80,80,40,120);
    //Titles and layout stuff
78  //$graph ->title->Set("FROM AS".$srcas."");
    $graph ->title->Set("BGP Statistics : Traffic for old 6Days by peer");
80  $graph ->xaxis->title->Set("Peer");
    //$graph ->xaxis->SetTickLabels("XXX");
82  $graph ->xgrid->Show(true,false);
    $graph ->xaxis->SetTextTickInterval(1);
84  $graph->xaxis->SetTickLabels($ydata);
    $graph->xaxis->SetLabelAngle(90);
86  $graph ->yaxis->SetColor("blue");
    $graph ->yaxis->SetWeight("1");
88  $graph ->yaxis->title->Set("Traffic Volume (Mb/s)");
    $graph ->yaxis->scale->ticks->SupressFirst();
90  $graph ->SetShadow();
```

```
$graph ->legend->SetLayout(LEGEND_HOR);
$graph ->legend->Pos(.05,.90,"right","bottom");
$graph ->ygrid->Show(true,false);
$graph->yaxis->scale->SetGrace(20);

//Create linear graph for weight
//for($boucle=0;$boucle<$tailletableau;$boucle++) {

    $barplot1 = new BarPlot($datain);
    $barplot1->SetFillColor(trim($COLORJPGRAPH[2%$NBRCOLOR]));
    $barplot1->value->Show();
    $barplot1->value->SetAngle(90);
    $barplot1->SetValuePos('top');
    $barplot1->SetShadow();
    $barplot2 = new BarPlot($dataout);
    $barplot2->SetFillColor(trim($COLORJPGRAPH[5%$NBRCOLOR]));
    $barplot2->value->Show();
    $barplot2->value->SetAngle(90);
    $barplot2->SetShadow();
    $barplot2->SetValuePos('top');
    $aggplot = new GroupBarPlot(array($barplot1,$barplot2));
    $aggplot->SetLegend($ydata);
    $graph->Add($aggplot);
    //$graph->Add($barplot1);
    //$graph->Add($barplot2);
//}

//Draw the graphs
$graph->Stroke();


?>
```

Fichier : gestionrouter.php

```
<?PHP
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Cricket.php";
require "./lib/Whois.php";
require "./lib/Network.php";


# QUERY
if(!isset($detail)) {
    $detail = 0;
}

$dbh=ConnectMysql();
$query="select * from routerinterface where actual=1 order by routerip,numerointerface";
$query2="select * from routerdecription order by routerip";

$result = mysql_query($query2)
                or die("Query failed<br>Query: ".$query2."<br>".mysql_error($dbh)."<br>");
$bouclerouter=0;
while($row=mysql_fetch_object($result)) {
    $routerdesc[$bouclerouter][0] = $row->routerip;
    $routerdesc[$bouclerouter][1] = $row->description;
    $routerdesc[$bouclerouter][2] = 0;
    $bouclerouter++;
}
mysql_free_result($result);

$result = mysql_query($query)
                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
```

```
$boucle=0;
$bouclerouter=0;
$oldrouter = $routerdesc[0][0];
while($row=mysql_fetch_object($result)) {
      if(strcmp($oldrouter,$row->routerip)!= 0) {
            $bouclerouter++;
            $boucle=0;
            $oldrouter = $row->routerip;
      }
      $routerinterface[$bouclerouter][$boucle][0] = $row->numerointerface;
      $routerinterface[$bouclerouter][$boucle][1] = $row->typeinterface;
      $routerinterface[$bouclerouter][$boucle][2] = $row->idpeer;
      $routerinterface[$bouclerouter][$boucle][3] = $row->id;
      $routerdesc[$bouclerouter][2]++;
      $boucle++;
}
mysql_free_result($result);

// old one
if($detail==1) {
   $query3="select * from routerinterface where actual=0 order by routerip,heure,numerointerface";
   $result = mysql_query($query3)
                  or die("Query failed<br>Query: ".$query3."<br>".mysql_error($dbh)."<br>");
   $boucle=0;
   $bouclerouter=0;
   $oldrouter = $routerdesc[0][0];
   $routerdescold2[$bouclerouter]=0;
   $oldheure = 0;
   $boucleheure = 0;
   while($row=mysql_fetch_object($result)) {
         $queryheure = "select unix_timestamp(".$row->heure.") as heure";
         $resultheure = mysql_query($queryheure)
                  or die("Query failed<br>Query: ".$queryheure."<br>".mysql_error($dbh)."<br>");
     $rowheure = mysql_fetch_object($resultheure);
     $heure = $rowheure->heure;
         if($oldheure == 0) {
            $oldheure = $heure;
         }
         if(strcmp($oldrouter,$row->routerip)!= 0) {
               $bouclerouter++;
               $routerdescold2[$bouclerouter][0]=0;
               $routerdescold2[$bouclerouter][1]=0;
               $oldrouter = $row->routerip;
               $oldheure = 0;
         }
         if($oldheure != $heure) {
            $boucleheure++;
            $boucle=0;
            $routerdescold2[$bouclerouter][0]++;
            $routerdescold[$bouclerouter][$boucleheure]=0;
            print $routerdescold2[$bouclerouter][0]." : %%@
".$routerdescold[$bouclerouter][$boucleheure]."<br>";
         }
         $routerinterfaceold[$bouclerouter][$boucleheure][$boucle][0] = $row->numerointerface;
         $routerinterfaceold[$bouclerouter][$boucleheure][$boucle][1] = $row->typeinterface;
         $routerinterfaceold[$bouclerouter][$boucleheure][$boucle][2] = $row->idpeer;
         $routerinterfaceold[$bouclerouter][$boucleheure][$boucle][3] = $row->heure;
         $routerdescold[$bouclerouter][$boucleheure]++;
         $routerdescold2[$bouclerouter][1]++;
         $boucle++;
   }
mysql_free_result($result);


}
```

```
100 Entete2("Sky ITM: Routers Management");

102 ?>
<H2>Routers Interfaces Management</h2><br>
104 <br><br>
<center>Actual Congiuration</center>
106 <br>
<form name="router" method="post" action="gestionrouterconfirm.php">
108 <table border = "1" width="100%" cellspacing="0" cellspacing="0" align="center">
<tr>
110 <th>Router</th><th>Description</th><th>Interface</th><th>Type</th><th>Id Peer Connected</th>
</tr>
112 <?
$nombrerouter = count($routerdesc);
114 for($bouclerouter=0;$bouclerouter < $nombrerouter;$bouclerouter++) {
$nombreinterface = $routerdesc[$bouclerouter][2];
116 print '
<input type="hidden" name="routerdesc['.$bouclerouter.'][2]" %%@
118 value="'.$routerdesc[$bouclerouter][2].'">
<tr>
120 <td rowspan="'.$nombreinterface.'" valign="center" align="center">
<input type="hidden" name="routerdesc['.$bouclerouter.'][0]"
122 value="'.$routerdesc[$bouclerouter][0].'">
'.$routerdesc[$bouclerouter][0].'
124 </td>
<td rowspan="'.$nombreinterface.'" valign="center" align="center">
126 <input type="hidden" name="routerdesc['.$bouclerouter.'][1]"
value="'.$routerdesc[$bouclerouter][1].'">
128 '.$routerdesc[$bouclerouter][1].'
</td>
130 ';
for($boucleinterface=0;$boucleinterface < $nombreinterface;$boucleinterface++) {
132 if($boucleinterface > 0) {
print '
134 </tr>
<tr>';
136 }
print '
138 <td align = "center">
<input type="text" maxlength = "5" length="5"
140 name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][0]"
value="'.$routerinterface[$bouclerouter][$boucleinterface][0].'">
142 <input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][0]"
value="'.$routerinterface[$bouclerouter][$boucleinterface][0].'">
144 </td>
<td align = "center">
146 <input type="text" maxlength = "5" length="5"
name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][1]"
148 value="'.$routerinterface[$bouclerouter][$boucleinterface][1].'">
<input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][1]"
150 value="'.$routerinterface[$bouclerouter][$boucleinterface][1].'">
</td>
152 <td align = "center">
<input type="text" maxlength = "5" length="5"
154 name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][2]"
value="'.$routerinterface[$bouclerouter][$boucleinterface][2].'">
156 <input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][2]"
value="'.$routerinterface[$bouclerouter][$boucleinterface][2].'">
158 </td>
<input type="hidden" name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][3]"
160 value="'.$routerinterface[$bouclerouter][$boucleinterface][3].'">
<input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][3]"
162 value="'.$routerinterface[$bouclerouter][$boucleinterface][3].'">
';
164 }
print '
166 </tr>
```

```
    ';
}
print '</table>
<input type="submit" value="Update">
</form>
<br>
<br>
';

?>
<form action="gestionrouter.php" method="post">
Previous configurations ? (max 7 days)
<select name="detail">
<option value="1" <?if ($detail==1) { echo 'selected';}?>>Oui
<option value="0" <?if ($detail==0) { echo 'selected';}?>>Non
</select>
<br>
<input type="submit" value="See"><br>
</form>
<?

if($detail) {
    print '
    <table border = "1" width="100%" cellspacing="0" cellspacing="0" align="center">
    <tr>
    <th>Router</th><th>Description</th><th>Interface</th><th>Type</th><th>Id Peer
        Connected</th><th>Time</th>
    </tr>
    ';
    $nombrerouter = count($routerdesc);
    for($bouclerouter=0;$bouclerouter < $nombrerouter;$bouclerouter++) {
        $nombreheure = $routerdescold2[$bouclerouter][0];
        $nombreinterfacetotal = $routerdescold2[$bouclerouter][1];
        if($nombreinterfacetotal == 0) {
            $nombreinterfacetotal = 1;
        }
        print '
        <tr>
        <td rowspan="'.$nombreinterfacetotal.'" valign="center"
            align="center">'.$routerdesc[$bouclerouter][0].'</td>
        <td rowspan="'.$nombreinterfacetotal.'" valign="center"
            align="center">'.$routerdesc[$bouclerouter][1].'</td>
        ';
        for($boucleheure=0;$boucleheure < $nombreheure;$boucleheure++) {
            $nombreinterface = $routerdescold[$bouclerouter][$boucleheure];
            for($boucleinterface=0;$boucleinterface < $nombreinterface;$boucleinterface++) {
                if($boucleinterface > 0) {
                    print '
                    </tr>
                    <tr>';
                }
                print '
                <td align =
            "center">'.$routerinterfaceold[$bouclerouter][$boucleheure][$boucleinterface][0].'</td>
                <td align =
            "center">'.$routerinterfaceold[$bouclerouter][$boucleheure][$boucleinterface][1].'</td>
                <td align =
            "center">'.$routerinterfaceold[$bouclerouter][$boucleheure][$boucleinterface][2].'</td>
                <td align =
            "center">'.$routerinterfaceold[$bouclerouter][$boucleheure][$boucleinterface][3].'</td>
                ';
            }
        }
        print '
        </tr>
        ';
```

```
234     }
        print '
236     </table>
        ';
238
    }
240 print '
        <br>
242     <br>
        <a href="net.php">Home Page</a><br>
244     <br>
        ';
246

248 Pied2("");
    mysql_close($dbh);
250 ?>
```

Fichier : gestionrouterconfirm.php

```
 2 <?PHP
   require "./lib/Html.php";
 4 require "./lib/Mysql.php";
   require "./lib/Cricket.php";
 6 require "./lib/Whois.php";
   require "./lib/Network.php";
 8

10 # QUERY
   if(!isset($confirm)) {
12         $confirm = 0;
   }
14
   if($confirm == 1) {
16     $dbh=ConnectMysql();
       $nombrerouter = count($routerdesc);
18     for($bouclerouter=0;$bouclerouter < $nombrerouter;$bouclerouter++) {
           $nombreinterface = $routerdesc[$bouclerouter][2];
20         for($boucleinterface=0;$boucleinterface < $nombreinterface;$boucleinterface++) {
               $tableauinterface = &$routerinterface[$bouclerouter][$boucleinterface];
22             $tableauinterfaceold = &$routerinterfaceold[$bouclerouter][$boucleinterface];
               $taillebouclе = count($tableauinterface);
24             $update = 0;
               for($boucle=0;$boucle<$taillebouclе;$boucle++) {
26                 if(strcmp($tableauinterface[$boucle],$tableauinterfaceold[$boucle]) != 0) {
                       switch($boucle){
28                         case 0: $set[$update] = "numerointerface = ".$tableauinterface[$boucle];
                                   $update++;
30                                 break;
                           case 1: $set[$update] = "typeinterface = '".$tableauinterface[$boucle]."'";
32                                 $update++;
                                   break;
34                         case 2: $set[$update] = "idpeer = ".$tableauinterface[$boucle];
                                   $update++;
36                                 break;
                           case 3: break;
38                         default: print "Error, Wrong number of argument
                                 supplied in routerinterface[][]";
40                                  exit(2);
                                    break;
42                 }
               }
44             }
               if($update>0) {
46                 $query = "update routerinterface set ";
                   for($boucle = 0;$boucle<($update-1);$boucle++) {
```

```
48                  $query .= $set[$boucle]."," ;
                }
50              $query .= $set[$boucle]." where id = ".$tableauinterface[3];
                print $query."<br>";
52          }
        }
54  }
    mysql_close($dbh);
56  if($update > 0) {
        print "<center><H3>Update succesful</H3><center><br>" ;
58  }
    else {
60      print "<center><H3>Update canceled: No new Data supplied</H3><center><br>";
    }
62
}
64
    //query = "update table routerinterface".$set
66 Entete2("Sky ITM: Routers Interface Management");
?>
68 <H2>Router Interface Management</h2><br>
<br><br>
70 <?
if($confirm == 0) {
72  ?>
    <center>Actual Configuration</center>
74  <?
}
76 else {
    ?>
78  <center>New Configuration</center>
    <?
80 }
?>
82 <br>
<form name="router" method="post" action="gestionrouterconfirm.php">
84 <input type="hidden" name="confirm" value="1">
<table border = "1" width="100%" cellspacing="0" cellspacing="0" align="center">
86 <tr>
    <th>Router</th><th>Description</th><th>Interface</th><th>Type</th><th>Id Peer Connected</th>
88 </tr>
<?
90 $nombrerouter = count($routerdesc);
for($bouclerouter=0;$bouclerouter < $nombrerouter;$bouclerouter++) {
92  $nombreinterface = $routerdesc[$bouclerouter][2];
    print '
94  <input type="hidden" name="routerdesc['.$bouclerouter.'][2]"
        value="'.$routerdesc[$bouclerouter][2].'">
96  <tr>
    <td rowspan="'.$nombreinterface.'" valign="center" align="center">
98      <input type="hidden" name="routerdesc['.$bouclerouter.'][0]"
        value="'.$routerdesc[$bouclerouter][0].'">
100     '.$routerdesc[$bouclerouter][0].'
    </td>
102 <td rowspan="'.$nombreinterface.'" valign="center" align="center">
    <input type="hidden" name="routerdesc['.$bouclerouter.'][1]"
104     value="'.$routerdesc[$bouclerouter][1].'">
        '.$routerdesc[$bouclerouter][1].'
106 </td>

108 ';
    for($boucleinterface=0;$boucleinterface < $nombreinterface;$boucleinterface++) {
110     if($boucleinterface > 0) {
            print '
112         </tr>
            <tr>';
114     }
```

```
        print '
116     <td align = "center">
            <input type="text" maxlength = "5" length="5"
118             name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][0]"
                value="'.$routerinterface[$bouclerouter][$boucleinterface][0].'">
120         <input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][0]"
                value="'.$routerinterfaceold[$bouclerouter][$boucleinterface][0].'">
122     </td>
        <td align = "center">
124         <input type="text" maxlength = "5" length="5"
                name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][1]"
126             value="'.$routerinterface[$bouclerouter][$boucleinterface][1].'">
            <input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][1]"
128             value="'.$routerinterfaceold[$bouclerouter][$boucleinterface][1].'">
        </td>
130     <td align = "center">
            <input type="text" maxlength = "5" length="5"
132             name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][2]"
                value="'.$routerinterface[$bouclerouter][$boucleinterface][2].'">
134         <input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][2]"
                value="'.$routerinterfaceold[$bouclerouter][$boucleinterface][2].'">
136     </td>
        <input type="hidden" name="routerinterface['.$bouclerouter.']['.$boucleinterface.'][3]"
138             value="'.$routerinterface[$bouclerouter][$boucleinterface][3].'">
        <input type="hidden" name="routerinterfaceold['.$bouclerouter.']['.$boucleinterface.'][3]"
140             value="'.$routerinterface[$bouclerouter][$boucleinterface][3].'">
        ';
142 }
    print '
144 </tr>
    ';
146 }
    print '</table>
148 <input type="submit" value="CONFIRM">
    </form>
150 Once Confirm is clicked, modifications will be effective in the database<br>
    <br>
152 <a href="gestionrouteur.php">Router Management</a><br>
    <br>
154 <br>
    ';
156 Pied2("");
    ?>
```

Fichier : toptraffic.php

```
2 <?PHP
  require "./lib/Html.php";
4 require "./lib/Mysql.php";
  require "./lib/Cricket.php";
6 require "./lib/Whois.php";
  require "./lib/Network.php";
8
  # QUERY
10 Entete2("Sky ITM");
  print "
12 <H3> Top 100 IP/24 traffic entrance </H3><br>
  <br>
14 <table cellpadding='0' cellspacing='0' border='0'>
  <tr><th>IP</th></tr>
16 ";
  $dbh=ConnectMysql();
18 $query = 'select Ip from TrafficIp where Type="I" order by Bytes DESC limit 100';
  $result = mysql_query($query)
20                  or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
  $fp = fopen("files/top100.txt", "w");
```

```
22 while($row=mysql_fetch_object($result)) {
     print "
24   <tr> <td>
       $row->Ip
26   </td>
     </tr>
28   ";
     $pref = preg_split("/\./",$row->Ip);
30   $pref[3]++;
     $Ip = $pref[0].".".$pref[1].".".$pref[2].".".$pref[3]."\n";
32   fwrite($fp,$Ip);
   }
34 fclose($fp);
   print "
36 </table>
   <br>
38 <br>
   <a href='files/top100.txt'>Get Top 100 file</a><br>
40 <br>
   <center><a href='net.php'>Back</a></center>
42 ";

44 Pied2("");
   mysql_close($dbh);
46 ?>
```

Fichier : top100trafficFtp.php

```
2  <?PHP
   require "./lib/Html.php";
4  require "./lib/Mysql.php";
   require "./lib/Cricket.php";
6  require "./lib/Whois.php";
   require "./lib/Network.php";
8
   # QUERY
10 Entete2("Sky ITM");
   print "
12 <H3> Top 100 IP traffic entrance (FTP Traffic)</H3><br>
   <br>
14 <table cellpadding='2' cellspacing='2' border='0'>
   <tr><th>IP</th><th>Gb</th><th>% Total FTP Traffic</th></tr>
16 ";
   $dbh=ConnectMysql();
18 $query = 'select sum(Bytes) as total from TrafficIp21';
   $result = mysql_query($query)
20                 or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   $row = mysql_fetch_object($result);
22 $total = $row->total;

24 $query = 'select Ip,Bytes from TrafficIp21 order by Bytes DESC limit 100';
   $result = mysql_query($query)
26                 or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   $fp = fopen("files/top100ftp.txt", "w");
28 while($row=mysql_fetch_object($result)) {
     print "
30   <tr> <td align='center'>
       $row->Ip
32   </td>
     <td align='center'>
34 ";
   printf("%.2f",$row->Bytes/pow(1024,2));
36 print "
     </td>
38   <td align='center'>
     ";
```

```
40 printf ("%.2f",($row->Bytes/$total)*100);
   print "
42    </td>
      </tr>
44    ";
      $pref = preg_split("/\./",$row->Ip);
46    $Ip = $pref[0].".".$pref[1].".".$pref[2].".".$pref[3]."\n";
      fwrite($fp,$Ip);
48 }
   fclose($fp);
50 print "
   <tr>
52 <td>Total Traffic</td>
   <td align='center'>
54 ";
   printf("%.2f",$total/pow(1024,2));
56 print "
   </td>
58 <td align='center'>
   100
60 </td>
   </tr>
62 </table>
   <br>
64 <br>
   <a href='files/top100ftp.txt'>Get Top 100 file</a><br>
66 <br>
   <center><a href='net.php'>Back</a></center>
68 ";

70 Pied2("");
   mysql_close($dbh);
72 ?>
```

Fichier : top100trafficHttp.php

```
2 <?PHP
   require "./lib/Html.php";
4 require "./lib/Mysql.php";
   require "./lib/Cricket.php";
6 require "./lib/Whois.php";
   require "./lib/Network.php";
8
   # QUERY
10 Entete2("Sky ITM");
   print "
12 <H3> Top 100 IP traffic entrance (HTTP Traffic)</H3><br>
   <br>
14 <table cellpadding='2' cellspacing='2' border='0'>
   <tr><th>IP</th><th>GB</th><th>% total HTTP traffic</th></tr>
16 ";
   $dbh=ConnectMysql();
18 $query = 'select sum(Bytes) as total from TrafficIp80';
   $result = mysql_query($query)
20                  or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   $row = mysql_fetch_object($result);
22 $total = $row->total;

24 $query = 'select Ip,Bytes from TrafficIp80 order by Bytes DESC limit 100';
   $result = mysql_query($query)
26                  or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   $fp = fopen("files/top100http.txt", "w");
28 while($row=mysql_fetch_object($result)) {
      print "
30    <tr> <td align='center'>
         $row->Ip
```

```
32      </td>
        <td align='center'>
34      ";
        printf("%.2f",$row->Bytes/pow(1024,2));
36      print "
        </td>
38      <td align='center'>
        ";
40      printf ("%.2f",($row->Bytes/$total)*100);
        print "
42
        </td>
44      </tr>
        ";
46      $pref = preg_split("/\./",$row->Ip);
        $Ip = $pref[0].".".$pref[1].".".$pref[2].".".$pref[3]."\n";
48      fwrite($fp,$Ip);
    }
50  fclose($fp);
    print "
52  <tr>
    <td>Total Traffic</td>
54  <td align='center'>
    ";
56  printf("%.2f",$total/pow(1024,2));
    print "
58  </td>
    <td align='center'>
60  100
    </td>
62  </tr>
    </table>
64  <br>
    <br>
66  <a href='files/top100http.txt'>Get Top 100 file</a><br>
    <br>
68  <center><a href='net.php'>Back</a></center>
    ";
70
    Pied2("");
72  mysql_close($dbh);
    ?>
```

Fichier : displaysim.php

```
    <?PHP
2   require "./lib/Html.php";
    require "./lib/Mysql.php";
4   require "./lib/Cricket.php";
    require "./lib/Whois.php";
6   require "./lib/Network.php";

8   $MYSQL_U="pdevemy";
    $MYSQL_P="digital";
10  $MYSQL_D="BgpCheck";
    $MYSQL_H="localhost";
12
    # QUERY
14  Entete2("Sky Bat");

16  $dbh=ConnectMysql();
    print "
18  <H3>Simulation</H3><br>
    ";
20  $query = "  select    distinct IdBgpPeer,
                    Name,
22                  Description
```

```
            from   BgpPeer as a,
24                 PeerSimulation as b,
                   PeeringInfo as c
26          where IdBgpPeer = idpeer
                   and a.idPeeringInfo=c.idPeeringInfo
28          order by Description";
   $result = mysql_query($query)
30    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

32 print '
   Actual Simulation is made for Peer: <br>
34 <br>
   <table border="0" cellpadding="0" cellspacing="0" align="center" width="100%">
36 <tr><th align="center">Name</th><th>Type</th></tr>
   ';
38 $bnix = 0;
   while($row = mysql_fetch_object($result)) {
40    if($row->Description == "BNIX") {
         $bnix = 1;
42       $asName[$row->IdBgpPeer] = $row->Name;
         $listepeer[] = $row->IdBgpPeer;
44    }
      else {
46       print "
            <tr><td align='center'>
48          $row->Name
            </td>
50          <td align='center'>
            $row->Description
52          </td>
            </tr>
54          ";
         $asName[$row->IdBgpPeer] = $row->Name;
56       $listepeer[] = $row->IdBgpPeer;
      }
58 }
   if($bnix) {
60    print "
         <tr><td align='center'>
62          BNIX
         </td>
64       <td align='center'>
            BNIX
66       </td>
         </tr>
68       ";
   }
70
   $boucle = 0;
72 $listepeerstring = "";
   while($listepeer[$boucle]) {
74    if ($boucle <> 0) {
         $listepeerstring .= "&";
76       $listepeermysql .= ",";
      }
78    $listepeerstring .= "listepeer[]=".$listepeer[$boucle];
      $listepeermysql .= $listepeer[$boucle];
80    $boucle++;
   }
82
   $query = "truncate temporaire_Cumul_Sim";
84 mysql_query($query) or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   $query = "  insert into temporaire_Cumul_Sim
86          select    min(pathlong),
                  min(nbras),
88                prefix,
                  mask
```

```
90          from BGPDATA
            where idpeer in (".$listepeermysql.")
92          group by prefix,
                     mask ";
94
mysql_query($query)
96     or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
       $boucle = 0;
98
print "
100 </table>
    <br>
102 <img src='simdrawbgppathcumul.php'><br>
    <br>
104 <table border='0' cellpadding='2' cellspacing='2'>
    <tr><th>Pathlong</th><th>%</th><th>% Cumul</th><tr>
106 ";
    $query = "  select sum(Bytes) as total
108          from temporaireCalculGraphiquePonderation";
    $result = mysql_query($query)
110    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
    $row = mysql_fetch_object($result);
112 $totalBytes = $row->total;
    $query = "  select   pathlong,
114                 (sum(Bytes)/".$totalBytes.")*100 as total
            from temporaireCalculGraphiquePonderation
116         group by pathlong
            order by pathlong";
118 $result = mysql_query($query)
       or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
120 $cumul = 0;
    while($row=mysql_fetch_object($result)) {
122        $cumul += $row->total;
           if($cumul > 100) { $cumul = 100;}
124        print "
           <tr><td align='center'>
126           $row->pathlong
           </td>
128        <td align='center'>
              $row->total
130        </td>
           <td align='center'>
132           $cumul
           </td>
134        </tr>
           ";
136 }
    print "
138 </table><br>
    <br>
140 <br>
    <img src='simdrawbgpproxcumul.php'><br>
142 <br>
    <table border='0' cellpadding='2' cellspacing='2'>
144 <tr><th>NbrAS</th><th>%</th><th>% Cumul</th><tr>
    ";
146 $query = "  select   nbras,
                    (sum(Bytes)/".$totalBytes.")*100 as total
148         from temporaireCalculGraphiquePonderation
            group by nbras
150         order by nbras";
    $result = mysql_query($query)
152    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
    $cumul=0;
154 while($row=mysql_fetch_object($result)) {
           $cumul += $row->total;
156        if($cumul > 100) { $cumul = 100;}
```

```
        print "
158     <tr><td align='center'>
            $row->nbras
160     </td>
        <td align='center'>
162         $row->total
        </td>
164     <td align='center'>
            $cumul
166     </td>
        </tr>
168     ";
    }
170 print "
    </table><br>
172 <br>
    <a href='controlsimul.php'>back</a><br>
174 <br>
    ";
176 $query = "update verrou set simulationData = 0";
    $result = mysql_query($query)
178     or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
    Pied2("");
180 mysql_close($dbh);
```

Fichier : simdrawBGPpathcumul.php

```
    <?php
 2 require "./lib/Html.php";
   require "./lib/Mysql.php";
 4 require "./lib/Whois.php";
   require "./lib/Network.php";
 6
   require ("./jpgraph-1.8/src/jpgraph.php");
 8 require ("./jpgraph-1.8/src/jpgraph_line.php");
   require ("./jpgraph-1.8/src/jpgraph_bar.php");
10 require ("./jpgraph-1.8/src/jpgraph_log.php");
   $gJpgBrandTiming=true;
12
   $COLORJPGRAPH = file("color.txt");
14 $NBRCOLOR = count($COLORJPGRAPH);

16 # QUERY
   $dbh=ConnectMysql();
18 $boucle = 0;

20 $query = "  select   count(*) as total,
                   minPathLong
22          from temporaire_Cumul_Sim
            group by minPathLong";
24 $result = mysql_query($query)
       or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
26 $i=0;
   $tmp=0;
28 while ($row = mysql_fetch_object($result)) {
       $data[$i]=$row->total;
30     $ydata[$i]=$row->minPathLong;
       $i++;
32 }

34 $query = "  select   sum(Bytes) as total
            from temporaireCalculGraphiquePonderation";
36 $result = mysql_query($query) or die("Query failed<br>Query: %%@
   ".$query."<br>".mysql_error($dbh)."<br>");
38 $row = mysql_fetch_object($result);
   $totalBytes = $row->total;
40
```

```
$query = "  select   pathlong,
                (sum(Bytes)/".$totalBytes.")*100 as total
        from temporaireCalculGraphiquePonderation
        group by pathlong
        order by pathlong";
$result = mysql_query($query)
   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
while($row=mysql_fetch_object($result)) {
      if($row->pathlong == 1) {
         $y2datacumul[($row->pathlong-1)] = $row->total;
      }
      else {
         $y2datacumul[($row->pathlong-1)] = $row->total + $y2datacumul[($row->pathlong-2)];
         if($y2datacumul[($row->pathlong-1)] > 100) {
               $y2datacumul[($row->pathlong-1)] = 100;
         }
      }
      $y2data[($row->pathlong-1)] = $row->total;
}

# FIN QUERY
mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection
/*
print_r($y2data);
exit();*/

//Create the graph
$graph = new Graph(900,500);
$graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
// Set the margins
$graph ->img->SetMargin(40,120,80,40);

//Titles and layout stuff
$graph ->title->Set("BGP MinPathLong from Cumulated Peer");
$graph ->xaxis->title->Set("Nb AS");
//$graph ->xaxis->SetTickLabels("XXX");
$graph ->xgrid->Show(true,false);
//$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
$graph ->yaxis->title->Set("Nbr Prefix");
$graph ->yaxis->scale->ticks->SupressFirst();
//$graph->y2scale->SetAutoMax(110);
$graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_VER);
$graph ->legend->Pos(.05,.01,"right","top");
$graph ->ygrid->Show(true,false);
$graph->SetY2Scale("lin");


if($graphType == 1) {
   $graph->xaxis->HideTicks();

   $graph->xaxis->SetLabelFormat(" ");
   $graph->yaxis->HideTicks();

   $graph->yaxis->SetLabelFormat(" ");
}
else {
   $graph ->xaxis->SetTextTickInterval(1);
   $graph->xaxis->SetTickLabels($ydata);
}

//Create linear graph for weight
$lineplot = new LinePlot($data);
```

```
$lineplot ->SetColor(trim($COLORJPGRAPH[0]));
$lineplot ->mark->SetColor(trim($COLORJPGRAPH[0]));
$lineplot ->SetWeight("2");

$lineplot2=new LinePlot($y2data);
$lineplot2 ->SetColor(trim($COLORJPGRAPH[2]));
$lineplot2 ->mark->SetColor(trim($COLORJPGRAPH[2]));
$lineplot2 ->SetWeight("2");


$lineplot3=new LinePlot($y2datacumul);
$lineplot3 ->SetColor(trim($COLORJPGRAPH[4]));
$lineplot3 ->mark->SetColor(trim($COLORJPGRAPH[4]));
$lineplot3 ->SetWeight("2");


if($graphType == 0) {
    $lineplot ->SetLegend("Nb As Through");
    $lineplot2->SetLegend("% Skynet Traffic");
    $lineplot3->SetLegend("% Skynet Traffic cumulated");
}
$graph->Add($lineplot);
$graph->AddY2($lineplot2);
$graph->AddY2($lineplot3);


//Draw the graphs
$graph->Stroke();


?>
```

Fichier : simdrawBGPproxcumul.php

```
<?php
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Whois.php";
require "./lib/Network.php";

require ("./jpgraph-1.8/src/jpgraph.php");
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");

$COLORJPGRAPH = file("color.txt");
$NBRCOLOR = count($COLORJPGRAPH);

$gJpgBrandTiming=true;

# QUERY
$dbh=ConnectMysql();
$boucle = 0;

$query = "  select    count(*) as total,
                minNbrAs
        from temporaire_Cumul_Sim
        group by minNbrAs";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$i=0;

$tmp=0;
while ($row = mysql_fetch_object($result)) {

    $data[$i]=$row->total;
```

```
34      $ydata[$i]=$row->minPathLong;
        $i++;
36
}
38
$query = "  select   sum(Bytes) as total
40          from temporaireCalculGraphiquePonderation";
$result = mysql_query($query)
42      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$row = mysql_fetch_object($result);
44 $totalBytes = $row->total;

46 $query = "  select   nbras,
                    (sum(Bytes)/".$totalBytes.")*100 as total
48          from temporaireCalculGraphiquePonderation
            group by nbras
50          order by nbras";
$result = mysql_query($query)
52      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
while($row=mysql_fetch_object($result)) {
54          if($row->nbras == 1) {
                $y2datacumul[($row->nbras-1)] = $row->total;
56          }
            else {
58              $y2datacumul[($row->nbras-1)] = $row->total + $y2datacumul[($row->nbras-2)];
                if($y2datacumul[($row->nbras-1)] > 100) {
60                  $y2datacumul[($row->nbras-1)] = 100;
                }
62          }
            $y2data[($row->nbras-1)] = $row->total;
64 }

66
# FIN QUERY
68 mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection
70
/*print_r($y2data);
72 exit();*/

74 //Create the graph
$graph = new Graph(900,500);
76 $graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
78 // Set the margins
$graph ->img->SetMargin(40,120,80,40);
80
//Titles and layout stuff
82 $graph ->title->Set("BGP MinNbrAs from Cumulated Peer");
$graph ->xaxis->title->Set("Nb AS");
84 //$graph ->xaxis->SetTickLabels("XXX");
$graph ->xgrid->Show(true,false);
86 //$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
88 $graph ->yaxis->SetWeight("1");
$graph ->yaxis->title->Set("Nbr Prefix");
90 $graph ->yaxis->scale->ticks->SupressFirst();
//$graph->y2scale->SetAutoMax(110);
92 $graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_VER);
94 $graph ->legend->Pos(.05,.01,"right","top");
$graph ->ygrid->Show(true,false);
96 $graph->SetY2Scale("lin");

98
if($graphType == 1) {
100     $graph->xaxis->HideTicks();
```

```
102     $graph->xaxis->SetLabelFormat(" ");
        $graph->yaxis->HideTicks();
104
        $graph->yaxis->SetLabelFormat(" ");
106 }
    else {
108     $graph ->xaxis->SetTextTickInterval(1);
        $graph->xaxis->SetTickLabels($ydata);
110 }

112 //Create linear graph for weight
    $lineplot = new LinePlot($data);
114 $lineplot ->SetColor(trim($COLORJPGRAPH[0]));
    $lineplot ->mark->SetColor(trim($COLORJPGRAPH[0]));
116 $lineplot ->SetWeight("2");

118 $lineplot2=new LinePlot($y2data);
    $lineplot2 ->SetColor(trim($COLORJPGRAPH[2]));
120 $lineplot2 ->mark->SetColor(trim($COLORJPGRAPH[2]));
    $lineplot2 ->SetWeight("2");
122
    $lineplot3=new LinePlot($y2datacumul);
124 $lineplot3 ->SetColor(trim($COLORJPGRAPH[4]));
    $lineplot3 ->mark->SetColor(trim($COLORJPGRAPH[4]));
126 $lineplot3 ->SetWeight("2");


128

130 if($graphType == 0) {
        $lineplot ->SetLegend("Nb As diff");
132     $lineplot2->SetLegend("% Skynet Traffic");
        $lineplot3->SetLegend("% Skynet Traffic cumalated");
134 }
    $graph->Add($lineplot);
136 $graph->AddY2($lineplot2);
    $graph->AddY2($lineplot3);
138
    //Draw the graphs
140 $graph->Stroke();

142
    ?>
```

Fichier : color.txt

```
2 black
  bisque
4 blue
  brown
6 burlywood4
  cadetblue4
8 chartreuse1
  chocolate
10 coral
   cornsilk
12 cyan
   darkblue
14 gray5
   gray
16 green
   pink
18 magenta
   navy
20 orange
   purple
```

```
22 red
   yellow
```

Fichier : controlsimul.php

```
   <?PHP
 2 require "./lib/Html.php";
   require "./lib/Mysql.php";
 4 require "./lib/Cricket.php";
   require "./lib/Whois.php";
 6 require "./lib/Network.php";

 8 # QUERY
   Entete2("Sky Bat");
10
   $dbh=ConnectMysql();
12 print "
   <H3>Control Page of the Simulation Traffic Tool</H3><br>
14 ";
   $query = "select * from verrou";
16 $result = mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
18 $row = mysql_fetch_object($result);
   if($row->simulation == 1 || $row->simulationData == 1) {
20    print "<H3> Simulator is running. Please Wait before launching new simulation</h3>";
   }
22

24 $query = "  select    distinct Name,
                  Description
26          from  BgpPeer as a,
                  BgpTable_Results as b,
28                PeeringInfo as c
            where IdBgpPeer = idpeer
30                and a.idPeeringInfo=c.idPeeringInfo
            order by Description";
32 $result = mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
34
   print '
36 Actual Simulation is made for Peer: <br>
   <br>
38 <table border="0" cellpadding="0" cellspacing="0" align="center" width="100%">
   <tr><th align="center">Name</th><th>Type</th></tr>
40 ';
   $bnix = 0;
42 while($row = mysql_fetch_object($result)) {
      if($row->Description == "BNIX") {
44       $bnix = 1;
      }
46    else {
         print "
48          <tr><td align='center'>
            $row->Name
50          </td>
            <td align='center'>
52          $row->Description
            </td>
54          </tr>
            ";
56    }
   }
58 if($bnix) {
      print "
60       <tr><td align='center'>
            BNIX
62       </td>
```

```
        <td align='center'>
64          BNIX
        </td>
66      </tr>
        ";
68  }
    print "
70  </table>
    <br><br>
72  Please choose Peer you want to use for a new simulation and Press Generate Simulation<br>
    <br>
74  <form name='checkPeerSimulation' method='post' action='generateSim.php'>
    <table cellpadding='0' cellspacing='0'width='100%' border='0'>
76  <tr><th>Select</th><th>Name</th><th>Type</th>
    <tr>
78     <td align='center'><input type='checkbox' name='listpeersim[]' value='-1'></td>
       <td align='center'>BNIX</td>
80     <td align='center'>BNIX</td>
    </tr>
82  ";
    $query = "  select   IdBgpPeer,
84                   Name,
                     Description
86            from   BgpPeer as a,
                     PeeringInfo as b
88            where a.IdPeeringInfo in (2,5)
                     and a.IdPeeringInfo = b.IdPeeringInfo";
90  $result = mysql_query($query)
       or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
92
    while($row = mysql_fetch_object($result)) {
94     print "
       <tr>
96        <td align='center'><input type='checkbox' name='listpeersim[]' value='$row->IdBgpPeer'></td>
          <td align='center'>$row->Name</td>
98        <td align='center'>$row->Description</td>
       </tr>
100    ";
    }
102 print "
       </table>
104    <input type='submit' value='Generate Simulation'>
       </form>
106    <br>
       <a href='bgp.php'>back</a><br>
108    ";
    Pied2("");
110 mysql_close($dbh);
```

Fichier : generatesim.php

```
2   <?PHP
    require "./lib/Html.php";
4   require "./lib/Mysql.php";
    require "./lib/Cricket.php";
6   require "./lib/Whois.php";
    require "./lib/Network.php";
8
    # QUERY
10  Entete2("Sky Bat");

12  $dbh=ConnectMysql();
    $query = "select * from verrou";
14  $result = mysql_query($query)
                    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
16  $row = mysql_fetch_object($result);
```

```
if($row->simulation == 1 || $row->simulationData == 1) {
    print "<H3> Simulator already running. Please Re Use the simulator later</h3>";
    print "<a href='controlsimul.php'>Back to Control of Simulator</a>";
    Pied2("");
    mysql_close($dbh);
    exit();

}
$query = "update verrou set simulation = 1, simulationData = 1";
$result = mysql_query($query)
        or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
print "
<H3>Simulation</H3><br>
Attention: For security and sharing reason, a locksystem has been placed on data from simulator.<br>
Please visit the results to unlock the data and authorize other utilization of the simulator.<br>
<br>
<br>
Peer Selected for Simulation<br>
";
$bnix = 0;
$listepeerselect = "";
if(isset($listpeersim)) {
    $boucle = 0;
    $diffmoins1 = 0;
    while($listpeersim[$boucle]) {
        if($listpeersim[$boucle] != -1) {
            if($diffmoins1 != 0) {
                $listepeerselect .= ",";
            }
            $listepeerselect .= $listpeersim[$boucle] ;
            $diffmoins1 = 1;
        }
        else {
            $bnix = 1;
        }
        $boucle++;
    }
}

print '
<table border="0" cellpadding="0" cellspacing="0" align="center" width="100%">
<tr><th align="center">Name</th><th>Type</th></tr>
';
if($listepeerselect != "" ) {
    $query = "  select   Name,
                    Description
            from  BgpPeer as a,
                    PeeringInfo as b
            where IdBgpPeer IN ($listepeerselect)
                    and a.IdPeeringInfo = b.IdPeeringInfo
            order by Description";
    $result = mysql_query($query)
        or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
    while($row = mysql_fetch_object($result)) {
        print "
            <tr><td align='center'>
            $row->Name
            </td>
            <td align='center'>
            $row->Description
            </td>
            </tr>
            ";
    }
}
if($bnix) {
    print "
```

```
84        <tr><td align='center'>
             BNIX
86        </td>
          <td align='center'>
88           BNIX
          </td>
90        </tr>
          ";
92  }
    print "
94  </table>
    <br>
96  Inserting idPeer for simulation in table<br>
    ";
98  flush();
    if(isset($listpeersim)) {
100    $boucle = 0;
       $query = "truncate PeerSimulation";
102    $result = mysql_query($query)
                  or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
104    while($listpeersim[$boucle]) {
          if($listpeersim[$boucle] == -1) {
106          $query = "select IdBgpPeer from BgpPeer where IdPeeringInfo = 1";
             $result = mysql_query($query)
108                  or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

110       while($row = mysql_fetch_object($result)) {
             $query = "insert into PeerSimulation values(".$row->IdBgpPeer.")";
112             $result2 = mysql_query($query)
                     or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
114
          }
116    }
          else {
118
             $query = "insert into PeerSimulation values(".$listpeersim[$boucle].")";
120          $result = mysql_query($query)
                     or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
122    }
          $boucle++;
124    }
    }
126 print "
    Insertion terminated<br>
128 <br>
    Starting Generating Routing Table Simulation<br>
130 <br>
    ";
132
    flush();
134 system("/home/cponsen/mysql/genPrefixSim.pl",$result);

136 if($result!= 1) {
       print "
138    Error genPrefixSim.pl check the script <br>
       <br>
140    $result <br>
       <br>
142    ";
       $query = "update verrou set simulation = 0, simulationData = 0";
144    $result = mysql_query($query)
            or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
146    exit();
    }
148 flush();

150 print "
```

```
   Generation terminated<br>
152 <br>
   Starting simulating through simulation table<br>
154 <br>
   ";
156
   flush();
158 system("/home/cponsen/mysql/GroupementMask.pl",$result);

160 if($result != 1) {
      print "
162    Error GroupementMask.pl check the script <br>
      <br>
164    $result <br>
      <br>
166    ";
      $query = "update verrou set simulation = 0,simulationData = 0";
168    $result = mysql_query($query)
           or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
170    exit();
   }
172 flush();

174 print "
   Grouping information for Displaying<br>
176 ";
   flush();
178 $query = "truncate table temporaireCalculGraphiquePonderation" ;
   $result = mysql_query($query)
180                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");

182 $query = "insert into temporaireCalculGraphiquePonderation
              select prefix,mask,Bytes,pathlong,nbras from BgpTable_Results
184           group by prefix,mask" ;
   $result = mysql_query($query)
186                or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   flush();
188
   print "
190 Grouping Terminated<br>
   <br>
192 Simulation terminated<br>
   <br>
194 <br>
   <a href='displaysim.php'>Click here to see the results</a><br>
196 <br>
   <a href='controlsimul.php'>back</a><br>
198 <br>
   ";
200 $query = "update verrou set simulation = 0";
   $result = mysql_query($query)
202        or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
   Pied2("");
204 mysql_close($dbh);
```

Fichier : bgpselect.php

```
 2 <?php

 4 require "./lib/Html.php";
   require "./lib/Mysql.php";
 6 require "./lib/Cricket.php";

 8 $dbh = ConnectMysql();

10 $query = "  Select distinct idpeer,
```

```
            Name
12      from BGPDATA d, BgpPeer b
        where d.idpeer=b.idBgpPeer
14      order by b.idPeeringInfo";
$result = mysql_query($query)
16   or die("Failed to select idpeer: ".$query."<br>".mysqlerror($dbh)."<br>");

18 Entete2("Sky BAT");

20 print '
<H3>BGP Table Analyse Tool</H3>
22 <br>
Please select BGP Peer wich you want to see informations for<br>
24   <form action="draw.php" method="POST" name="selection peer">
';
26
$boucle=0;
28 while($row = mysql_fetch_object($result)) {
   print '<input type="checkbox" name="listepeer[]"
30         value="'.$row->idpeer.'|'.$row->Name.'">'.$row->Name.'<br>';
}
32
mysql_free_result($result);
34
print '  <input type="submit" value="Envoyer">
36   </form>';

38 Pied2("");
?>
```

Fichier : draw.php

```
<?PHP
2 require "./lib/Html.php";
require "./lib/Mysql.php";
4 require "./lib/Cricket.php";

6 $dbh=ConnectMysql();

8 Entete2("Sky Bat");
$listepeerstring = "";
10 $boucle=0;
while($listepeer[$boucle]) {
12   if ($boucle <> 0) {
       $listepeerstring .= "&";
14     $listeasName .= "&";
       $listepeermysql .= ",";
16     $listepeerform .= "&";
     }
18   list($peer,$name) = preg_split("/[|]/",$listepeer[$boucle]);
     $listepeer2[] = $peer;
20   $listepeermysql .= $peer;
     $listepeerstring .= "listepeer[".$boucle."]=".$peer;
22   $listeasName .= "asName[".$peer."]=".$name;
     $listepeerform .= "listepeer[]=".$listepeer[$boucle];
24   $boucle++;
}
26
//Check des cumuls
28 $query = "select idpeer from temporaire_Cumul_Peer";
$result = mysql_query($query)
30   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
while($row = mysql_fetch_object($result)) {
32   $tableidpeer[] = $row->idpeer;
}
34 $diffarray = array_diff($tableidpeer,$listepeer2);
if(count($listepeer2) != count($tableidpeer) || count($diffarray) != 0 ) {
```

```
36
    $query = "truncate temporaire_Cumul";
38  mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
40
    $query = "truncate temporaire_Cumul_Peer";
42  mysql_query($query)
      or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
44
    $query = "insert into temporaire_Cumul select min(pathlong),min(nbras),prefix,mask
46              from BGPDATA
                where idpeer in (".$listepeermysql.")
48              group by prefix,mask ";
    mysql_query($query)
50    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
    $boucle = 0;
52  while($listepeer2[$boucle]) {
      $query = "insert into temporaire_Cumul_Peer values(".$listepeer2[$boucle].")";
54    mysql_query($query)
        or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
56    $boucle++;
    }
58 }
  if(!isset($graphType)) {
60  $graphType = 0;
  }
62 ?>
  <H3> BGP Analyses Graphs </H3>
64 <br>
  <form action="draw.php?<?echo $listepeerform?>" method = "post">
66 Graph Type: <br>
  <select name="graphType">
68 <option value="0" <? if($graphType == 0) { echo "selected"; }?> >Full
  <option value="1" <? if($graphType == 1) { echo "selected"; }?> >Anonym
70 </select>
  <br>
72 <input type="submit" value="Re-Draw">
  </form>
74 <br><br>
  <center>Nbr Distinct AS Through</center><br>
76 <img src="drawbgp.php?graphType=<?echo $graphType?>&<?echo %%@
  $listepeerstring?>&<?echo$listeasName?>"><br>
78 <br><br>
  <center>Path Length</center><br>
80 <img src="drawbgppath.php?graphType=<?echo $graphType?>&<?echo %%@
  $listepeerstring?>&<?echo$listeasName?>"><br>
82 <br><br>
  <center>Minimum Path Length using cumulated data from selected Peer</center><br>
84 <img src="drawbgppathcumul.php?graphType=<?echo $graphType?>&<?echo %%@
  $listepeerstring?>&<?echo$listeasName?>"><br>
86 <br><br>
  <center>Minimum Nbr Distinct AS Through using cumulated data from selected Peer</center><br>
88 <img src="drawbgpproxcumul.php?graphType=<?echo $graphType?>&<?echo %%@
  $listepeerstring?>&<?echo$listeasName?>"><br>
90 <br>
  <br>
92 <center><a href="bgpselect.php">Back</a></center>
  <?
94 Pied2("");
  ?>
```

Fichier : drawBGP.php

```
  <?php
2 require "./lib/Html.php";
  require "./lib/Mysql.php";
4 require "./lib/Whois.php";
```

```
require "./lib/Network.php";

require ("./jpgraph-1.8/src/jpgraph.php");
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");

$COLORJPGRAPH = file("color.txt");
$NBRCOLOR = count($COLORJPGRAPH);
$gJpgBrandTiming=true;

# QUERY
$dbh=ConnectMysql();
$boucle = 0;
$listepeerstring = "";
while($listepeer[$boucle]) {
    if ($boucle <> 0) {
        $listepeerstring .= ",";
    }
    $listepeerstring .= $listepeer[$boucle];
    $boucle++;
}
$query = "  select    idpeer,
                count(*) as total,
                nbras
          from  BGPDATA
          where idpeer in (".$listepeerstring.")
          group by idpeer,
                   nbras
          order by idpeer,
                   nbras";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$i=0;
$tailletableau = count($listepeer);
for($boucle=0;$boucle<$tailletableau;$boucle++) {
    for($boucle2=0;$boucle2 < 10;$boucle2++) {
        $data [$boucle] [$boucle2] = 0;
    }
}

for($boucle2=0;$boucle2 < 10;$boucle2++) {
        $ydata [$boucle2] = $boucle2;
}

$i=-1;
$tmp=0;
while ($row = mysql_fetch_object($result)) {
    if ($tmp <> $row->idpeer) {
            $tmp = $row->idpeer;
            $i++;
            $name[$i] = $row->idpeer;
    }
    $data[$i][$row->nbras]=$row->total;
}

# FIN QUERY
mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection

//Create the graph
$graph = new Graph(900,500);
$graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
// Set the margins
```

```
$graph ->img->SetMargin(60,300,50,50);
if($interval=='T') {
    $port=" ALL PORT";
}
else
{
    $port=$srcport;
}

//Titles and layout stuff
//$graph ->title->Set("FROM AS".$srcas."");
$graph ->title->Set("BGP Nbr As traversal");
$graph ->xaxis->title->Set("Nb AS");
//$graph ->xaxis->SetTickLabels("XXX");
$graph ->xgrid->Show(true,false);
//$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
$graph ->yaxis->scale->ticks->SupressFirst();
$graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_VER);
$graph ->legend->Pos(.05,.01,"right","top");
$graph ->ygrid->Show(true,false);
$graph ->yaxis->title->Set("Nbr Prefix");
if($graphType == 1) {
    $graph->xaxis->HideTicks();

    $graph->xaxis->SetLabelFormat(" ");
    $graph->yaxis->HideTicks();

    $graph->yaxis->SetLabelFormat(" ");
}
else {
    $graph ->xaxis->SetTextTickInterval(1);
    $graph->xaxis->SetTickLabels($ydata);
}

for($boucle=0;$boucle<$tailletableau;$boucle++) {

    $lineplot[$boucle] = new LinePlot($data[$boucle]);
    $lineplot[$boucle] ->SetColor(trim($COLORJPGRAPH[$boucle%$NBRCOLOR]));
//$lineplot ->SetFillColor("blue");
    $lineplot[$boucle] ->mark->SetColor(trim($COLORJPGRAPH[$boucle%$NBRCOLOR]));
    $lineplot[$boucle] ->SetWeight("2");
    if($graphType == 0) {
        $lineplot[$boucle] ->SetLegend($asName[$name[$boucle]]);
    }
// $lineplot[$boucle] ->value->Show();
// $lineplot[$boucle] ->value->SetColor($COLORJPGRAPH[$boucle%6]);
    $graph->Add($lineplot[$boucle]);
}

//Draw the graphs
$graph->Stroke();


?>
```

Fichier : drawBGPpath.php

```
<?php
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Whois.php";
require "./lib/Network.php";

```

```
require ("./jpgraph-1.8/src/jpgraph.php");
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");

$COLORJPGRAPH = file("color.txt");
$NBRCOLOR = count($COLORJPGRAPH);
$gJpgBrandTiming=true;

# QUERY
$dbh=ConnectMysql();
$boucle = 0;
$listepeerstring = "";
while($listepeer[$boucle]) {
    if ($boucle <> 0) {
        $listepeerstring .= ",";
    }
    $listepeerstring .= $listepeer[$boucle];
    $boucle++;
}

$query = "  select    idpeer,
                count(*) as total,
                pathlong
          from  BGPDATA
          where idpeer in (".$listepeerstring.")
          group by idpeer,
                   pathlong
          order by idpeer,
                   pathlong";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$i=0;
$tailletableau = count($listepeer);

for($boucle=0;$boucle<$tailletableau;$boucle++) {
    for($boucle2=0;$boucle2 < 10;$boucle2++) {
        $data [$boucle] [$boucle2] = 0;
    }
}

for($boucle2=0;$boucle2 < 10;$boucle2++) {
        $ydata [$boucle2] = $boucle2;
}

$i=-1;
$tmp=0;
while ($row = mysql_fetch_object($result)) {
    if ($tmp <> $row->idpeer) {
            $tmp = $row->idpeer;
            $i++;
            $name[$i] = $row->idpeer;
    }
    $data[$i][$row->pathlong]=$row->total;

}


# FIN QUERY
mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection


//Create the graph
$graph = new Graph(900,500);
$graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
```

```
// Set the margins
$graph ->img->SetMargin(60,300,50,50);
if($interval=='T') {
    $port=" ALL PORT";
}
else
{
    $port=$srcport;
}

//Titles and layout stuff
//$graph ->title->Set("FROM AS".$srcas."");
$graph ->title->Set("BGP As Path Length");
$graph ->xaxis->title->Set("Nb AS");
//$graph ->xaxis->SetTickLabels("XXX");
$graph ->xgrid->Show(true,false);
//$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
$graph ->yaxis->title->Set("Nbr Prefix");
$graph ->yaxis->scale->ticks->SupressFirst();
$graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_VER);
$graph ->legend->Pos(.05,.01,"right","top");
$graph ->ygrid->Show(true,false);
if($graphType == 1) {
    $graph->xaxis->HideTicks();

    $graph->xaxis->SetLabelFormat(" ");
    $graph->yaxis->HideTicks();

    $graph->yaxis->SetLabelFormat(" ");
}
else {
    $graph ->xaxis->SetTextTickInterval(1);
    $graph->xaxis->SetTickLabels($ydata);
}

//Create linear graph for weight
for($boucle=0;$boucle<$tailletableau;$boucle++) {

    $lineplot[$boucle] = new LinePlot($data[$boucle]);
    $lineplot[$boucle] ->SetColor(trim($COLORJPGRAPH[$boucle%$NBRCOLOR]));
//$lineplot ->SetFillColor("blue");
    $lineplot[$boucle] ->mark->SetColor(trim($COLORJPGRAPH[$boucle%$NBRCOLOR]));
    $lineplot[$boucle] ->SetWeight("2");
    if($graphType == 0) {
        $lineplot[$boucle] ->SetLegend($asName[$name[$boucle]]);
    }
    //$lineplot[$boucle] ->value->Show();
    //$lineplot[$boucle]->value->SetColor($COLORJPGRAPH[$boucle%6]);
    $graph->Add($lineplot[$boucle]);
}

//Draw the graphs
$graph->Stroke();


?>
```

Fichier : drawBGPpathcumul.php

```
<?php
require "./lib/Html.php";
require "./lib/Mysql.php";
require "./lib/Whois.php";
```

```
require "./lib/Network.php";

require ("./jpgraph-1.8/src/jpgraph.php");
require ("./jpgraph-1.8/src/jpgraph_line.php");
require ("./jpgraph-1.8/src/jpgraph_bar.php");
require ("./jpgraph-1.8/src/jpgraph_log.php");
$gJpgBrandTiming=true;

$COLORJPGRAPH = file("color.txt");
$NBRCOLOR = count($COLORJPGRAPH);

# QUERY
$dbh=ConnectMysql();
$boucle = 0;
$listepeerstring = "";
while($listepeer[$boucle]) {
    if ($boucle <> 0) {
        $listepeerstring .= ",";
        $listepeerlegend .= " ";
    }
    $listepeerstring .= $listepeer[$boucle];
    $listepeerlegend .= $asName[$listepeer[$boucle]];
    $boucle++;
}

$query = "  select    count(*) as total,
                minPathLong
          from  temporaire_Cumul
          group by minPathLong";
$result = mysql_query($query)
   or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$i=0;

$i=0;
$tmp=0;
while ($row = mysql_fetch_object($result)) {

    $data[$i]=$row->total;
    $ydata[$i]=$row->minPathLong;
    $i++;

}


# FIN QUERY
mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection


//Create the graph
$graph = new Graph(900,500);
$graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
// Set the margins
$graph ->img->SetMargin(40,120,40,40);

//Titles and layout stuff
$graph ->title->Set("BGP MinPathLong from Cumulated Peer");
$graph ->xaxis->title->Set("Nb AS");
//$graph ->xaxis->SetTickLabels("XXX");
$graph ->xgrid->Show(true,false);
//$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
$graph ->yaxis->title->Set("Nbr Prefix");
$graph ->yaxis->scale->ticks->SupressFirst();
$graph ->SetShadow();
```

```
72 $graph ->legend->SetLayout(LEGEND_VER);
   $graph ->legend->Pos(.05,.01,"right","top");
74 $graph ->ygrid->Show(true,false);
   if($graphType == 1) {
76    $graph->xaxis->HideTicks();

78    $graph->xaxis->SetLabelFormat(" ");
      $graph->yaxis->HideTicks();
80
      $graph->yaxis->SetLabelFormat(" ");
82 }
   else {
84    $graph ->xaxis->SetTextTickInterval(1);
      $graph->xaxis->SetTickLabels($ydata);
86 }

88 //Create linear graph for weight
   $lineplot = new LinePlot($data);
90 $lineplot ->SetColor(trim($COLORJPGRAPH[0]));
   $lineplot ->mark->SetColor(trim($COLORJPGRAPH[0]));
92 $lineplot ->SetWeight("2");
   if($graphType == 0) {
94    $lineplot ->SetLegend("Nb As Through");
   }
96 $graph->Add($lineplot);

98
   //Draw the graphs
100 $graph->Stroke();

102
   ?>
```

Fichier : drawBGPproxcumul.php

```
   <?php
 2 require "./lib/Html.php";
   require "./lib/Mysql.php";
 4 require "./lib/Whois.php";
   require "./lib/Network.php";
 6
   require ("./jpgraph-1.8/src/jpgraph.php");
 8 require ("./jpgraph-1.8/src/jpgraph_line.php");
   require ("./jpgraph-1.8/src/jpgraph_bar.php");
10 require ("./jpgraph-1.8/src/jpgraph_log.php");

12 $COLORJPGRAPH = file("color.txt");
   $NBRCOLOR = count($COLORJPGRAPH);
14
   $gJpgBrandTiming=true;
16
   # QUERY
18 $dbh=ConnectMysql();
   $boucle = 0;
20 $listepeerstring = "";
   while($listepeer[$boucle]) {
22    if ($boucle <> 0) {
         $listepeerstring .= ",";
24       $listepeerlegend .= " ";
      }
26    $listepeerstring .= $listepeer[$boucle];
      $listepeerlegend .= $asName[$listepeer[$boucle]];
28    $boucle++;
   }
30
   $query = "  select    count(*) as total,
32                minNbrAs
```

```
            from   temporaire_Cumul
            group by minNbrAs";
$result = mysql_query($query)
    or die("Query failed<br>Query: ".$query."<br>".mysql_error($dbh)."<br>");
$i=0;

$i=0;
$tmp=0;
while ($row = mysql_fetch_object($result)) {

    $data[$i]=$row->total;
    $ydata[$i]=$row->minPathLong;
    $i++;

}

# FIN QUERY
mysql_free_result($result); // Free result
mysql_close($dbh); // Closing connection


//Create the graph
$graph = new Graph(900,500);
$graph -> SetScale("textlin");
#$graph->SetBackgroundImage("logoskynet.png",BGIMG_CENTER);
// Set the margins
$graph ->img->SetMargin(60,120,50,50);

//Titles and layout stuff
$graph ->title->Set("BGP MinNbrAs from Cumulated Peer");
$graph ->xaxis->title->Set("Nb AS");
//$graph ->xaxis->SetTickLabels("XXX");
$graph ->xgrid->Show(true,false);
//$graph->xaxis->SetLabelAngle(90);
$graph ->yaxis->SetColor("blue");
$graph ->yaxis->SetWeight("1");
$graph ->yaxis->title->Set("Nbr Prefix");
$graph ->yaxis->scale->ticks->SupressFirst();
$graph ->SetShadow();
$graph ->legend->SetLayout(LEGEND_VER);
$graph ->legend->Pos(.05,.01,"right","top");
$graph ->ygrid->Show(true,false);
if($graphType == 1) {
    $graph->xaxis->HideTicks();

    $graph->xaxis->SetLabelFormat(" ");
    $graph->yaxis->HideTicks();

    $graph->yaxis->SetLabelFormat(" ");
}
else {
    $graph ->xaxis->SetTextTickInterval(1);
    $graph->xaxis->SetTickLabels($ydata);
}

//Create linear graph for weight
$lineplot = new LinePlot($data);
$lineplot ->SetColor(trim($COLORJPGRAPH[0]));
$lineplot ->mark->SetColor(trim($COLORJPGRAPH[0]));
$lineplot ->SetWeight("2");
if($graphType == 0) {
    $lineplot ->SetLegend("Nb As diff");
}
$graph->Add($lineplot);

```

```
100 //Draw the graphs
    $graph->Stroke();
102

104 ?>
```

4.2 Code Perl

Fichier : calcRealTraf.pl

```
    #! /usr/bin/perl
 2  use DBI;
    use router2;
 4  $wherein = getWhereRouterIn();
    $whereout = getWhereRouterOut();
 6  my $peer = @_[0];
    my $database =DBI->connect("DBI:mysql:flowtools:localhost:3306","flowtools", "netflow");
 8  $query = "truncate table trafficByPeer";
    $statement = $database->prepare($query);
10  $statement->execute
       or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
12
    $query = "truncate table trafficByPeerD";
14  $statement = $database->prepare($query);
    $statement->execute
16     or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";

18
    $query = "truncate table trafficByAs";
20  $statement = $database->prepare($query);
    $statement->execute
22     or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";

24  $query = "truncate table trafficByPref";
    $statement = $database->prepare($query);
26  $statement->execute
       or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
28
    print "Calcul du traffic par Peer (6 jours)\n";
30  for($boucle=0;$boucle<6;$boucle++) {
       $query = "  select   idpeersrc,
32                    sum(bytes)
                from  asD_".$boucle."
34              where destas = 5432
                      and srcas <> 5432
36              group by idpeersrc";
       $statement = $database->prepare($query);
38     $statement->execute
          or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
40     while(@row = $statement->fetchrow_array()) {
          $data[$row[0]][0]+= $row[1];
42        $data[$row[0]][1] =0;
       }
44  }
    for($boucle=0;$boucle<6;$boucle++) {
46        $query = "    select   idpeerdst,
                        sum(bytes)
48                from  asD_".$boucle."
                  where srcas = 5432
50                      and destas <> 5432
                  group by idpeerdst";
52        $statement = $database->prepare($query);
          $statement->execute
54         or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
          while(@row = $statement->fetchrow_array()) {
56                $data[$row[0]][1]+= $row[1];
```

```
        if(!($data[$row[0]][0])) {
58          $data[$row[0]][0]=0;
        }
60        }
}
62
for($indice=0;$indice<@data;$indice++) {
64    if($data[$indice][0] != 0 || $data[$indice][1] != 0) {
        $query = "insert into trafficByPeer
66          values(".$indice.",".$data[$indice][0].",".$data[$indice][1].")";
                $statementinsert = $database->prepare($query);
68              $statementinsert->execute()
              or  die "Could not execute query: ".$query. "\n Error: %%@
70 ".mysql_err($database)."\n";
    }
72 }
@data = ();
74 print "Calcul du traffic par Peer (derniere 48H)\n";
for($boucle=0;$boucle<47;$boucle++) {
76        $query = "    select    idpeersrc,
                      sum(bytes)
78              from  asH_".$boucle."
                where destas = 5432
80                    and srcas <> 5432
                group by idpeersrc";
82        $statement = $database->prepare($query);
          $statement->execute
84         or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
          while(@row = $statement->fetchrow_array()) {
86              $data[$row[0]][0]+= $row[1];
                $data[$row[0]][1] =0;
88        }
}
90 for($boucle=0;$boucle<47;$boucle++) {
          $query = "    select    idpeerdst,
92                      sum(bytes)
                from  asH_".$boucle."
94              where srcas = 5432
                      and destas <> 5432
96              group by idpeerdst";
          $statement = $database->prepare($query);
98        $statement->execute
           or die "Could not execute query: ".$query. "\n";
100       while(@row = $statement->fetchrow_array()) {
                $data[$row[0]][1]+= $row[1];
102             if(!($data[$row[0]][0])) {
                        $data[$row[0]][0]=0;
104             }
          }
106 }

108 for($indice=0;$indice<@data;$indice++) {
          if($data[$indice][0] != 0 || $data[$indice][1] != 0) {
110             $query = "insert into trafficByPeerD
                      values(".$indice.",".$data[$indice][0].",".$data[$indice][1].")";
112             $statementinsert = $database->prepare($query);
                $statementinsert->execute() or
114            die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
          }
116 }

118


120
print "Calcul par peer effectue\n";
122 print "Calcul du traffic par AS\n";
@data = ();
```

```
for($boucle=0;$boucle<6;$boucle++) {
        $query = "    select    srcas,
                      sum(bytes)
                from  asD_".$boucle."
                where destas = 5432
                      and srcas <> 5432
                group by srcas";
        $statement = $database->prepare($query);
        $statement->execute or
         die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
        while(@row = $statement->fetchrow_array()) {
                $data[$row[0]][0]+= $row[1];
      $data[$row[0]][1] = 0;
        }
}
for($boucle=0;$boucle<6;$boucle++) {
        $query = "    select    destas,
                      sum(bytes)
                from  asD_".$boucle."
                where srcas = 5432
                      and destas <> 5432
                group by destas";
        $statement = $database->prepare($query);
        $statement->execute
         or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
        while(@row = $statement->fetchrow_array()) {
                $data[$row[0]][1]+= $row[1];
         if(!($data[$row[0]][0])) {
                        $data[$row[0]][0]=0;
                }

    }
}


for($indice=0;$indice<@data;$indice++) {
        if($data[$indice][0] != 0 || $data[$indice][1] != 0) {
                $query = "insert into trafficByAs
                values(".$indice.",".$data[$indice][0].",".$data[$indice][1].")";
                $statementinsert = $database->prepare($query);
                $statementinsert->execute()
                or  die "Could not execute query: ".$query. "\n Error: ".$database->err."\n";
        }
        $indice++;

}

@data = ();
for($boucle=0;$boucle<47;$boucle++) {
        $query = "    select    srcas,
                      sum(bytes)
                from  asH_".$boucle."
                where destas = 5432
                      and srcas <> 5432
                group by srcas";
        $statement = $database->prepare($query);
        $statement->execute
         or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
        while(@row = $statement->fetchrow_array()) {
                $data[$row[0]][0]+= $row[1];
         $data[$row[0]][1] = 0;
    }
}
for($boucle=0;$boucle<47;$boucle++) {
        $query = "    select    destas,
                      sum(bytes)
```

```
                from  asH_".$boucle."
192             where srcas = 5432
                      and destas <> 5432
194             group by destas";
        $statement = $database->prepare($query);
196     $statement->execute
         or die "Could not execute query: ".$query. "\n Error: ".msql_err($database)."\n";
198     while(@row = $statement->fetchrow_array()) {
                $data[$row[0]][1]+= $row[1];
200      if(!($data[$row[0]][0])) {
                        $data[$row[0]][0]=0;
202             }

204   }

206 }

208

210 for($indice=0;$indice<@data;$indice++) {
        if($data[$indice][0] != 0 || $data[$indice][1] != 0) {
212             $query = "insert into trafficByAsD
                values(".$indice.",".$data[$indice][0].",".$data[$indice][1].")";
214             $statementinsert = $database->prepare($query);
                $statementinsert->execute()
216             or  die "Could not execute query: ".$query. "\n Error: ".msql_err($database)."\n";
        }
218     $indice++;

220 }

222
  print "Calcul du traffic par AS effectue\n";
224 print "Calcul du traffic par prefix\n";
  for($boucle=0;$boucle<6;$boucle++) {
226     $query = "  select  netsrc,
                    sum(bytes)
228             from  netD_".$boucle."
                where asdst = 5432
230                   and assrc <> 5432
                group by netsrc";
232     $statement = $database->prepare($query);
        $statement->execute
234      or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
   while(@row = $statement->fetchrow_array()) {
236    #$cle = "'".$row[0]."'";
       $data2{$row[0]} [0] += $row[1];
238    $data2{$row[0]} [1] = 0;
       }
240 }
  for($boucle=0;$boucle<6;$boucle++) {
242     $query = "  select  netsrc,
                    sum(bytes)
244             from  netD_".$boucle."
                where asdst <> 5432
246                   and asdst = 5432
                group by netsrc";
248     $statement = $database->prepare($query);
        $statement->execute
250      or die "Could not execute query: ".$query. "\n Error: ".mysql_err($database)."\n";
        while(@row = $statement->fetchrow_array()) {
252             #$cle = "'".$row[0]."'";
                $data2{$row[0]}[1]+= $row[1];
254      if(!($data{$row[0]}[0])) {
                        $data{$row[0]}[0]=0;
256             }
```

```
258     }
    }
260

262
    foreach $clef (keys %data2) {
264     @record = $data2{$clef};
        if($record[0] != 0 || $record[1] != 0) {
266                  $query = "insert into trafficByPref
                    values('".$clef."',".$record[0].",".$record[1].")";
268                  $statementinsert = $database->prepare($query);
                     $statementinsert->execute()
270                 or  die "Could not execute query: ".$query. "\n Error: %%@
    ".mysql_err($database)."\n";
272          }

274 }
    print "Calcul par prefix effectue\n";
```

Fichier : genPrefixSim.pl

```
    #!/usr/bin/perl
 2
    use DBI;
 4
    $database = DBI->connect("DBI:mysql:BgpCheck:localhost:3306","flowtools", "netflow");
 6  $query = "truncate table MinBgp";
    $statement = $database->prepare($query)
 8      or die "Erreur preparation Query: $query \n Error:".$database->errstr."\n";
    $statement->execute()
10      or die "Erreur execution Query : $query \n Error:".$statement->errstr."\n";

12  $query = "insert into MinBgp
        select prefix,mask,min(pathlong) as minpath,min(nbrAs) as minas
14      from BGPDATA as a,PeerSimulation as b
        where a.idpeer = b.idpeer
16      group by prefix,mask
        order by prefix,mask";
18  $statement = $database->prepare($query)
        or die "Erreur preparation Query: $query \n Error:".$database->errstr."\n";
20  $statement->execute()
        or die "Erreur execution Query : $query \n Error:".$statement->errstr."\n";
22
    $query= "truncate table BgpTable_Draft";
24  $statement = $database->prepare($query)
        or die "Erreur preparation Query: $query \n Error:".$database->errstr."\n";
26  $statement->execute()
        or die "Erreur execution Query : $query \n Error:".$statement->errstr."\n";
28
    $query = " insert into BgpTable_Draft
30          select a.idpeer,a.prefix,a.mask,b.minpathlong,b.minnbras
            from MinBgp as b, BGPDATA as a, PeerSimulation as c
32          where a.prefix = b.prefix
            and a.mask = b.mask
34          and a.pathlong = b.minpathlong
            and c.idpeer = a.idpeer";
36  $statement = $database->prepare($query)
        or die "Erreur preparation Query: $query \n Error:".$database->errstr."\n";
38  $statement->execute()
        or die "Erreur execution Query : $query \n Error:".$statement->errstr."\n";
40
    $statement->finish;
42  $database->disconnect();
    exit(1);
```

Fichier : groupementMask.pl

```
#!/usr/bin/perl

use DBI;
my $database = DBI->connect("DBI:mysql:BgpCheck:localhost:3306","flowtools", "netflow");
$date = `date`;
print "Debut: $date <br>\n";

##############################
#
#Chargement des masques dans un tableau
#
##############################
for($bouclemasque=0;$bouclemasque <= 8;$bouclemasque++) {
    $valeur = 256 - 2**$bouclemasque;
    $masque[$bouclemasque]= pack("I4",255,255,$valeur,0);
    print "Creation du masque: 255.255.$valeur.0 <br>\n";
    ($test1,$test2,$test3,$test4) = unpack("I4",$masque[$bouclemasque]);
    print "Masque cree: $test1.$test2.$test3.$test4 <br>\n";
}
for($bouclemasque=1;$bouclemasque <= 8;$bouclemasque++) {
        $valeur = 256- 2**$bouclemasque;
        $masque[8+$bouclemasque]= pack("I4",255,$valeur,0,0);
        print "Creation du masque: 255.$valeur.0.0 <br> \n";
    ($test1,$test2,$test3,$test4) = unpack("I4",$masque[8+$bouclemasque]);
        print "Masque cree: $test1.$test2.$test3.$test4 <br>\n";

 }
##############################
#
#Chargement des bytes par IP de la base
#
##############################
$query = "select Ip,Bytes  from TrafficIp where Bytes <> 0 and Type= 'I' order by Ip";

$statement = $database->prepare($query)
    or die "Erreur preparation Query: $query \n Error:".$database->errstr."\n";
$statement->execute() or die "Erreur execution Query : $query \n Error:".$statement->errstr."\n";
$boucleip = 0;
$maxipa = 0;
$maxipb = 0;
$maxipc = 0;

while(@row = $statement->fetchrow_array()) {
    ($ipa,$ipb,$ipc,$ipd) = split(/\./,$row[0]);
    if($ipa > $maxipa) {
        $maxipa = $ipa;
    }
    if($ipb > $maxipb) {
        $maxipb = $ipb;
    }
    if($ipc > $maxipc) {
        $maxipc = $ipc;
    }
    $ip[$ipa][$ipb][$ipc][0] = $row[0];
    $ip[$ipa][$ipb][$ipc][1] = $row[1];
    #print "IP: $row[0] \n";
    #print "Binaire : ".ip_vers_bin($row[0])."\n\n\n";
    $boucleip++;
}
print "Nombre d'IP chargees: $boucleip <br> \n";
$nbrip = $boucleip;
$statement->finish;


##############################
#
#Chargement des prefixes de la base
```

```
68 #
   ################################
70 $query2 = "select distinct idpeer from BgpTable_Draft where mask <= 24 order by idpeer";

72 $statement = $database->prepare($query2)
      or die "Erreur preparation Query: $query2 \n Error:".$database->errstr."\n";
74 $statement->execute()
      or die "Erreur execution Query : $query2 \n Error:".$statement->errstr."\n";
76
   while(@row = $statement->fetchrow_array()) {
78    print "idpeer pris en compte: $row[0] <br> \n";
   }
80

82 $query2 = " select    idpeer,
                  prefix,
84                mask,
                  pathlong,
86                nbras
            from  BgpTable_Draft
88          where mask <= 24
            order by prefix,
90                   mask";

92 $statement = $database->prepare($query2)
      or die "Erreur preparation Query: $query2 \n Error:".$database->errstr."\n";
94 $statement->execute()
      or die "Erreur execution Query : $query2 \n Error:".$statement->errstr."\n";
96 $old = "";
   $maxprefa = 0;
98 $maxprefb = 0;
   $maxprefc = 0;
100 $nbrprefix=0;
   $bouclemasque = 0;
102
   while(@row = $statement->fetchrow_array()) {
104   $test = $row[1]."/".$row[2];
      if($test eq $old) {
106      $bouclenbrpeer++;
         ($prefa,$prefb,$prefc,$prefd) = split(/\./,$row[1]);
108      $prefix[$prefa][$prefb][$prefc][$row[2]][$bouclenbrpeer][0]=$row[0];
         $prefix[$prefa][$prefb][$prefc][$row[2]][$bouclenbrpeer][1]= $row[1];
110      $prefix[$prefa][$prefb][$prefc][$row[2]][$bouclenbrpeer][2]= $row[2];
         $prefix[$prefa][$prefb][$prefc][$row[2]][$bouclenbrpeer][3]= 0;
112      $prefix[$prefa][$prefb][$prefc][$row[2]][$bouclenbrpeer][4]= $row[3];
           $prefix[$prefa][$prefb][$prefc][$row[2]][$bouclenbrpeer][5]= $row[4];
114      $prefix[$prefa][$prefb][$prefc][$row[2]][0][0]=$bouclenbrpeer;
         $nbrprefix++;
116   }
      else  {
118      $bouclemasque++;
         ($prefa,$prefb,$prefc,$prefd) = split(/\./,$row[1]);
120         if($prefa > $maxprefa) {
            $maxprefa = $prefa;
122      }
         if($prefb > $maxprefb) {
124         $maxprefb = $prefb;
         }
126      if($prefc > $maxprefc) {
            $maxprefc = $prefc;
128      }
         $prefix[$prefa][$prefb][$prefc][$row[2]][1][0]=$row[0];
130        $prefix[$prefa][$prefb][$prefc][$row[2]][1][1]= $row[1];
           $prefix[$prefa][$prefb][$prefc][$row[2]][1][2]= $row[2];
132        $prefix[$prefa][$prefb][$prefc][$row[2]][1][3]= 0;
         $prefix[$prefa][$prefb][$prefc][$row[2]][1][4]= $row[3];
134      $prefix[$prefa][$prefb][$prefc][$row[2]][1][5]= $row[4];
```

```
        $prefix[$prefa][$prefb][$prefc][$row[2]][0][1]= 1;
136     $prefix[$prefa][$prefb][$prefc][$row[2]][0][2]= 0;
        $prefix[$prefa][$prefb][$prefc][$row[2]][0][0]=1;
138     $old = $row[1]."/".$row[2];
        $bouclenbrpeer = 1;
140     $nbrprefix++;
    }
142 }
  print "Nombre de Prefix distincts Charge $bouclemasque <br>\n";
144 print "Nombre de Prefix Charge $nbrprefix <br>\n";
  $nbrdiffmasq = $bouclemasque;
146

148 ##############################
  #
150 # Comparaison d'une IP a  un masque et attribution au masque des Bytes de l'IP
  #
152 #
  ##############################
154 print "Debut de la comparaison IP Masque.  Ce traitement peut etre long, soyez patient.<br>\n";
  print "Un message apparaitra tous les 1% de traitement effectue<br>\n";
156
  open (OUT,">/tmp/loadresultprefix.txt");
158 $boucleip = 0;
  $bouclepourc = 0;
160 $errorIp = 0;
  $oldprefb = 0;
162 $oldprefc = 0;
  $boucleindex = 0;
164 for($ipa = 0;$ipa<= $maxipa;$ipa++) {
    for($ipb = 0;$ipb<= $maxipb;$ipb++) {
166     for($ipc = 0;$ipc <= $maxipc;$ipc++) {
        if($ip[$ipa][$ipb][$ipc]) {
168       #print $ip[$ipa][$ipb][$ipc][0]."\n";
          $trouve = 0;
170       $compteur = 0;
          while($trouve==0 && $compteur <= 16) {
172
            $comparateurIp = ip_vers_bin($ip[$ipa][$ipb][$ipc][0])&$masque[$compteur];
174
            ($prefa,$prefb,$prefc,$prefd) = bin_vers_ip($comparateurIp);
176         ($ipa,$ipb,$ipc,$ipd) = bin_vers_ip(ip_vers_bin($ip[$ipa][$ipb][$ipc][0]));
            ($ip2a,$ip2b,$ip2c,$ip2d) = %%@
178 bin_vers_ip(ip_vers_bin($ip[$ipa][$ipb][$ipc][0])&$masque[$compteur]);
            if($prefix[$prefa][$prefb][$prefc][24-$compteur][0][1] == 1) {
180           for($bouclenbrpeer = 1;$bouclenbrpeer <= %%@
  $prefix[$prefa][$prefb][$prefc][24-$compteur][0][0];$bouclenbrpeer++) {
182             $prefix[$prefa][$prefb][$prefc][24-$compteur][$bouclenbrpeer][3] += %%@
  $ip[$ipa][$ipb][$ipc][1];
184           }
              if($prefix[$prefa][$prefb][$prefc][24-$compteur][0][2]==0) {
186             $index[$boucleindex][0] = $prefa;
                  $index[$boucleindex][1] = $prefb;
188               $index[$boucleindex][2] = $prefc;
                  $index[$boucleindex][3] = 24-$compteur;
190             $prefix[$prefa][$prefb][$prefc][24-$compteur][0][2]=1;
                $boucleindex++;
192           }
              $trouve = 1;
194         }
            $compteur++;
196       }

198       if($trouve == 0 && $compteur >= 16) {
            $errorIp ++;
200       }
```

```
202             if(((($boucleip /$nbrip)*100) >= $bouclepourc) {
                    print "$bouclepourc effectue <br>\n";
204                 $bouclepourc++;
                }
206             $boucleip++;
            }
208         }
    }
210 }
    $boucle = 0;
212 while($boucle <= $boucleindex) {
        $prefa = $index[$boucle][0];
214     $prefb = $index[$boucle][1];
        $prefc = $index[$boucle][2];
216     $mask = $index[$boucle][3];
        $nombrepeer = $prefix[$prefa][$prefb][$prefc][$mask][0][0];
218     for($bouclenbrpeer = 1;$bouclenbrpeer<= $nombrepeer;$bouclenbrpeer++) {
            print OUT $prefix[$prefa][$prefb][$prefc][$mask][$bouclenbrpeer][0]."','".
220             $prefix[$prefa][$prefb][$prefc][$mask][$bouclenbrpeer][1]."',".
                $prefix[$prefa][$prefb][$prefc][$mask][$bouclenbrpeer][2]."',".
222             $prefix[$prefa][$prefb][$prefc][$mask][$bouclenbrpeer][3]."',".
                $prefix[$prefa][$prefb][$prefc][$mask][$bouclenbrpeer][4]."',".
224             $prefix[$prefa][$prefb][$prefc][$mask][$bouclenbrpeer][5]."\n";
        }
226     $boucle++;

228 }

230 close OUT;
    ##################################
232 #
    # Update de la base avec les bytes pour les masques
234 #
    ##################################
236 print "Debut update de la table des masques <br>\n";
    print "Maxprefa: $maxprefa MaxPrefB: $maxprefb MaxprefC: $maxprefc<br>\n";
238 $bouclemasque = 0;
    $query ="truncate table BgpTable_Results";
240 $statement = $database->prepare($query)
            or sortie("Erreur preparation Query: $query \n Error:".$database->errstr." <br>\n");
242 $statement->execute()
            or sortie("Erreur preparation Query: $query \n Error:".$statement->errstr." <br>\n");
244
    $query = "  load data infile '/tmp/loadresultprefix.txt'
246             into table BgpTable_Results
                fields terminated by ','
248             optionally enclosed by '\\''";
    $statement = $database->prepare($query)
250     or sortie("Erreur preparation Query: $query \n Error:".$database->errstr." <br>\n");
    $statement->execute()
252     or sortie("Erreur preparation Query: $query \n Error:".$statement->errstr."<br>\n");
    unlink("/tmp/loadresultprefix.txt");
254 print "Fin de l'update de la table des masques<br>\n";
    $d = `date`;
256 print "Fin: $d <br>\n";
    print "Nombre d'Ip non matchee: $errorIp <br>\n";
258 exit(1);

260 ##################################
    #
262 # Fonction de sortie, permet d'afficher un message avant de quitter
    #
264 ##################################

266 sub sortie {
        if($_[0]) {
268         print $_[0];
```

```
    }
270     exit(-1);

272 }

274
    ##############################
276 #
    # Fonction de conversion binaire->decimal et decimal -> binaire
278 #
    ##############################
280 sub dec_vers_bin {
        return pack("I",shift);
282 }

284 sub bin_vers_dec {
        return unpack("I",shift);
286  }

288 ##############################
    #
290 # Fonction de conversion ip -> binaire
    #
292 # Recoit une IP et un masque, retourne la valeur binaire de l'IP de la taille du masque.
    #
294 ##############################

296 sub ip_vers_bin {

298     $ip = $_[0];
        ($a,$b,$c,$d) = split(/\./,$ip);
300     return pack("I4",$a,$b,$c,$d);
    }
302
    ##############################
304 #
    # Fonction de conversion binaire -> IP
306 #
    # Recoit une valeur binaire sur 32 bits et retourne une liste contenant
308 # chaque valeur partie decimale de l'IP
    #
310 ##############################

312 sub bin_vers_ip {

314     ($a,$b,$c,$d) = unpack("IIII",$_[0]);
        return $a,$b,$c,$d;
316 }
```

Chapitre 5

Code source de la collecte des données

Fichier : collect.pl

```
#! /usr/bin/perl
use DBI;
use Net::SFTP;
use Net::FTP;

########################################
#
# Script de récupération automatique
# des fichier cflowd sur les collecteurs
#
# Utilise le fichier collect.cfg qui doit contenir
# l'IP de la machine
# le user, la pass pour le login,
# le répertoire source et destination du fichier
########################################

#Test de la présence des lock
#Stop du script si un lock est en place
#Mise en place du lock si le script peut démarrer

if ((-e "/home/cponsen/mysql/global.lock") || (-e "/home/cponsen/mysql/insertAs.lock") || (-e %%@
"/home/cponsen/mysql/insertPort.lock")) {
    print"Script already running";
    exit(2);
}
open(OUT,"> /home/cponsen/mysql/global.lock");
print OUT "en cours";
close(OUT);

#Chargement de la config

open(IN,"/home/cponsen/mysql/collect.cfg");
while($line=<IN>){
    ($var1,$var2) = split(/ *\t*= *\t*/,$line);
    if(uc($var1) eq "USER") { $user = $var2; chomp($user) };
    if(uc($var1) eq "PASS") { $pass = $var2; chomp($pass) };
    if(uc($var1) eq "HOSTNAME") { $hostname = $var2;chomp($hostname) };
    if(uc($var1) eq "SRCDIR") { $srcdir = $var2;chomp($srcdir) };
    if(uc($var1) eq "DSTDIR") { $dstdir = $var2;chomp($dstdir) };
}
#Fin du chargement de la config

#Test de la config
#Exit si pas bon
if($user eq "" or $pass eq "" or $hostname eq "" or $srcdir eq "" or $dstdir eq "") { die "Nombre de %
```

```
  parametre de configuration incorrect, veuillez vérifier votre fichier de configuration collect.cfg";
48 }
  #Fin du test de la config
50
  #Debut connection FTP
52 %logindata = ( user => $user,
        password => $pass,
54      compression => 1,
        protocol => 2);
56
  $connection = Net::SFTP->new($hostname,%logindata) or die "Connection to $hostname failed";
58

60 #Récupération de la liste des fichiers à récupérer sur le serveur
  @listoffile=$connection->ls($srcdir);
62 $boucle = 0;
  $stop = 0;
64
  #Création de la liste des fichiers à récupérer en fonction de la date du fichier source
66 while(@listoffile[$boucle] &&  $stop == 0) {
     if (@listoffile[$boucle]->{'filename'} =~ /^mysql.*/) {
68      $oldTime = @listoffile[$boucle]->{'a'}->mtime;
        $oldName= @listoffile[$boucle]->{'filename'} ;
70      $stop = 1;
     }
72   $boucle++;
  }
74
  while($list = @listoffile[$boucle]) {
76 #foreach $list (@listoffile) {
     if ( $list->{'filename'} =~  /^mysql.*/  ) {
78      if ($oldTime<=$list->{'a'}->mtime || $oldTime==0) {
           @tableau = (@tableau, $oldName);
80                      $oldTime = $list->{'a'}->mtime;
                        $oldName = $list->{'filename'};
82
        }
84      elsif ($oldTime>$list->{'a'}->mtime){
           @tableau=(@tableau, $list->{'filename'});
86      }
     }
88   $boucle++;
  }
90
  print "Liste des fichiers a transferer\n";
92
  #Récupération de la liste
94 if( scalar(@tableau)==0) {
     print "Pas de fichier a transferer.\n";
96 }
  else {
98   foreach $data(@tableau) {
        print $data."\n";
100  }
     print "\n";
102  foreach $data (@tableau) {
        $connection2= Net::FTP->new($hostname);
104        $connection2->login($user,$pass) or die "Login Failed";
        ($dummy,$numero) = split /-/,$data;
106     print "Recuperation du fichier : ".$data."\n";
        $srcfile = $srcdir.$data;
108     $dstfile = $dstdir.$data;
        print "srcfile: $srcfile dstfile: $dstfile\n";
110     $connection2->get($srcfile,$dstfile) or die "Recuperation a echoue\n";
        print "Recuperation effectuee avec succes\n";
112     $connection2->delete($srcfile) or print "Error File delete:".$srcdir.$data."\n";
        $connection2->quit;
```

```
114     }
    }
116 print "Recuperation de tous les fichiers effectuee avec succes. Have a good Work\n";

118 #Déverrouillage du script
    unlink("/home/cponsen/mysql/global.lock");
```

Fichier : filtreSkynet.pl

```
    #!/usr/bin/perl
 2
    use DBI;
 4 my $database = DBI->connect("DBI:mysql:BgpCheck:localhost:3306","flowtools", "netflow");
    $date = `date`;
 6 print "Debut: $date <br>\n";

 8 ################################
    #
10 #Chargement des masques dans un tableau
    #
12 ################################
    for($bouclemasque=0;$bouclemasque <= 8;$bouclemasque++) {
14     $valeur = 256 - 2**$bouclemasque;
       $masque[$bouclemasque]= pack("I4",255,255,$valeur,0);
16     print "Creation du masque: 255.255.$valeur.0 <br>\n";
       ($test1,$test2,$test3,$test4) = unpack("I4",$masque[$bouclemasque]);
18     print "Masque cree: $test1.$test2.$test3.$test4 <br>\n";
    }
20 for($bouclemasque=1;$bouclemasque <= 8;$bouclemasque++) {
           $valeur = 256- 2**$bouclemasque;
22         $masque[8+$bouclemasque]= pack("I4",255,$valeur,0,0);
           print "Creation du masque: 255.$valeur.0.0 <br> \n";
24     ($test1,$test2,$test3,$test4) = unpack("I4",$masque[8+$bouclemasque]);
           print "Masque cree: $test1.$test2.$test3.$test4 <br>\n";
26
     }
28 ################################
    #
30 #Chargement des bytes par IP de la base
    #
32 ################################
    $query = "select Ip,Bytes  from TrafficIp where Bytes <> 0 and Type= 'I' order by Ip";
34
    $statement = $database->prepare($query)
36     or die "Erreur preparation Query: $query \n Error:".$database->errstr."\n";
    $statement->execute()
38     or die "Erreur execution Query : $query \n Error:".$statement->errstr."\n";
    $boucleip = 0;
40 $maxipa = 0;
    $maxipb = 0;
42 $maxipc = 0;

44 while(@row = $statement->fetchrow_array()) {
       ($ipa,$ipb,$ipc,$ipd) = split(/\./,$row[0]);
46     if($ipa > $maxipa) {
           $maxipa = $ipa;
48     }
       if($ipb > $maxipb) {
50         $maxipb = $ipb;
       }
52     if($ipc > $maxipc) {
           $maxipc = $ipc;
54     }
       $ip[$ipa][$ipb][$ipc][0] = $row[0];
56     $ip[$ipa][$ipb][$ipc][1] = $row[1];
       #print "IP: $row[0] \n";
58     #print "Binaire : ".ip_vers_bin($row[0])."\n\n\n";
```

```
    $boucleip++;
}
print "Nombre d'IP chargees: $boucleip <br> \n";
$nbrip = $boucleip;
$statement->finish;

################################
#
#Chargement des prefixes Skynet de la base
#
################################
$query2 = "select prefix,mask from SkynetPrefix order by mask DESC";

$statement = $database->prepare($query2)
    or die "Erreur preparation Query: $query2 \n Error:".$database->errstr."\n";
$statement->execute()
    or die "Erreur execution Query : $query2 \n Error:".$statement->errstr."\n";
$old = "";
$maxprefa = 0;
$maxprefb = 0;
$maxprefc = 0;
$nbrprefix=0;
$bouclemasque = 0;

while(@row = $statement->fetchrow_array()) {
    $prefix[$nbrprefix][0]=$row[0];
        $prefix[$nbrprefix][1]= $row[1];
    $nbrprefix++;
}
print "Nombre de Prefix Charge $nbrprefix <br>\n";

################################
#
# Comparaison d'une IP a  un masque
# et suppression dans la base des IP invalides
#
################################
print "Debut de la comparaison IP Masque.  Ce traitement peut etre long, soyez patient.<br>\n";
print "Un message apparaitra tous les 1% de traitement effectue<br>\n";

$boucleip = 0;
$bouclepourc = 0;
$nbrIpmatch = 0;
$oldboucle = 0;
for($ipa = 0;$ipa<= $maxipa;$ipa++) {
    for($ipb = 0;$ipb<= $maxipb;$ipb++) {
        for($ipc = 0;$ipc <= $maxipc;$ipc++) {
            if($ip[$ipa][$ipb][$ipc]) {
                $trouve = 0;
                $compteur = 0;
                $boucle = $oldboucle;
                while($trouve == 0 && $boucle < @prefix) {
                    $comparateurIp = %%@
ip_vers_bin($ip[$ipa][$ipb][$ipc][0])&$masque[24-$prefix[$boucle][1]];
                    ($a,$b,$c,$d) =  bin_vers_ip($comparateurIp);
                        $resultip = $a.".".$b.".".$c.".".$d;
                    if($resultip eq $prefix[$boucle][0]) {
                        ($a,$b,$c,$d) =  bin_vers_ip($comparateurIp);
                        $query = 'delete from TrafficIp where Ip = "'.$ip[$ipa][$ipb][$ipc][0].'"';
                        $statement = $database->prepare($query)
                            or die "Erreur preparation Query: $query \n %%@
Error:".$database->errstr."\n";
                        $statement->execute()
                            or die "Erreur execution Query : $query \n %%@
Error:".$statement->errstr."\n";
```

```
126
                    $nbrIpmatch++;
128                 $trouve = 1;
                    $oldboucle = $boucle;
130             }
                $boucle++;
132         }
            if(((($boucleip /$nbrip)*100) >= $bouclepourc) {
134             print "$bouclepourc effectue <br>\n";
                $bouclepourc++;
136         }
            $boucleip++;
138     }
    }
140 }
142
print "Nombre d'IP matchee supprimee: $nbrIpmatch \n";
144
##################################
146 #
# Fonction de sortie, permet d'afficher un message avant de quitter
148 #
##################################
150
sub sortie {
152     if($_[0]) {
            print $_[0];
154     }
        exit(-1);
156
}
158

160 ##############################
    #
162 # Fonction de conversion binaire->decimal et decimal -> binaire
    #
164 ##############################
sub dec_vers_bin {
166     return pack("I",shift);
}
168
sub bin_vers_dec {
170     return unpack("I",shift);
 }
172
##############################
174 #
# Fonction de conversion ip -> binaire
176 #
# Recoit une IP et un masque, retourne la valeur binaire de l'IP de la taille du masque.
178 #
##############################
180
sub ip_vers_bin {
182
    my $ip = $_[0];
184     (my $a,my $b,my $c,my $d) = split(/\./,$ip);
        return pack("I4",$a,$b,$c,$d);
186 }

188 ############################
    #
190 # Fonction de conversion binaire -> IP
    #
192 # Recoit une valeur binaire sur 32 bits et retourne
```

```
# une liste contenant chaque valeur partie decimale de l'IP
#
##########################

sub bin_vers_ip {

    (my $a,my $b,my $c,my $d) = unpack("IIII",$_[0]);
    return $a,$b,$c,$d;
}
```

Fichier : insertPortH.pl

```
#!/usr/bin/perl
unshift (@INC,"/home/cponsen/mysql");
use router;

if((-e "/home/cponsen/mysql/insertPort.lock")||(-e "/home/cponsen/mysql/global.lock")) {
    print "script already running\n";
    exit(2);
}

open(OUT, "> /home/cponsen/mysql/insertPort.lock");
print OUT "encours";
close(OUT);
use DBI;
my $database = DBI->connect("DBI:mysql:flowtools:localhost:3306","flowtools", "netflow");
$timeportmaxi = 0;
for($boucle=0;$boucle<48;$boucle++) {
    $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from %%@
portHsrc_in_'.$boucle.'')
      or die "peut pas faire le select : ".$boucle."\n";
    $statement->execute() or die "peut pas execute le select\n";
    @timedebut = $statement->fetchrow_array();
    $statement->finish;
    if($timedebut[0] && ($timeportmaxi < $timedebut[0] || $boucle == 0)) {
       $timeportmaxi = $timedebut[0];
    }
    $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from %%@
portHsrc_out_'.$boucle.'')
        or die "peut pas faire le select\n";
       $statement->execute() or die "peut pas execute le select\n";
       @timedebut2 = $statement->fetchrow_array();
       $statement->finish;
       if($timedebut2[0] && $timeportmaxi < $timedebut2[0]) {
              $timeportmaxi = $timedebut2[0];
       }

    $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from %%@
portHdst_in_'.$boucle.'')
        or die "peut pas faire le select\n";
       $statement->execute() or die "peut pas execute le select\n";
       @timedebut3 = $statement->fetchrow_array();
       $statement->finish;
       if($timedebut3[0] && $timeportmaxi < $timedebut3[0]) {
              $timeportmaxi = $timedebut3[0];
       }

       $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from %%@
portHdst_out_'.$boucle.'')
        or die "peut pas faire le select\n";
       $statement->execute() or die "peut pas execute le select\n";
       @timedebut4 = $statement->fetchrow_array();
       $statement->finish;
       if($timedebut4[0] && $timeportmaxi < $timedebut4[0]) {
              $timeportmaxi = $timedebut4[0];
       }
```

```
        $timefininterval = $time+299;
124     print"    Table $table Heure courante: $heure : $minutes : $secondes.
              Heure debut interval: $time.\n
126           Heure fin interval: $timefininterval.
              Heure fin traitement prevu: $timefin\n";
128     $query = " select count(*)
                              from Data_".$table."
130                           where starttime >= $time
                              and starttime < $timefininterval
132                           and srcas <>0
                              and destas <> 0
134                           and ".$wherein."";
        $statement = $database->prepare($query);
136     $statement->execute();
        @nombrerecord = $statement->fetchrow_array();
138     $statement->finish;
        print "nombrerecords:".$nombrerecord[0]."\n";
140     if($nombrerecord[0] == 0) {
                        #print "ici:".$statement->rows."\n";
142                     $time=$time+300;
                        next;
144             }

146     $query1 ="select sum(bytes) as total,
              srcport
148           from Data_$table
              where starttime >= $time
150           and starttime < $timefininterval
              and srcas <>0
152           and destas <> 0
              and srcport <> dstport
154           and ".$wherein."
              group by srcport
156           order by total DESC";
        $query2 ="select sum(bytes) as total,
158                     dstport
                  from Data_$table
160               where starttime >= $time
                  and starttime < $timefininterval
162               and srcas <>0
                  and destas <> 0
164               and dstport <> srcport
                  and ".$wherein."
166           group by dstport
              order by total DESC ";
168
        $query3 ="select sum(bytes) as total,
170               srcport
                  from Data_$table
172               where starttime >= $time
                  and starttime < $timefininterval
174               and srcas <>0
                  and destas <> 0
176           and dstport = srcport
              and ".$wherein."
178               group by srcport
              order by total DESC ";
180
        $query4 ="select sum(bytes) as total,
182           srcport
              from Data_$table
184           where starttime >= $time
              and starttime < $timefininterval
186           and srcas <>0
              and destas <> 0
188           and srcport <> dstport
              and ".$whereout."
```

```
56      $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from %%@
    portHsrcdst_in_'.$boucle.'')
58          or die "peut pas faire le select\n";
            $statement->execute() or die "peut pas execute le select\n";
60          @timedebut = $statement->fetchrow_array();
            $statement->finish;
62          if($timedebut5[0] && $timeportmaxi < $timedebut5[0] ) {
                    $timeportmaxi = $timedebut5[0];
64          }

66          $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from %%@
    portHsrcdst_out_'.$boucle.'')
68           or die "peut pas faire le select\n";
            $statement->execute() or die "peut pas execute le select\n";
70          @timedebut = $statement->fetchrow_array();
            $statement->finish;
72          if($timedebut6[0] && $timeportmaxi < $timedebut6[0]) {
                    $timeportmaxi = $timedebut6[0];
74      }
    }
76

78  $wherein = "(".getWhereRouterIn().")";
    $whereout ="(". getWhereRouterOut().")";
80  if($timeportmaxi==0)
    {
82      $i;
        $minimum=0;
84      for($i=0;$i<24;$i++) {
            $statement = $database->prepare('select truncate(min(starttime)/300,0)*300 from Data_'.$i.' ')
86              or die "peut pas faire le select";
            $statement->execute() or die "peut pas execute le select\n";
88          @timedebut = $statement->fetchrow_array();
            $statement->finish;
90          print"before test minimum: $minimum time: ".$timedebut[0]."\n";
            if($minimum==0){
92              $minimum=$timedebut[0]+0;

94          }
            else
96          {
                if($timedebut[0]) {
98                  if($timedebut[0]<$minimum) {
                        $minimum = $timedebut[0];
100                 }
                }
102         }
            print"after test minimum: $minimum time: ".$timedebut[0]."\n";
104
        }
106     if($minimum == 0) { print"peut pas, tables vides\n";exit();}
        $timeportmaxi = $minimum;
108 }

110 print "TimeportMaxi= ".$timeportmaxi."\n";
    #$table=((@time[0]/86400)%7);
112 $statement = $database->prepare('select UNIX_TIMESTAMP(NOW())')or die "Peut pas preparer la demande de
    now";
114 $statement->execute();
    @timefin = $statement->fetchrow_array();
116 $statement->finish;
    $time = $timeportmaxi;
118 $timefin=$timefin[0]-300;
    for($table=0;$table<24;$table++) {
120     print "Traitement de la table Data_$table\n";
        while($time <= $timefin) {
122         ($secondes,$minutes,$heure) = (localtime)[0,1,2];
```

```
                                die "Peux pas preparer le insert:".$database->errstr." statement: %%@
".$insert;
                    $statementinsert2->execute()
                    or die "Peux pas executer l'insert:".$database->errstr;
                    $statementinsert2->finish;
            }
            $statement2->finish;

        $statement3 = $database->prepare($query3)
            or die "peux pas preparer la requete de select".$database->errstr."\n";
        $statement3->execute()
            or die "peut pas executer le select: ".$database->errstr;

        while(@data3 = $statement3->fetchrow_array()) {
                    $insert = "insert into portHsrcdst_in_".$realtable."  values (
                                                        ".$data3[1].",
                                                        ".$data3[0].",
                                                        '".$heure[0]."')";
                    $statementinsert3 = $database->prepare($insert) or
                                die "Peux pas preparer le insert:".$database->errstr." statement: %%@
".$insert;
                    $statementinsert3->execute() or die "Peux pas executer %%@
l'insert:".$database->errstr;
                    $statementinsert3->finish;
            }
            $statement3->finish;

        $statement4 = $database->prepare($query4)
            or die "peux pas preparer la requete de select".$database->errstr."\n";
        $statement4->execute() or die "peut pas executer le select: ".$database->errstr;

        while(@data4 = $statement4->fetchrow_array()) {
                    $insert = "insert into portHsrc_out_".$realtable."  values (
                    ".$data4[1].",
                    ".$data4[0].",
                    '".$heure[0]."')";

                    $statementinsert4 = $database->prepare($insert) or
                                die "Peux pas preparer le insert:".$database->errstr." statement: %%@
".$insert;
                    $statementinsert4->execute()
                    or die "Peux pas executer l'insert:".$database->errstr;
                    $statementinsert4->finish;
            }
            $statement4->finish;

        $statement5 = $database->prepare($query5)
            or die "peux pas preparer la requete de select".$database->errstr."\n";
        $statement5->execute()
            or die "peut pas executer le select: ".$database->errstr;

        while(@data5 = $statement5->fetchrow_array()) {
                    $insert = "insert into portHdst_out_".$realtable."  values (
                                                        ".$data5[1].",
                                                        ".$data5[0].",
                                                        '".$heure[0]."')";

                    $statementinsert5 = $database->prepare($insert) or
                                die "Peux pas preparer le insert:".$database->errstr." statement: %%@
".$insert;
                    $statementinsert5->execute() or die "Peux pas executer %%@
l'insert:".$database->errstr;
                    $statementinsert5->finish;
            }
            $statement5->finish;

        $statement6 = $database->prepare($query6)
```

```
190             group by srcport
                order by total DESC ";
192
        $query5 ="select sum(bytes) as total,
194                     dstport
                        from Data_$table
196                     where starttime >= $time
                        and starttime < $timefininterval
198                     and srcas <>0
                        and destas <> 0
200                     and dstport <> srcport
                        and ".$whereout."
202             group by dstport
                order by total DESC ";
204
        $query6 ="select sum(bytes) as total,
206                     srcport
                        from Data_$table
208                     where starttime >= $time
                        and starttime < $timefininterval
210                     and srcas <>0
                        and destas <> 0
212             and dstport = srcport
                and ".$whereout."
214                     group by srcport
                order by total DESC ";
216
        #print $query1."\n".$query2."\n".$query3."\n";
218     $statementheure=$database->prepare("select FROM_UNIXTIME(".$time.")");
           $statementheure->execute;
220        @heure = $statementheure->fetchrow_array();
           $statementheure->finish;
222

224     $statement = $database->prepare($query1) or die "peux pas preparer la requete de %%@
    select".$database->errstr."\n";
226     $statement->execute() or die "peut pas executer le select: ".$database->errstr;

228     $realtable = ($time/3600)%48;
        while(@data1 = $statement->fetchrow_array()) {
230                 $insert = "insert into portHsrc_in_".$realtable." values (
                    ".$data1[1].",
232                 ".$data1[0].",
                    '".$heure[0]."')";
234
                    $statementinsert1 = $database->prepare($insert) or
236                             die "Peux pas preparer le insert:".$database->errstr." statement: %%@
    ".$insert;
238                 $statementinsert1->execute()
                    or die "Peux pas executer l'insert:".$database->errstr."\n %%@
240 insert:".$insert."\n";
                    $statementinsert1->finish;
242         }
        $statement->finish;
244
        $statement2 = $database->prepare($query2)
246        or die "peux pas preparer la requete de select".$database->errstr."\n";
        $statement2->execute()
248        or die "peut pas executer le select: ".$database->errstr;

250     while(@data2 = $statement2->fetchrow_array()) {
                    $insert = "insert into portHdst_in_".$realtable."  values (
252                                                     ".$data2[1].",
                                                        ".$data2[0].",
254                                                     '".$heure[0]."')";

256                 $statementinsert2 = $database->prepare($insert) or
```

```
324          or die "peux pas preparer la requete de select".$database->errstr."\n";
        $statement6->execute() or die "peut pas executer le select: ".$database->errstr;
326
        while(@data6 = $statement6->fetchrow_array()) {
328                 $insert = "insert into portHsrcdst_out_".$realtable."  values (
                                                        ".$data6[1].",
330                                                     ".$data6[0].",
                                                        '".$heure[0]."')";
332                 $statementinsert6 = $database->prepare($insert) or
                                die "Peux pas preparer le insert:".$database->errstr." statement: %%@
334 ".$insert;
                    $statementinsert6->execute()
336                 or die "Peux pas executer l'insert:".$database->errstr;
                    $statementinsert6->finish;
338         }
            $statement6->finish;
340
        $time=$time+300;
342     }

344         $time = $timeportmaxi;
    }
346 $database->disconnect;
    unlink ("/home/cponsen/mysql/insertPort.lock");
```

Fichier : insertAsH.pl

```
    #!/usr/bin/perl
 2  if((-e "/home/cponsen/mysql/insertAs.lock") || (-e "/home/cponsen/mysql/global.lock")) {
       print "Script already running";
 4     exit(2);
    }
 6  open(OUT,"> /home/cponsen/mysql/insertAs.lock");
    print OUT "encours";
 8  close(OUT);
    use DBI;
10  use router;
    my $database = DBI->connect("DBI:mysql:flowtools:localhost:3306","flowtools", "netflow");
12  $timeasmaxi = 0;
    for($boucle=0;$boucle<48;$boucle++) {
14     $statement = $database->prepare('select UNIX_TIMESTAMP(max(heure))+300 from asH_'.$boucle.'')
          or die "peut pas faire le select\n";
16     $statement->execute() or die "peut pas execute le select\n";
       my @timedebut;
18     @timedebut = $statement->fetchrow_array();
        print "time tested: ".$timedebut[0]." timeasmaxi: ".$timeasmaxi."\n";
20     if(@timedebut && ($timeasmaxi < $timedebut[0] || $boucle == 0)) {
          $timeasmaxi = $timedebut[0];
22     }
       print "time tested: ".$timedebut[0]." timeasmaxi: ".$timeasmaxi."\n";
24     $statement->finish;
    }
26  if(!$timeasmaxi)
    {
28     my $i;
       my $minimum=0;
30     for($i=0;$i<24;$i++) {
          $statement = $database->prepare('select truncate(min(starttime)/300,0)*300 from Data_'.$i.' ')
32           or die "peut pas faire le select";
          $statement->execute() or die "peut pas execute le select\n";
34        @timedebut = $statement->fetchrow_array();
          $statement->finish;
36        print"minimum: $minimum time: ".@timedebut[0]."\n";
          if($minimum==0){
38           $minimum=@timedebut[0]+0;
          }
40        else
```

```
        {
42          if(@timedebut[0]) {
                if(@timedebut[0]<$minimum) {
44                  $minimum = @timedebut[0];
                }
46          }
        }
48
    }
50  if($minimum == 0) { print"peut pas, tables vides\n";exit();}
    $timeasmaxi = $minimum;
52 }
print "TimeAsMaxi:".$timeasmaxi."\n";
54 #$table=((@time[0]/86400)%7);
$statement = $database->prepare('select UNIX_TIMESTAMP(NOW())')or die "Peut pas preparer la demande de %%@
56 now";
$statement->execute();
58 @timefin = $statement->fetchrow_array();
$statement->finish;
60 $timefin = @timefin[0]-300;
$time = $timeasmaxi;
62 $wherein = "(".getWhereRouterIn().")";
$whereout = "(".getWhereRouterOut().")";
64 print "Traitement de la table Data_$table\n";
for($table=0;$table<24;$table++) {
66    print "Traitement de la table Data_$table\n";
    while($time <= $timefin) {
68      ($secondes,$minutes,$heure) = (localtime)[0,1,2];
        $timefininterval = $time+299;
70      print"   Table $table Heure courante: $heure : $minutes : $secondes.
              Heure debut interval: $time.\n
72            Heure fin interval: $timefininterval.
                 Heure fin traitement prevu: $timefin\n";
74      $query = " select count(*)
                          from Data_".$table."
76                        where starttime >= $time
                          and starttime < $timefininterval
78                        and srcas <>0
                          and destas <> 0
80                        and ".$wherein."";
        $statement = $database->prepare($query);
82      $statement->execute();
        @nombrerecord = $statement->fetchrow_array();
84      print "nombrerecords:".$nombrerecord[0]."\n";
        $statement->finish;
86      if($nombrerecord[0] == 0) {
            #print "ici:".$statement->rows."\n";
88          $time=$time+300;
            next;
90      }

92

94      $query ="select router,
          inputifindex,
96        outputifindex,
          sum(bytes) as total,
98        srcas,
          destas
100       from Data_$table
          where starttime >= $time
102       and starttime < $timefininterval
          and srcas <>0
104       and destas <> 0
          group by router,inputifindex,outputifindex,srcas,destas";
106       $statement = $database->prepare($query)
            or die "peux pas preparer la requete de select".$database->errstr."\n";
```

```
108         #print "requete: $query\n";
            $statement->execute() or die "peut pas executer le select: ".$database->errstr;
110         print "rows traites:".$statement->rows."\n";
            $statementheure=$database->prepare("select FROM_UNIXTIME(".$time.")");
112         $statementheure->execute;
            @heure = $statementheure->fetchrow_array();
114         $statementheure->finish;
            $realtable = int($time/3600)%48;
116         while(@data = $statement->fetchrow_array()) {
               $insert = "insert into asH_".$realtable." values (
118                       '".@data[0]."',
                          ".@data[1].",
120                       ".@data[2].",
                          ".@data[3].",
122                       ".@data[4].",
                          ".@data[5].",
124                       '".@heure[0]."')";

126            $statement2 = $database->prepare($insert)
                  or die "Peux pas preparer le insert:".$database->errstr." statement: ".$insert;
128            $statement2->execute() or die "Peux pas executer l'insert:".$database->errstr;
               $statement2->finish;
130         }
            $time=$time+300;
132         $statement->finish;
         }
134      $time = $timeasmaxi;
      }
136   $database->disconnect;
      unlink("/home/cponsen/mysql/insertAs.lock");
```

Ici se termine l'ensemble du code source lié à l'implémentation de la méthode chez Skynet. Toute la partie collecte a été modifiée par l'équipe Skynet elle-même et ces fichiers sources n'apparaîtront pas dans ces pages.