

Rapport de stage :

Mise en place d'outils de supervision
IPv6 au sein du réseau RENATER

Entreprises:



Renater

Simon MUYAL
Mastère SCR, ENSEEIHT
2002-2003



Remerciements

Je tiens tout particulièrement à remercier mes maîtres de stage M. Silvère PRADELLA et M. Bernard TUY pour leur accueil chaleureux, ainsi que M. Dany VANDROMME, le directeur du GIP RENATER, de m'avoir accepté en tant que stagiaire au sein de CS et du GIP RENATER.

Je remercie également M. Jérôme DURAND, M. Pierre-Emmanuel GOIFFON, M. Thierry BONO et M. François-Xavier ANDREU pour leur soutien technique.

D'une façon plus générale, je remercie l'ensemble du NOC (Network Operations Center) CS et le GIP RENATER, pour l'intérêt qu'ils m'ont porté tout au long de mon stage ainsi que pour leur aide et précisions.

Je remercie de même, ma tutrice de stage Mme. Béatrice PAILLASSA pour son encadrement pendant celui-ci.

Sommaire

REMERCIEMENTS.....	3
SOMMAIRE	4
INTRODUCTION.....	5
1. PRESENTATION DES ENTREPRISES.....	6
1.1 PRESENTATION DE CS	6
1.1.1 Historique de CS.....	7
1.1.2 Organisation et activités de CS.....	8
1.1.3 Présentation du NOC	10
1.2 PRESENTATION DE RENATER.....	11
1.2.1 Le réseau RENATER.....	11
1.2.2 RENATER et IPv6	12
1.3 PRESENTATION DU GIP RENATER.....	12
1.3.1 Historique.....	12
1.3.2 Son métier : Maîtrise d'ouvrage.....	12
2. ETUDES DES BESOINS.....	13
2.1 OUTILS DE SUPERVISION UTILISES EN IPV4.....	14
2.1.1 Au NOC (CS).....	14
2.1.2 Au GIP Renater	15
2.2 ETAT DE L'ART DES MIB IPV6	17
2.3 LES OUTILS EXISTANTS EN IPV6	19
3. TRAVAUX REALISES	21
3.1 MISE EN PLACE D'UN LOOKING GLASS.....	21
3.1.1 Problématique	21
3.1.2 Solution – Mise en place de l'outil:	22
3.2 INVENTAIRE DES EQUIPEMENTS DE RENATER-3 :	25
3.2.1 Contexte.....	25
3.2.2 Objectifs	26
3.2.3 Présentation de l'application	27
3.3 CONCLUSION	34
4. EVOLUTIONS POSSIBLES	34
4.1 EVOLUTIONS A COURT TERME	34
4.2 EVOLUTIONS A MOYEN ET LONG TERMES	34
5. CONCLUSION.....	35
6. GLOSSAIRE.....	36
7. REFERENCES BIBLIOGRAPHIQUES.....	37
8. ANNEXES.....	38

Introduction

Ce stage, d'une durée de six mois, a consisté à mettre en place des outils d'administration IPv6 pour le réseau RENATER.

Ce rapport présente le travail que j'ai effectué lors de mon stage au sein de CS et du GIP RENATER. Il s'est déroulé du 1 avril au 16 mai 2003 au NOC RENATER dans l'entreprise CS et du 19 mai au 30 septembre 2003 au GIP RENATER. Pendant la période au NOC RENATER, je me suis familiarisé avec un environnement technique et un ensemble d'applications IPv6. Ceci m'a permis ensuite, dans la deuxième partie de mon stage au GIP RENATER de mettre en place des outils d'administration IPv6.

Le projet réalisé s'est avéré très intéressant et très enrichissant pour mon expérience professionnelle. En effet, ma formation s'inscrit précisément dans ce secteur (spécialisation Systèmes de Communications et Réseaux). Grâce à ce stage, j'ai travaillé sur des projets qui m'ont permis d'entrevoir en quoi consiste la profession d'ingénieur dans ce secteur d'activité.

Le but de ce rapport n'est pas de faire uniquement une présentation exhaustive de tous les aspects techniques que j'ai pu apprendre ou approfondir, mais aussi, de manière synthétique et claire, de faire un tour d'horizon des aspects techniques et humains auxquels j'ai été confronté.

Je vous expose dans ce rapport en premier lieu une présentation des entreprises. Ensuite, je vous explique les différents aspects de mon travail durant ces quelques mois et enfin, en conclusion, je résume les apports de ce stage.

1. Présentation des entreprises

1.1 Présentation de CS

CS Communication & Systèmes est un acteur majeur des technologies de l'information et de l'intégration de systèmes. Il se compose de 3000 collaborateurs dont 70 % d'ingénieurs. Il a réalisé un chiffre d'affaires en 2002 de 387 millions d'euros.

La vocation du groupe CS est de construire des solutions globales dans le domaine des télécommunications, des systèmes et services informatiques et de la sécurité. CS met au service de ses clients son intelligence des réseaux, son expertise scientifique et technique et son savoir-faire industriel.

Associant avance technologique, orientation produit / marché et solidité financière, CS apporte à ses clients des réponses en forte réactivité aux grandes mutations des technologies et des marchés mondiaux.

Etre un acteur engagé de la révolution des réseaux qui modèle déjà le troisième millénaire : c'est ainsi que le Groupe CS exprime sa fidélité à sa vocation originelle d'innovateur technologique sur des marchés à forte croissance. Sa vocation est de participer à la révolution des réseaux de communication et d'information. Celle-ci se situe au croisement de l'industrie, des systèmes et des services.

Son ambition est de s'établir parmi les leaders européens sur ses marchés grâce à sa capacité d'innovation, son potentiel humain et technologique, sa solidité financière et sa stratégie de croissance dynamique.

1.1.1 Historique de CS

- 1902** Création de la *Compagnie des Signaux et d'Entreprises Electriques* (CSEE) par Francis Cumont, un pionnier de la signalisation électrique pour les chemins de fer et le métropolitain. La société devient la référence majeure dans les domaines mécanique, électrique puis électromécanique.
- Années 50-60** CS prend le virage de l'électronique pour l'appliquer à la signalisation, aux télé-contrôles et aux télémesures. La société s'impose alors sur des marchés en pleine croissance : Télécoms, Défense, Péages routiers et Transports.
- Années 90** CS se positionne, à travers ses différents métiers, comme un spécialiste des réseaux et des systèmes d'information.
- 1991-1995** CS est marqué par une croissance résolue dans le domaine des technologies de l'information, en particulier grâce à l'acquisition des sociétés SECRE, RCE, Vérilog et CSTI.
- 1996-1997** Le Groupe CS mène à bien un recentrage décisif de ses activités sur des secteurs à forte croissance liés aux systèmes d'information : développement dans le domaine du logiciel avec l'acquisition du groupe CISI, renforcement de la dimension équipement télécoms et ingénierie de réseau avec l'acquisition de Philips Communication d'Entreprise, création du pôle sécurité avec l'acquisition de MATRA Sécurité, de Ritzenthaler et de sa filiale Haffner.
Par la même occasion, il abandonne ses activités CSEE-Transport et CS-Défense
- Juillet 1999** CS Compagnie des Signaux devient *CS Communication & Systèmes*, unifiant ainsi la marque commerciale et la dénomination sociale du groupe, intégrant les marques CISI, ATHESA, EXPERDATA, TRANSTEC, AIP. Ces marques, encore présentes dans l'esprit de tous ceux qui leur font confiance sont amenées à disparaître progressivement.

Aujourd'hui, le groupe CS s'est définitivement recentré sur les technologies de l'information à travers sa branche d'activité initialement connue sous le nom de CS SI (Systèmes d'Informations), après le dépôt de bilan de CS Télécoms (équipements réseaux) et la revente de son activité CS Security (sécurité physique).

1.1.2 Organisation et activités de CS



CS se positionne aujourd'hui comme une SSII différenciée, forte de ses 4 pôles de compétences complémentaires :

- Missions critiques (Applications industrielles et scientifiques, Défense et Contrôle du Trafic Aérien (CTA) et Route)
- Network Services
- Solutions et Conseil en Technologies
- Infogérance

1.1.2.1 Missions Critiques

- **Applications Industrielles et Scientifiques**, dont la mission est de promouvoir et développer des services et des solutions logicielles pour l'industrie et les organismes de recherche, plus spécifiquement pour les marchés de l'espace, l'aéronautique, l'automobile, le nucléaire et les autres industries. Ses offres s'articulent autour des logiciels embarqués, systèmes temps réels, réalité virtuelle, etc...
- **Défense / CTA**, dont la mission est de fournir "clé en main" des systèmes liés aux domaines sectoriels, comme le commandement, la conduite et la communication pour des applications militaires, le renseignement, simulateurs de contrôle du trafic aérien civil ou militaires, systèmes d'informations logistiques, etc..
- **Route**, dont la mission est d'intégrer des systèmes appliqués au secteur du transport routier. Elle propose des offres pour les systèmes de péage et télé péage, pour les réseaux d'appels d'urgence et la gestion et le contrôle de trafic.

1.1.2.2 *Network Services*

Cette activité a pour mission de concevoir, déployer, intégrer et maintenir les réseaux des grandes ou moyennes entreprises de l'ensemble du secteur des services. Ses offres:

- Audit
- Intégration de Réseaux
- Service clients

1.1.2.3 *Solutions et Conseils en Technologie*

Ses missions sont de promouvoir et développer une offre de services associés aux systèmes de communication, ainsi que de développer les services pour certaines activités (banques, etc...).

Pour cela ses offres son très larges et englobent aussi bien :

- la sécurité des communications et applications distribuées,
- les solutions d'administration, supervision, hypervision des systèmes de communication,
- la convergence multimédia des technologies réseau
- l'interaction entre l'opérateur et ses clients (Centres d'appels)
- migration, conversion de données
- monétique

1.1.2.4 *Infogérance*

Cette activité a pour mission de gérer et faire évoluer l'outil informatique de ses clients. Les solutions mises en œuvre sont des solutions adaptées aux besoins précis de chaque client, elles couvrent tout ou partie du système d'information. La direction d'activité Infogérance possède une compétence dans les activités de l'informatique scientifique et technique, dans les activités de l'informatique de gestion portant sur le maintien en condition opérationnelle des équipements (PC, serveurs, réseau), leur évolution, et la production assurée sur les ordinateurs du client ou sur ses moyens propres (plate-forme de traitement). Les services proposés sont les suivants :

- Infogérance de systèmes distribués,
- Infogérance de production,
- Infogérance de réseaux,
- Infogérance de bout en bout,
- Infogérance globale

1.1.3 Présentation du NOC

Le NOC CS est le centre où sont administrés les réseaux des clients. Ce centre traite plusieurs contrats « Education-Recherche » tels que RENATER, GEANT ou 6NET mais aussi des contrats avec de grandes entreprises telles que Manpower, Kiabi ou Quick. Dans ces différents cas, CS propose une offre complète et modulaire de prestations de services liées à la prise en charge, la conduite et l'évolution des composants du Système d'Information et la rénovation de leurs réseaux dans le cadre d'un contrat d'infogérance globale.

1.2 Présentation de RENATER

1.2.1 Le réseau RENATER

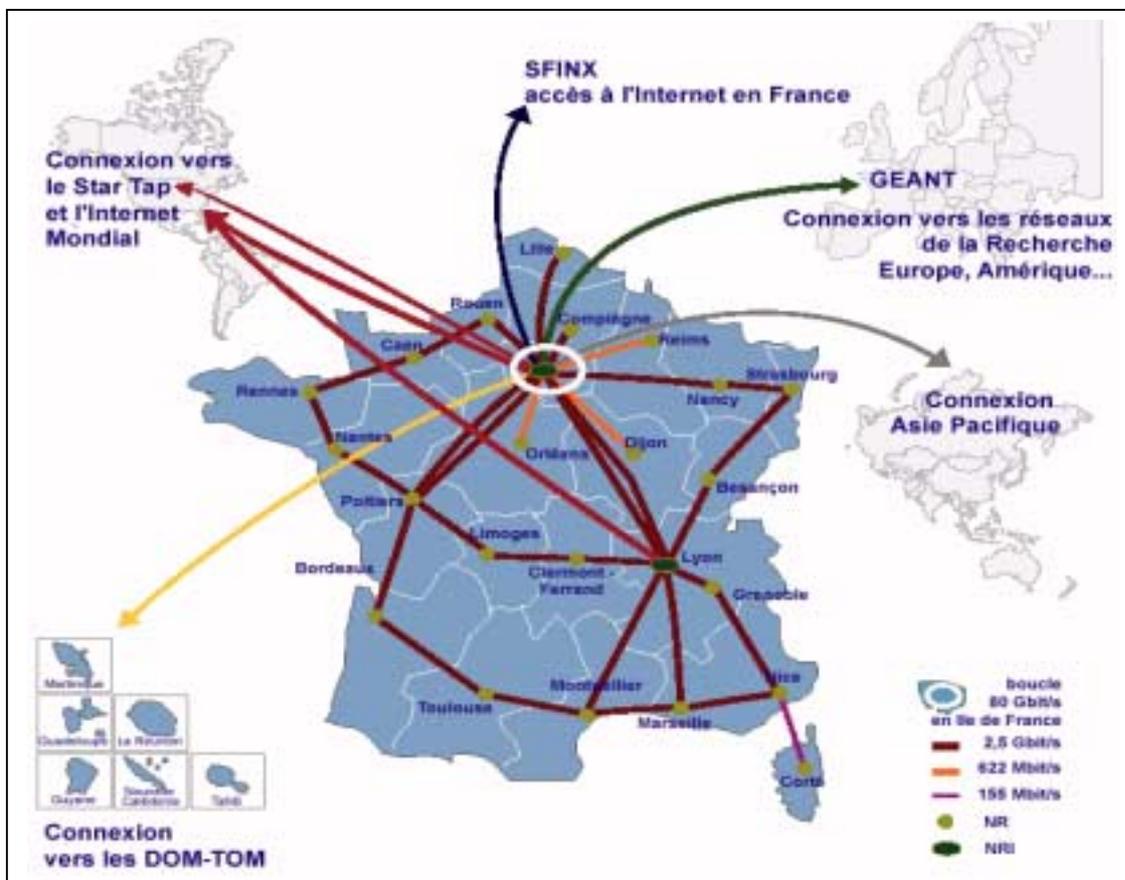
Le réseau Renater (Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche) a été créé dans les années 1990 dans le but de fédérer et d'organiser les infrastructures de télécommunications pour l'Education, la Recherche et l'Enseignement.

Aujourd'hui, plus de 600 sites sont raccordés à ce réseau. Ceci leur permet de communiquer entre eux, d'accéder aux centres de recherche publique et privée ainsi qu'aux établissements d'enseignement du monde entier via l'Internet.

Le réseau Renater est composé d'une infrastructure métropolitaine et des liaisons internationales à haut débit. Des points de présence de Renater sont également implantés dans les départements d'Outre Mer. Renater est basé sur une architecture distribuée : il comprend une épine dorsale nationale à haut débit qui fédère des réseaux de collecte (RdC) régionaux développés avec le soutien des collectivités territoriales.

Renater est interconnecté à 2.5 Gbit/s aux autres réseaux de recherche européens via le réseau européen GEANT. D'autre part, Renater contribue au développement et à l'optimisation de l'Internet en France. Pour cela, le Groupement d'Intérêt Public (GIP) Renater a créé le SFINX, un point d'échange entre les opérateurs présents en France. Le débit d'interconnexion entre Renater et le SFINX est de 1 Gbit/s. Enfin, la communication avec l'Internet dans le reste du monde est assurée par le raccordement de Renater à 2.5 Gbit/s à l'épine dorsale Internet OpenTransit de France Télécom.

Voici un schéma décrivant l'architecture globale du réseau RENATER3:



1.2.2 RENATER et IPv6

IPv6 est la nouvelle version du protocole IP de l'Internet. Ce protocole a été conçu pour s'affranchir des limitations d'IPv4 (pénurie d'adresses IPv4, explosion des tables de routage...), mais aussi pour prendre en compte les avancées issues des recherches sur les réseaux, comme l'auto configuration, la mobilité, le multicast ou encore la sécurité.

En Europe, les réseaux de la recherche sont très actifs pour préparer et commencer cette migration, et proposer un service IPv6 pour les expérimentations des premiers utilisateurs. Renater est au premier plan de cette évolution : dans Renater 3, le service IPv6 est disponible dans chaque point de présence régional de l'épine dorsale. Tous les routeurs de Renater 3 sont « dual stack » (double pile IPv4 et IPv6). Depuis le 15 Avril 2003, la connexion de Renater avec GEANT transporte du trafic IPv6 en mode natif.

1.3 Présentation du GIP RENATER

1.3.1 Historique

Créé en 1993, le GIP RENATER compte aujourd'hui 7 organismes membres : Les ministères en charge de l'enseignement supérieur et de la recherche, le CNRS, le CEA, l'INRIA, le CNES, l'INRA et le CIRAD.

Un GIP est un organisme à but non lucratif, réunissant des administrations de l'Etat et des organismes publics pour une activité définie : dans le cas du GIP Renater il s'agit de la maîtrise d'ouvrage du réseau Renater.

1.3.2 Son métier : Maîtrise d'ouvrage

Le GIP Renater est le maître d'ouvrage de la partie commune de Renater, constituée de son épine dorsale, des liaisons internationales, de ses actions pilotes, et du service SFINX. Il est le coordinateur du réseau pour l'ensemble des communautés académique et de recherche. Il représente le réseau Renater auprès des institutions françaises et étrangères, et notamment auprès des autres réseaux de la recherche.

2. Etudes des besoins

L'administration des réseaux se décompose en un ensemble de tâches, chacune ayant une fonction bien particulière. Afin de mieux définir les besoins, nous allons d'abord présenter brièvement l'ensemble de ces tâches:

- Supervision - Monitoring: La supervision est essentielle à la bonne administration d'un réseau. Elle consiste à vérifier qu'un ensemble d'équipements constituant un réseau (Routeurs, switches, serveurs, PCs) fonctionne correctement. Elle permet donc de connaître à tout moment la disponibilité du réseau. Un standard est utilisé dans la quasi-totalité des réseaux pour réaliser ceci. Il s'agit de SNMP (Simple Network Management Protocol) : Ce protocole permet de collecter diverses informations stockées dans les équipements du réseau dans des bases de données appelées MIB (Management Information Base). Les équipements sont aussi capables de faire remonter des alertes (traps) au collecteur SNMP via ce protocole.
- Métriologie: La métriologie fait partie de la supervision. Elle consiste à surveiller et analyser le trafic véhiculé par les équipements réseaux. Elle permet donc d'évaluer le type et la quantité de trafic dans le réseau. La métriologie a pris ainsi une place importante dans le monde de l'administration des réseaux: Parmi les utilisateurs de ce service se trouvent les opérateurs qui l'emploient entre autres pour suivre la consommation de leurs clients et vérifier qu'elle est conforme à leur contrat (Accounting – Billing). De même, ils vérifient que leurs liens physiques n'atteignent pas la capacité limite. Grâce aux fonctions de quelques outils, il est possible de faire du "reporting". De cette façon, il est plus facile de prévoir le dimensionnement du réseau lors de migrations.
- Sécurité: De nos jours, il est indispensable d'avoir une politique de sécurité dans un réseau afin d'assurer principalement l'intégrité et la confidentialité des données. Pour cela, il faut mettre en place plusieurs niveaux de sécurité. Premièrement, il est nécessaire de sécuriser l'accès physique aux équipements réseaux (routeurs, switch) et aux serveurs (collecteurs, serveur d'authentification...). Ensuite, afin de restreindre l'accès aux utilisateurs non autorisés, des filtres sur les adresses IP et les ports (Access List, IPTables, ACL) ainsi que sur les services applicatifs (Certificats de sécurité, PKI) sont mis en place. Finalement, l'information transmise sur le réseau doit être cryptée pour éviter que des informations confidentielles comme les mots de passe circulent en clair. Actuellement la plus part des outils d'administration offrent ces fonctionnalités. Ainsi, l'administration peut se faire de manière sûre et efficace.
- Topologie: La topologie permet de connaître à travers l'élaboration de schémas l'architecture du réseau. Il est donc très important de maintenir à jour ces schémas pour avoir une vision correcte du réseau.

- **Inventaire:** L'inventaire permet de recenser l'ensemble des équipements qui constitue un réseau. Il a aussi pour but de tenir à jour la configuration de ces équipements. Si un inventaire n'est pas fait, il se peut, par exemple, que certains équipements du réseau ne soient pas supervisés. C'est pour cela qu'il est important de maintenir à jour l'inventaire, en même temps que le réseau évolue.

Actuellement, il existe un éventail d'outils permettant d'administrer des réseaux IPv4. Il est nécessaire de disposer également d'un certain nombre d'instruments pour administrer les réseaux IPv6. Quelques outils existants en IPv4 sont déjà disponibles en IPv6.

Le fait d'administrer des réseaux IPv6 ne signifie pas que les outils employés transportent l'information en IPv6. En effet, la majorité des équipements sur le réseau étant en Dual Stack (IPv4 – IPv6), l'accès aux équipements peut se faire en IPv4 pour récupérer des informations sur la supervision IPv6. Cette solution est retenue très souvent car certaines applications ne supportent pas encore le transport en IPv6. Cela permet aussi aux NOC n'ayant pas encore un plan d'adressage de supervision en IPv6, d'administrer des réseaux aussi bien IPv4 qu' IPv6. Généralement, un pool d'adresses est réservé pour l'administration des équipements. On peut différencier les interfaces dédiées au trafic des interfaces de supervision. Ainsi, un plan d'adressage est défini et permet aux NOC d'accéder aux équipements.

Cependant, un effort reste à faire pour atteindre le même niveau de supervision qu'en IPv4. Les récentes normalisations réalisées par les organismes comme l'IETF ne sont pas encore mises en œuvre par les constructeurs d'équipements ou les éditeurs de logiciels de supervision. Par exemple, les MIB permettant de mesurer le trafic IPv6 sont pratiquement inexistantes chez des constructeurs comme Cisco.

2.1 Outils de supervision utilisés en IPv4

2.1.1 Au NOC (CS)

Afin de superviser de façon globale des réseaux comme RENATER, le NOC utilise des plate-formes de supervision telles que HP OpenView. Cette plate-forme intègre un ensemble d'outils très vaste (génération de cartes réseaux, interrogation des équipements, alarmes...). Cependant, ces plate-formes ne répondent pas forcément à des besoins précis. Ainsi très souvent, des programmes sont développés pour automatiser des tâches de supervision bien précises. Par exemple, la configuration ou la mise à jour des versions logicielles des routeurs peut se faire avec l'utilisation de scripts. Ces scripts sont écrits généralement en Perl ou en Shell Unix.

D'autre part, des outils de métrologie sont employés au NOC RENATER. Celui qui est utilisé principalement est MRTG. Il a le grand avantage de générer les graphes sur le web et d'être gratuit. Il se base sur des requêtes SNMP collectant les informations de trafic sur l'ensemble des interfaces des équipements. De plus, sa configuration est simple : Détection des interfaces actives sur un équipement lors de la génération de la configuration, puis interrogation par polling SNMP sur l'ensemble de ces interfaces.

D'autres outils semblables tels qu'Infovista sont employés pour suivre le trafic de réseaux tels que GÉANT. Cette application se base aussi sur des requêtes SNMP pour collecter les informations sur le trafic. Infovista peut générer des rapports sur l'ensemble des équipements du réseau. Avec ces rapports, il est possible d'analyser rapidement le trafic sur l'ensemble des liens pour une période donnée (semaine, moi, an). Cependant, il est nécessaire de configurer l'ensemble de ces équipements avec les mêmes paramètres pour que les rapports générés soient cohérents. Les compteurs utilisés par Infovista sont codés sur 64 bits (au lieu de 32 bits), ce qui évite la remise à zéro régulière, particulièrement dans le cas des interfaces ayant un débit élevé. Cette application demande l'installation de plug-in afin de consulter les graphes sur le web.

2.1.2 Au GIP Renater

Bien que l'administration soit réalisée par le NOC, le GIP Renater utilise aussi des outils de métrologie. En effet, ces outils permettent principalement de vérifier si les débits définis dans les contrats des différents sites sont respectés. De plus, ils permettent de mieux dimensionner le réseau et de détecter des problèmes de sécurité (Déni de services...). Deux applications ont été développées au GIP ; la première se base sur le protocole SNMP et la deuxième sur la fonctionnalité Netflow, proposée dans les versions logicielles (IOS) des routeurs Cisco.

2.1.2.1 SNMP

Le premier outil de métrologie se base sur un ensemble de programmes écrits en C permettant de collecter les informations sur les MIB des routeurs de RENATER-3 via SNMP. Ces informations sont stockées dans une base de données Mysql et peuvent être consultées via le web à travers une interface réalisée en PHP (consultable par le personnel du GIP). Les informations collectées sont les champs de la MIB (OID) correspondant au trafic et à la charge CPU des routeurs.

Avec cet outil, le GIP est capable de connaître les sites qui dépassent le débit autorisé. En effet, dans le contrat d'un site raccordé à RENATER-3, un débit est spécifié et le site est tenu de le respecter.

Cet outil permet aussi de mieux dimensionner le réseau. Ainsi lors d'une migration, il est possible d'évaluer les liaisons qui se rapprochent de la saturation et qui doivent être mises à jour (cf. Annexe I). Il est possible aussi de détecter ou confirmer des attaques de type Déni de Service (Denial of Service DoS). En effet, lors d'une attaque de ce type, on peut observer soudainement un grand écart entre le trafic entrant et le trafic sortant sur l'équipement (cf. Annexe II). Ceci ne permet pas d'affirmer qu'il s'agisse d'un déni de service, mais permet de repérer une anomalie ou de confirmer une attaque de ce type.

2.1.2.2 Netflow

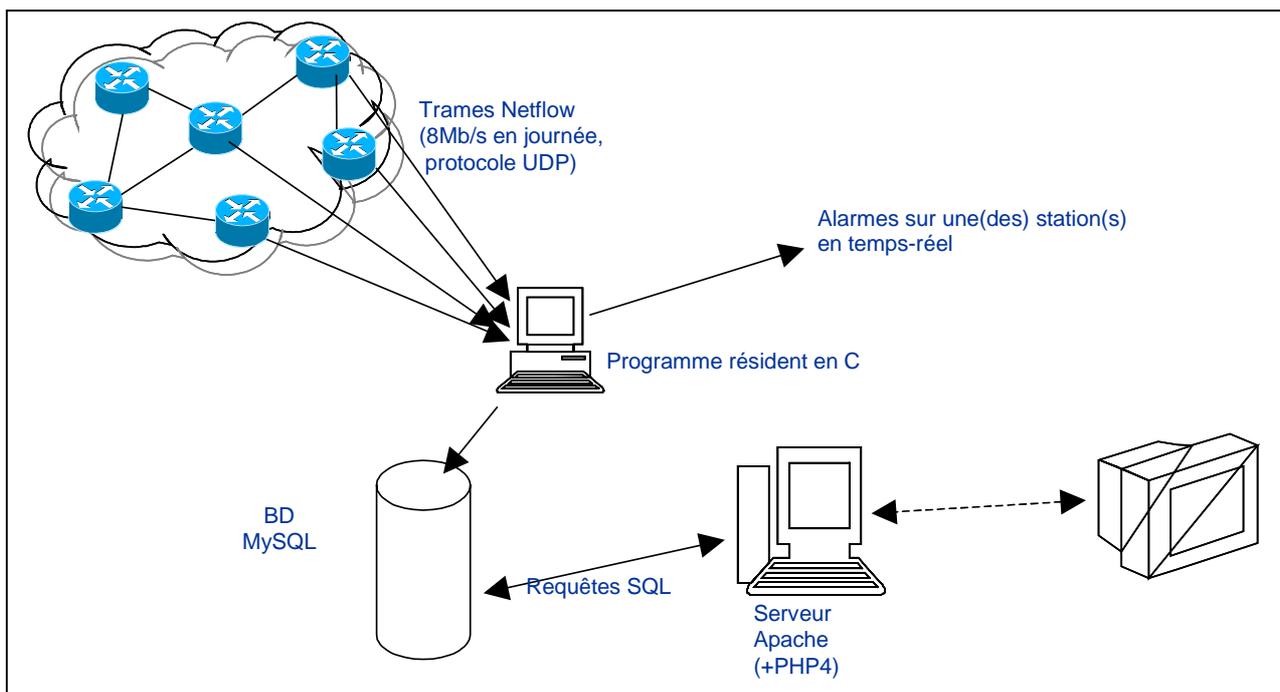
Le réseau RENATER-3 étant constitué d'équipements Cisco, le deuxième outil employé au GIP se base sur la fonctionnalité Netflow que propose le constructeur sur ses équipements. Netflow permet de caractériser les flux de données et d'avoir des statistiques précises sur le trafic.

Un flux est caractérisé par les adresses IP source et destination, les ports source et destination ainsi que le protocole, le type de service (Type of Service ToS) et l'index de l'interface. Pour un flux donné, Netflow renvoie les informations suivantes :

- Les compteurs sur les paquets et les octets reçus et envoyés.
- Le temps de début et fin du flux.
- Le numéro des interfaces d'entrée et sortie.
- Le protocole de transport employé (TCP ou UDP)
- Des informations sur le routage (Next-hop, AS source et destination, masque réseau source et destination).

Les routeurs envoient régulièrement les informations concernant les flux vers un collecteur Netflow. Un ensemble de scripts écrits en C traite les informations et les stockent dans une base de données MySQL. Connaissant la plage d'adresses attribuée à un site, les données peuvent être agrégées. Des histogrammes sur les flux peuvent être consultés sur le web à travers une interface PHP.

Voici le schéma décrivant l'architecture de l'outil :



Avec cet outil, le GIP est capable de caractériser le trafic (FTP, Web, peer to peer...) entre RENATER et les différents sites (cf. Annexe III). Ainsi, il est possible de voir la cause d'une congestion, de définir une classe de service (Class of Service : CoS) pour un site ou une application donnée ou de repérer des serveurs warez.

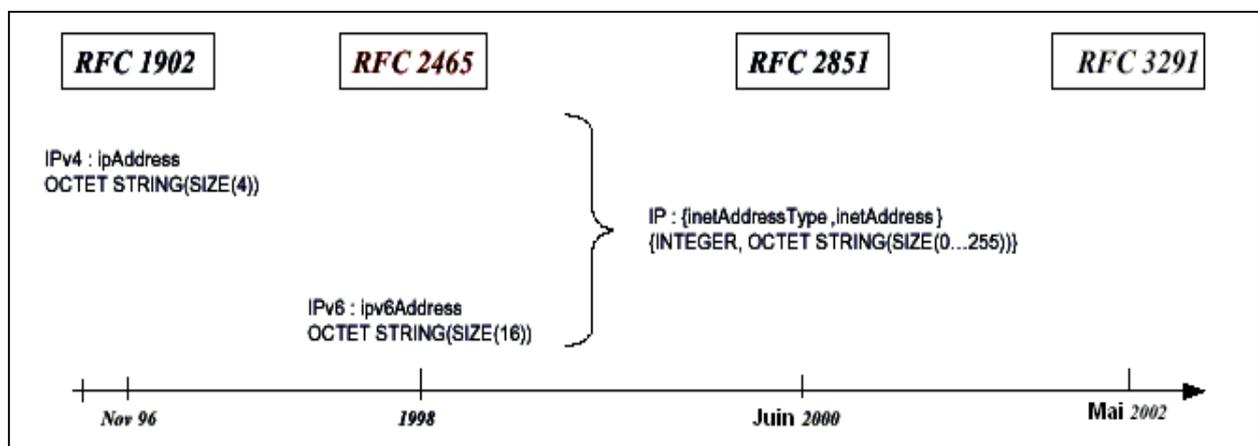
2.2 Etat de l'art des MIB IPv6

La croissance rapide des réseaux et la diversité des systèmes pendant la dernière décennie ont entraîné le besoin d'une gestion globale des infrastructures réseaux. SNMP s'est avéré être une bonne solution proposée et standardisée par l'IETF (Internet Engineering Task Force). Ainsi, le protocole SNMP et les MIB sont devenus les deux éléments principaux du modèle de supervision de réseaux.

Le protocole SNMP étant indépendant de l'architecture du protocole IP, son évolution vers IPv6 n'a pas représenté un problème majeur. La première implantation de SNMP pour le protocole IPv6 a été réalisée par l'équipe du Loria de l'université de Nancy (NET-SNMP OpenSource) et a été disponible dans la version 5.0.3 de net-snmp, en mai 2002. Avant cette première version, l'administration des réseaux IPv6 était possible du fait que les équipements étaient Dual Stack IPv4-IPv6. En effet, il était possible d'accéder en SNMP sur un équipement en IPv4 et de récupérer des champs de la MIB concernant IPv6. Ainsi, jusqu'ici, il n'y avait pas un grand besoin d'avoir une version de SNMP IPv6. Aujourd'hui, certains réseaux projets ne véhiculent que du trafic IPv6 d'où la nécessité de disposer d'une version IPv6 pour le transport du protocole SNMP.

Par contre, l'évolution des MIB est plus complexe. Depuis les spécifications initiales du protocole IPv6, en 1995, la définition de la MIB-2 pour l'administration des réseaux IPv6 a été modifiée à deux occasions : la première en 1998 et la deuxième en 2000. Le problème principal était de définir le type du champ "IP ADDRESS".

Voici son évolution dans les dernières années :



En 1996, une première représentation du champ "IP ADDRESS" est décrite dans la RFC 1902 où la longueur réservée pour ce champ est de 4 octets. Avec ce champ ne peuvent être représentées que les adresses IPv4. En effet, les adresses IPv6 ayant une longueur de 128 bits, 16 octets sont nécessaires pour les représenter. C'est pourquoi, en 1998, nous trouvons dans la RFC 2465, la définition du champ "Ipv6Address" sur 16 octets.

Ainsi de nombreuses RFCs ont été affectées par ces modifications. D'abord, avec la première approche de créer des MIB IPv4 et IPv6 indépendantes, de nouvelles RFC ont vu le jour. Principalement, les RFCs décrivant les MIB IPv6 sur transport TCP ou UDP (RFC 2452

et RFC 2454) ont été publiées en 1998. De même, une MIB concernant le protocole ICMPv6 a été décrite dans la RFC 2466.

Cependant, cette approche implique une gestion indépendante des protocoles IPv4 et IPv6. Ainsi, l'IETF a décidé de définir une MIB-2 unifiée, permettant de superviser les réseaux IPv4 et IPv6 (RFC 2851 – Juin 2000). Cette RFC définit le champ "IP ADDRESS" comme une structure avec deux champs. Le premier champ permet de différencier le type d'adresses (IPv4 ou IPv6). Le deuxième champ est une chaîne de caractères à longueur variable. Ainsi, ce champ peut contenir des valeurs de longueur égale à 4 ou 16 octets (IPv4 ou IPv6).

Afin d'améliorer la description de la RFC 2851 est apparue en mai 2002 la RFC 3291. Des informations supplémentaires sont décrites comme le préfixe réseau, le numéro de port utilisé par la couche transport ou le numéro d'AS (Autonomous System) correspondant à l'adresse IPv4 ou IPv6. Ainsi la RFC 2851 devient obsolète.

Ensuite, la volonté d'avoir une MIB unifiée a entraîné aussi la mise à jour de MIB déjà existantes. Actuellement, l'IETF publie des propositions (drafts) de mise à jour pour les RFCs 2011, 2012, 2013 et 2096. Les dernières propositions publiées sont draft-ietf-ipv6-rfc2011-update-03.txt (juillet 2003), draft-ietf-ipv6-rfc2012-update-03.txt (juin 2003), draft-ietf-ipv6-rfc2013-update-03.txt (avril 2003), draft-ietf-ipv6-rfc2096-update-04.txt (juin 2003). Ces drafts concernent respectivement les MIB IP, TCP, UDP et IP Forwarding table.

En raison de toutes ces modifications, les MIB ne sont pas entièrement disponibles aujourd'hui en IPv6. En effet, très peu de réalisations ont été effectuées par les constructeurs.

Juniper a réalisé un premier effort en implémentant une MIB propriétaire sur ses routeurs en se basant sur la RFC 2465. Cette MIB permet de faire de la métrologie sur le nombre de paquets entrants et sortants. Par contre, elle ne permet pas de récupérer le nombre d'octets émis et reçus.

Cisco a implémenté sur ses équipements une MIB propriétaire (CISCO-IETF-IP-MIB). Cette MIB permet de récupérer un certain nombre d'informations IPv6 de base (interfaces, messages ICMP : cf. Annexe IV). Par contre, malgré les demandes de plusieurs clients, Cisco n'a pas encore implanté une MIB permettant de différencier le trafic sur les interfaces transportant les deux versions IP le trafic IPv6. Cisco annonce une MIB permettant d'avoir des compteurs sur le trafic IPv6 prochainement.

Une autre conséquence est que les grandes plate-formes de supervision comme Tivoli ou InfoVista ne sont pas disponibles en IPv6; HP OpenView propose une version IPv6 en beta-test.

2.3 Les outils existants en IPv6

Pour chaque tâche de l'administration des réseaux vue précédemment, il existe un ensemble d'outils IPv6. Voici une liste des quelques outils IPv6 les plus employés aujourd'hui:

➤ **ASPath-Tree:**

Basé sur des captures régulières de la table BGP IPv6, ASpath-tree génère automatiquement un ensemble de pages HTML fournissant une vue graphique des chemins pour atteindre les autres AS sous forme d'arbre (Annexe V).

A la base conçu pour être employé par des sites IPv6 impliqués dans l'expérimentation du protocole BGP à l'intérieur du 6Bone, il peut être aujourd'hui utilisé dans n'importe quel réseau IPv6 opérationnel qui utilise BGP comme protocole de routage.

En plus, il permet la détection des entrées anormales de routes annoncées par BGP (les préfixes interdits ou non agrégés), des numéros d'AS erronés (réservés ou privés) et fournit un ensemble d'information complémentaire comme:

- le nombre de routes (valid/total/suppressed/damped/history)
- le nombre d'AS dans la table (total, originating only, originating/transit, transit only, private and reserved)
- le nombre de voisins actifs BGP (c.-à-d. annonçant des routes)
- une analyse de la taille de réseau, en termes de distance inter-AS
- le nombre de préfixes circulant dans le réseau (total, 6Bone pTLAs, sTLAs, 6to4, autres).

L'avantage d'ASPath-Tree est qu'il permet de connaître rapidement les chemins empruntés par les paquets pour atteindre un AS en se basant sur un routeur du réseau uniquement. Ceci simplifie beaucoup la mise en place de l'outil. Cependant, ceci peut aussi présenter un inconvénient. Normalement, nous devrions avoir un même arbre quel que soit le routeur interrogé au sein du réseau. Or, si un problème de configuration est fait (voisin mal déclaré ...), l'arbre ne sera plus le même selon le routeur interrogé.

ASPath-tree facilite donc la mise en place d'une politique de routage au niveau d'un backbone.

L'outil est disponible sur <http://carmen.ipv6.tilab.com/ipv6/tools/ASpath-tree/>

➤ **Looking Glass :**

Cet outil permet, à travers une interface WEB, d'avoir un accès direct sur les routeurs ou switches. L'utilisateur dispose d'une liste de commandes qui peuvent être exécutées. Des scripts CGI permettant la connexion telnet ou SSH (en IPv4 ou IPv6) récupèrent l'information désirée et l'affichent sur une page WEB.

Son grand avantage est qu'il permet d'obtenir des informations directement sur des équipements réseaux en temps réel sans avoir un compte dédié sur ces équipements. Cependant, le fait de donner des informations sur les équipements réseaux oblige à mettre en place un certain nombre de mesures de sécurité pour préserver la confidentialité des informations (accès restreint au serveur web...).

➤ **MRTG:**

MRTG permet de générer des graphes sur le trafic réseau. Une version IPv6 de MRTG a été développée par l'université de Rome-3. Elle permet d'interroger les équipements via SNMP sur un transport IPv6. D'autres outils comme RRDtool, disponible en IPv6 permettent de faire de la métrologie.

L'outil est disponible sur <http://www.uniroma3.6net.garr.it/mrtg>

➤ **Weather map :**

Cet outil permet de présenter une carte topologique du réseau avec son trafic actuel. Il se base généralement sur des applications comme MRTG pour pouvoir afficher les graphes de trafic entre deux liens du réseau. Si nous voulons avoir un weather map représentant le trafic IPv6 uniquement, il est nécessaire que les MIB des routeurs distinguent bien le trafic IPv4 et IPv6. Or, actuellement, tous les constructeurs ne proposent pas cela. Des réseaux projets où le trafic est exclusivement IPv6, comme 6NET, peuvent disposer de cartes affichant la charge de trafic IPv6. En ce qui concerne le transport, il peut être réalisé entièrement en IPv6.

➤ **Ethereal :**

Ethereal est un analyseur réseau. Il permet d'analyser le trafic en temps réel en distinguant le trafic IPv4 et IPv6 sur une interface.

L'outil est disponible sur <http://www.ethereal.com>

➤ **Mping :**

Mping (Multipoint ping) est un outil qui se base sur les fonctionnalités de ping6. Il permet de tester la connectivité entre plusieurs interfaces IPv6 et peut réaliser des mesures de performances entre elles. Il réalise une collecte de données qui lui permet de générer des rapports et des histogrammes.

Cet outil reste pratique tant que la taille du réseau n'est pas très importante. Lorsque le réseau grandit, le nombre de requêtes est multiplié. Ainsi, le trafic ICMP généré est de plus en plus important, ce qui peut faire augmenter la CPU des équipements réseaux.

➤ **Multicast beacon :**

Multicast beacon est une application client/serveur donnant des matrices de mesures sur le trafic Multicast en IPv4 et IPv6.

Chaque client possède un démon beacon. Le démon envoie un message périodiquement aux autres membres du groupe multicast pour mesurer les pertes, le délai, la gigue, les doublons et le mauvais séquençement des paquets. Ces informations sont envoyées au serveur beacon qui peut afficher ces informations dans une table.

Cette application est réalisée en java.

3. Travaux réalisés

3.1 Mise en place d'un looking Glass

3.1.1 Problématique

L'objectif principal est de mettre en place un outil permettant aux administrateurs de la communauté Renater d'accéder rapidement à quelques commandes sur les routeurs du backbone RENATER 3.

En effet, cela doit permettre aux sites connectés en IPv6 à RENATER 3 de consulter des données qui les concernent sans intervention de la part du GIP ou du NOC et sans avoir à se connecter aux équipements directement.

Les opérations pouvant être effectuées sur les équipements réseaux sont principalement des tests de connectivité (ping) ou des consultations sur l'état du routage BGP en IPv6. Il est possible aussi d'obtenir des informations sur les interfaces et le trafic (cf. Annexe VI).

Ainsi, lorsqu'un site ou un réseau régional est confronté à un problème, il peut d'abord vérifier si la cause provient réellement de RENATER. Ceci représente un gain de temps pour les experts et techniciens du NOC RENATER qui interviennent uniquement en cas de problème étant de leur ressort.

Cet outil peut être employé de même par les personnes du GIP n'ayant pas accès aux routeurs directement. En effet, pour des raisons d'administration du réseau, un nombre restreint d'ordinateurs du GIP Renater est autorisé à accéder directement aux routeurs.

Pour la mise en place de cet outil, plusieurs problèmes se posent. Le premier est la sécurisation de la connexion entre le serveur WEB où se trouvent les scripts CGI et les routeurs. En effet, un looking glass avait été mis en place dans un réseau de test au NOC RENATER, mais la connexion aux routeurs se faisait en telnet. Ceci posait des problèmes de sécurité puisque le mot de passe d'accès au routeur ainsi que les données transférées étaient non cryptées dans le réseau. Pour pallier ce problème la connexion aux routeurs se fait en SSH (Secure Shell).

SSH définit un protocole entre un client et un serveur pour l'établissement d'une connexion distante chiffrée. SSH remplace les r-commandes (rlogin, rsh...) présentant des carences au niveau sécurité. Avec SSH, une connexion est toujours initialisée par le client. Le serveur est en écoute sur le port 22 (par défaut, mais il est possible d'utiliser un port). L'authentification et les échanges de clés se basent sur les mécanismes de clés publiques et clés privées de type RSA (Rivest, Shamir, Adleman). Le chiffrement des communications se fait avec les algorithmes de chiffrement ayant des longueurs de clés différentes : DES (56 bits), IDEA (128 bits), 3DES (168 bits), RC4 (128 bits), Blowfish (256 bits). Ces algorithmes sont appelés ciphers. Avec SSH, il est donc possible d'assurer la confidentialité lors de transfert de données entre les équipements réseaux de Renater-3 et le looking glass.

Un autre problème qui se pose est le nombre de connexions SSH sur les routeurs. En effet, à chaque requête effectuée sur l'interface web, une connexion SSH sur le routeur se produit, ce qui fait augmenter la charge de la CPU (Central Processing Unit) de celui-ci. Si un ensemble de sites se connecte simultanément sur un routeur de concentration, la CPU risque d'augmenter, ce qui diminuerait les performances du routeur. Bien que le trafic IP soit pris en charge par les processeurs des cartes des routeurs, d'autres services traités par le processeur du routeur (accès SSH, SNMP, mise à jour des tables de routage...) risquent d'être perturbés.

Ceci peut être plus grave si un pirate envoie une multitude de requêtes sur le serveur web. En effet, cela produirait un déni de service sur le routeur.

Afin d'éviter ce type de problèmes, le nombre de connexions au serveur web est limité et un mot de passe est demandé pour accéder au looking glass.

3.1.2 Solution – Mise en place de l'outil:

Le serveur hébergeant le looking glass est un serveur Sun Solaris se trouvant au NOC RENATER. Ce serveur n'ayant pas encore migré vers IPv6 (Dual Stack IPv4 – IPv6), la connexion au serveur WEB ainsi que la connexion SSH entre le serveur et les routeurs se fait pour l'instant en IPv4. Cependant, l'outil a été testé sur un serveur ayant une pile IPv6 et fonctionne correctement.

Le langage utilisé pour développer cette application est perl. Ce langage dispose d'un module permettant d'effectuer des commandes en SSH. De plus, c'est un langage qui est bien adapté pour la génération de CGI et permet de traiter avec facilité les chaînes et expressions. Il est vrai que perl, étant un langage interprété, n'offre pas des performances aussi élevées que des langages compilés tel que le C ou C++, mais il est tout à fait adapté à nos besoins.

Le serveur WEB utilisé est un serveur apache2 supportant la pile IPv6. Ainsi lorsque le serveur Sun Solaris aura migré, les utilisateurs pourront accéder au serveur WEB en IPv6.

Un serveur TACACS+ permet de faire l'authentification ainsi que l'autorisation lors de la connexion aux routeurs à partir du looking glass.

Principe du serveur TACACS+ :

L'authentification correspond à l'identification de l'utilisateur. Cette identification passe par la présentation de l'identité de l'utilisateur. TACACS+ peut aussi bien utiliser des techniques d'authentification classiques type login/mot de passe statique ou bien des procédés plus évolués à base de challenge avec authentification réciproque. Nous utiliserons dans notre cas une authentification de type login/mot de passe où les informations seront cryptées.

Lors d'une nouvelle connexion, le routeur émet un message START au serveur TACACS+ décrivant le type d'authentification à utiliser. En retour, le démon envoie un message REPLY. Ce type de message peut indiquer ou bien que l'authentification est terminée, ou bien qu'elle doit continuer, auquel cas, le client récupère l'information manquante et la retourne dans un message CONTINUE.

Le type de requête provenant du serveur peut être une demande GETDATA, GETUSER ou GETPASS. GETDATA est une requête générique de récupération d'information du profil utilisateur.

L'autorisation permet de déterminer quels sont les droits de l'utilisateur. Par exemple, après s'être logué, l'utilisateur peut essayer d'utiliser certaines commandes. L'autorisation détermine alors si l'utilisateur peut ou non les utiliser.

Lors d'un accès à un service particulier, le routeur ouvre une session d'autorisation. Cette session consiste juste en l'échange d'une paire de messages : REQUEST/RESPONSE. La requête décrit l'authentification pour l'utilisateur ou le processus qui demande l'accès au service. La réponse du serveur contient un ensemble d'attributs pouvant restreindre ou modifier les actions du client, plutôt qu'une simple réponse affirmative de type oui/non. C'est ainsi qu'il sera possible de limiter les commandes à exécuter avec le compte du looking glass.

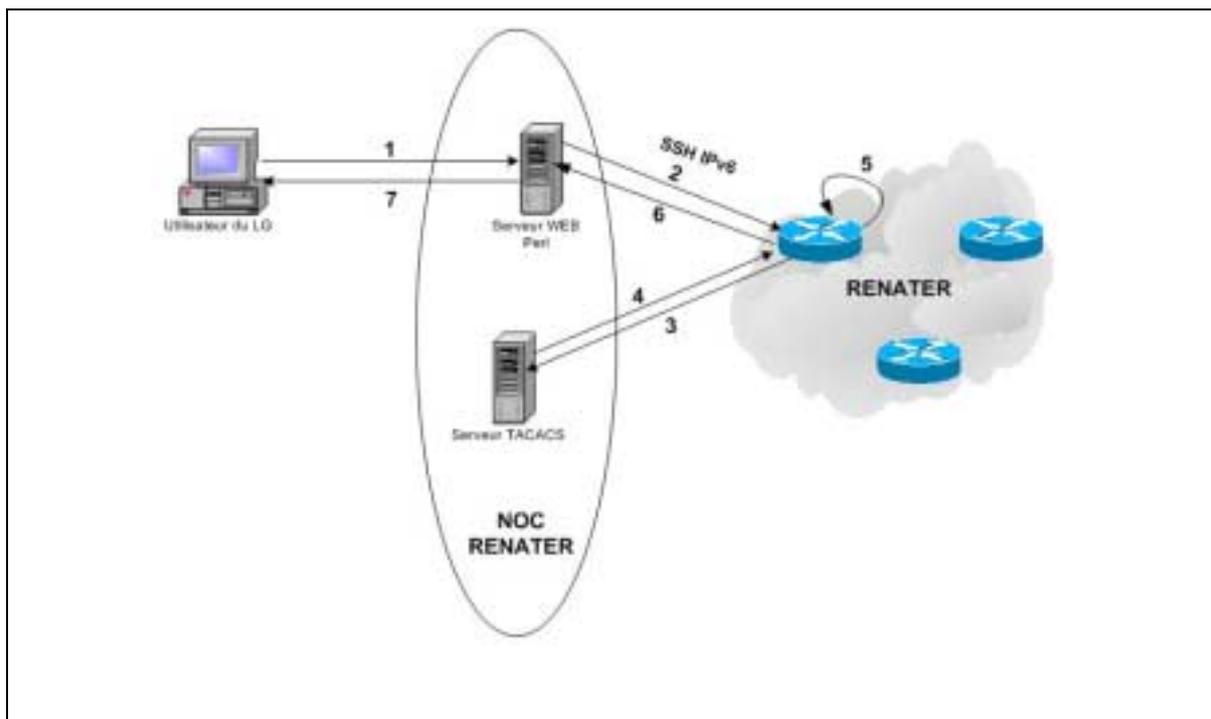
Installation et fonctionnement de l'outil :

La version 5.X de perl est déjà installée sur le serveur web. Un ensemble de modules perl a été installé afin de pouvoir se connecter en SSH sur les équipements du backbone (cf. Annexe VII). Puisque le module NET::SSH::Perl permet de se connecter uniquement en IPv4, le module IO::Socket6 a été installé et la librairie Perl.pm a été modifiée afin de pouvoir effectuer des connexions SSH en IPv6 (cf. Annexe VIII).

Pour le serveur Tacacs+, un compte pour le looking glass a été créé ; il n'autorise que les commandes disponibles sur l'interface web. Ainsi, si un pirate réussissait à accéder au serveur et à se connecter aux routeurs, il ne pourra effectuer que des commandes restreintes. Il ne pourra en aucun cas lire la configuration du routeur ni effectuer des modifications.

Les routeurs étant déjà configurés pour interroger le serveur tacacs+, il n'est pas nécessaire de modifier la configuration des routeurs (configuration : cf. Annexe IX).

Voici un schéma détaillant l'architecture globale de l'outil et son fonctionnement:



Tout d'abord un utilisateur (Site client, GIP ou NOC Renater) accède à travers son navigateur Web au serveur où se trouve le looking glass (1). L'utilisateur doit indiquer (cf. AnnexeX):

- L'équipement sur lequel il veut se connecter (liste déroulante)
- La commande qu'il veut effectuer sur cet équipement.

La liste des équipements est générée à partir d'un fichier de configuration contenant les équipements du backbone ainsi que leurs caractéristiques (cf. Annexe XI). Une fois les choix effectués, un script en perl effectue une connexion SSH vers l'équipement choisi (2). Ce script récupère les paramètres de connexion sur le même fichier de configuration. Pour des raisons de sécurité, il ne m'est pas possible de dire la version de SSH ainsi que le ciphre utilisé pour la connexion aux équipements de RENATER 3.

Ensuite le routeur interroge le serveur tacacs+ afin de vérifier la validité du mot de passe et de connaître les droits et les commandes que peut effectuer l'utilisateur connecté au routeur (3 et 4).

Une fois, l'identification réalisée, le routeur exécute la commande et renvoie le résultat au serveur (5 et 6). Finalement, le script génère une page HTML avec le résultat de la commande et le serveur Web envoie cette page à son tour à l'utilisateur (7).

Remarques :

Les scripts CGI présentent des failles de sécurité permettant à des utilisateurs d'exécuter des commandes sur le serveur où se trouvent ces scripts. Afin de se préserver de ce genre d'attaques, le code source a été analysé par le CERT Renater.

Le CERT Renater est la structure qui gère les incidents de sécurité qui lui sont rapportés.

3.2 Inventaire des équipements de RENATER-3 :

3.2.1 Contexte

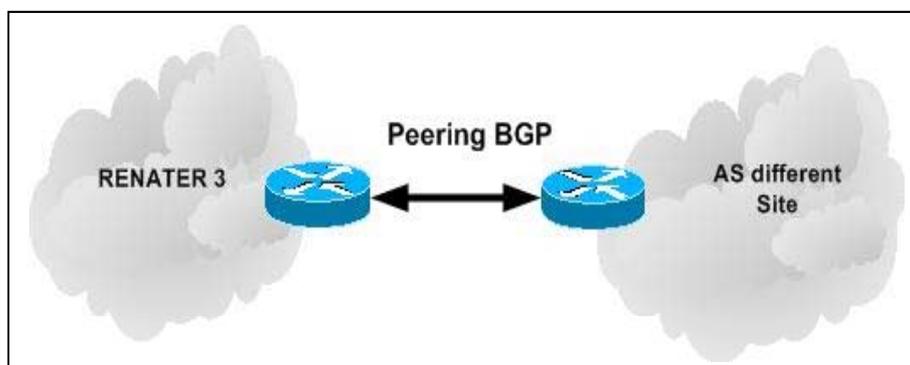
Lorsqu'un nouveau site fait une demande de raccordement en IPv6 sur RENATER-3, il est nécessaire dans certains cas d'avoir une interface disponible sur l'un des équipements du Nœud Renater (NR) sur lequel il va être connecté. Généralement, un NR est composé d'un routeur Cisco 12400 et d'un switch Cisco ATM 8540. Sur certains NR, un deuxième routeur est présent pour pouvoir établir des tunnels avec les sites. Les tunnels permettent aux sites qui sont raccordés à un réseau métropolitain (MAN) ou réseau régional n'ayant pas de connectivité IPv6 d'être connectés à Renater en IPv6. Les GSR (Giga Switch Router) de Cisco étant des équipements de backbone, la fonctionnalité de tunnel n'est pas utilisée dans le réseau Renater-3. En effet, ces équipements sont destinés à transporter de grandes quantités de trafic et la mise en place de tunnels pourrait entraîner des surcharges sur la CPU des GSR. C'est pour cela que des routeurs d'accès (Cisco 7200 ou 3600) sont installés dans certains NR.

Pour savoir si des interfaces sont disponibles, il n'existe pas un autre moyen aujourd'hui que de se connecter directement sur les équipements. Or, comme nous avons vu dans la partie précédente, l'accès aux équipements est limité à quelques personnes.

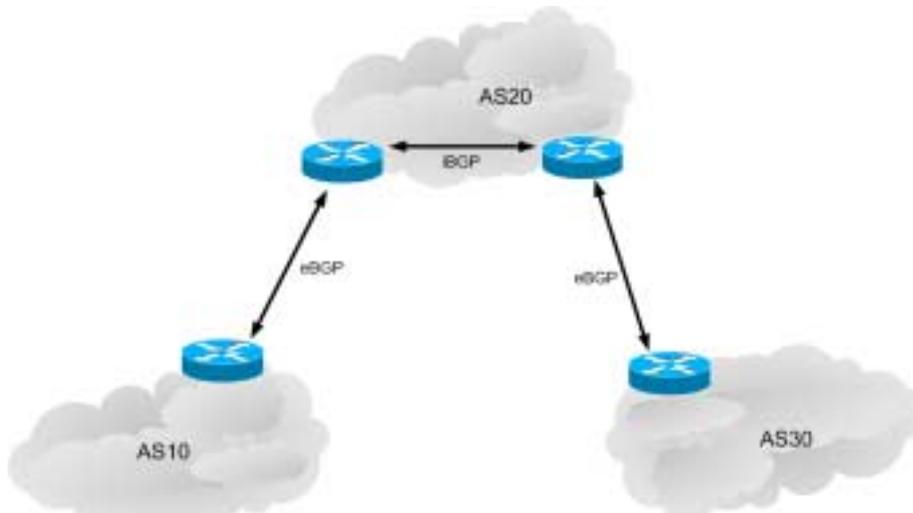
Une fois que l'interconnexion physique avec le nouveau site est faite, un peering BGP est configuré entre le routeur de Renater et le routeur du site afin que les paquets puissent être routés.

Deux protocoles assurent le bon fonctionnement de BGP : eBGP(external BGP) et iBGP (internal BGP).

Le protocole eBGP est un protocole de routage inter-système autonome (AS). Il a été développé pour remplacer Exterior Gateway Protocol (EGP). Pour qu'un AS puisse échanger du trafic avec un autre AS, il est nécessaire d'avoir un accord mutuel. Une fois cet accord établi, un peering est configuré entre deux routeurs des différents systèmes autonomes. Le routeur avec lequel le peering est établi est appelé neighbor BGP(voisin).



Le protocole iBGP permet aux routeurs appartenant à un même AS, de propager à l'intérieur d'un AS les informations reçues par eBGP:



Les échanges BGP se font sur des connexions TCP afin de rendre fiable le transfert des données.

3.2.2 Objectifs

L'objectif principal était de réaliser une application permettant de décrire la topologie du réseau Renater-3. Elle permet de faire:

- L'inventaire des interfaces disponibles sur les équipements du backbone
- L'inventaire des peerings BGP.

Ainsi, il est possible d'avoir rapidement une vue sur l'architecture d'un NR, savoir si une interface est libre ou connaître les peerings IPv6 configurés sur un équipement du backbone. Ceci représente un gain de temps, puisqu'il n'est pas nécessaire de se connecter aux routeurs pour obtenir ces informations. Cet outil permet donc à l'équipe IPv6 de faire un suivi lorsqu'un site fait une demande de raccordement en IPv6.

Cette application peut être aussi utilisée par le SSO pour consulter l'état des interfaces.

La récupération des informations sur les routeurs se fait deux fois dans la journée. Ceci est suffisant car il n'est pas question ici de surveiller l'état des peerings ou des interfaces mais d'avoir une vision sur l'architecture d'un nœud Renater.

Cette application est consultable à travers une interface web, pour que les utilisateurs du GIP puissent y accéder facilement. Les utilisateurs peuvent être l'équipe IPv6 mais aussi le SSO (Service de Suivi Opérationnel). Afin d'éviter que des personnes extérieures à RENATER accèdent à cette application, des règles de sécurité sont mises en place.

3.2.3 Présentation de l'application

Pour réaliser cette application, il est nécessaire de récupérer sur les équipements du backbone l'ensemble des interfaces ainsi que les peering BGP. Avant de commencer le développement de l'application, une étude sur les applications existantes au GIP a été faite; cela a permis de profiter d'outils déjà présents et éviter de refaire des choses existantes.

3.2.3.1 Utilisation de la base de données de métrologie

L'outil de métrologie présenté au paragraphe 2.1.2.1 récupère via SNMP les interfaces des équipements pour connaître le trafic par interface. Ces informations sont stockées dans une base de données MySQL. Nous utilisons donc cette base de données ce qui évite d'avoir plusieurs systèmes d'information. Ainsi, nous éliminons le risque d'avoir des divergences dans différentes bases de données. Les informations utilisées pour la supervision se trouvent à un seul endroit mais peuvent être utilisées par plusieurs outils. L'utilisation de la même base permet aussi d'économiser des ressources (espace disque, mémoire).

Le choix de MySQL comme base de données se justifie par plusieurs critères. Ce logiciel présente les avantages d'être gratuit et facile à interfacier avec le web (scripts CGI perl ou php). Ici, MySQL est suffisant car la taille de la base de données n'est pas très importante. Dans notre cas, il n'était pas nécessaire d'utiliser des bases de données payantes comme Oracle ou SQL Server qui offrent plus de fonctionnalités.

Pour l'outil déjà existant, un programme récupère un ensemble de champs sur les MIB correspondant aux interfaces. Pour notre application, des champs de la MIB ont été ajoutés à la base de données afin de répondre aux besoins de l'outil. Voici l'ensemble des champs de la MIB-2 récupérés par l'application:

interfaces.ifTable.ifEntry.ifIndex : Numéro identifiant l'interface sur l'équipement
interfaces.ifTable.ifEntry.ifType: Type d'interface (ATM, POS, Ethernet...)
interfaces.ifTable.ifEntry.ifDescr: Nom de l'interface. Ex: "ATM1/1"
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifAlias: Description de l'interface. Ex: "Lien vers Bordeaux".

interfaces.ifTable.ifEntry.ifAdminStatus: Etat de l'interface (1:UP, 2:DOWN) (champ ajouté)

Ces champs sont récupérés à l'aide des commandes snmpget et snmpwalk qui permettent d'interroger les MIB.

3.2.3.2 Choix du langage CGI

Pour la génération dynamique des pages html, plusieurs langages peuvent être utilisés. Les plus répandus sont Perl et PHP pour ce type d'application (interaction avec une base de données). Les deux langages présentent l'avantage d'être gratuit. Perl est pratique pour traiter des chaînes ou des textes, ce qui n'est pas le cas ici.

Le langage utilisé pour l'interface web est donc PHP.

3.2.3.3 Interrogation des équipements

La collecte des informations concernant les interfaces se fait par polling SNMP comme nous l'avons vu précédemment. Pour la collecte des peerings BGP IPv6, la première idée était d'utiliser aussi le protocole SNMP et la MIB BGP-4 (RFC 1657). Cependant, cette MIB ne permet pas de récupérer les peerings BGP IPv6 (uniquement les neighbors IPv4).

La solution choisie est de se connecter directement sur les routeurs et d'effectuer la commande qui permette de récupérer les peerings BGP. L'ensemble des routeurs étant des Cisco, la commande effectuée sera "show bgp ipv6 neighbor". Comme pour le looking glass, SSH est utilisé pour la connexion aux routeurs ce qui permet de sécuriser les échanges de données. De même, un compte Tacacs permet de faire l'authentification et l'autorisation.

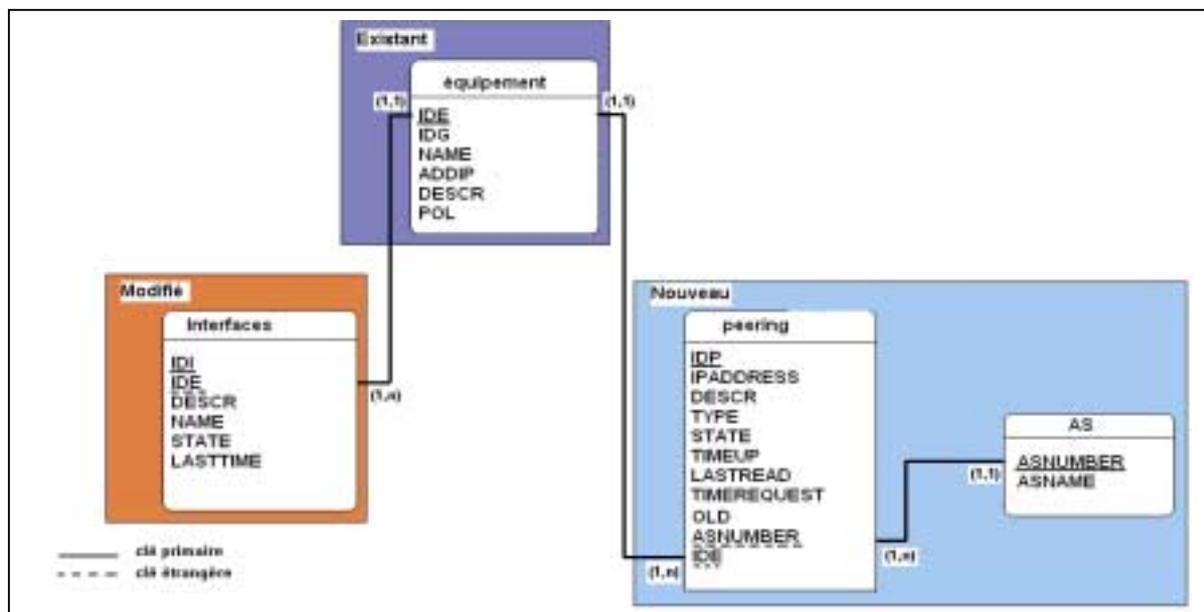
Le serveur utilisé pour faire de la collecte SNMP n'est pas autorisé à ce connecter en SSH sur les routeurs de Renater-3. Les machines présentes au GIP étant autorisées à ce connecter en SSH sont des PC de travail et non pas des serveurs dédiés à la supervision. C'est pour cela que l'interrogation se fera à partir d'un serveur du NOC Renater déjà autorisé à accéder en SSH aux routeurs de Renater-3.

Généralement, une connexion SSH n'est pas utilisée pour collecter régulièrement des informations sur des routeurs (augmentation de la charge CPU). Dans notre cas, cette solution est envisageable car la connexion SSH se fait uniquement deux fois par jour. En effet, le but de l'application est de donner une vision du réseau et non pas le superviser. Il ne serait pas envisageable de se connecter en SSH sur l'ensemble des routeurs du backbone avec une fréquence de deux minutes pour récupérer les peering IPv6.

3.2.3.4 Structure de la base de données

Toutes les informations récupérées sur les équipements sont stockées dans la base de données MySql employée aussi pour la métrologie. La structure de la base de données a été adaptée pour cette application. Deux champs ont été ajoutés à la table "interfaces" afin de pouvoir déterminer la disponibilité et la date depuis laquelle les interfaces sont Up ou Down. D'autre part, deux tables ont été créées (peering, AS) pour stocker les informations concernant les peering. La table équipement n'a pas été modifiée.

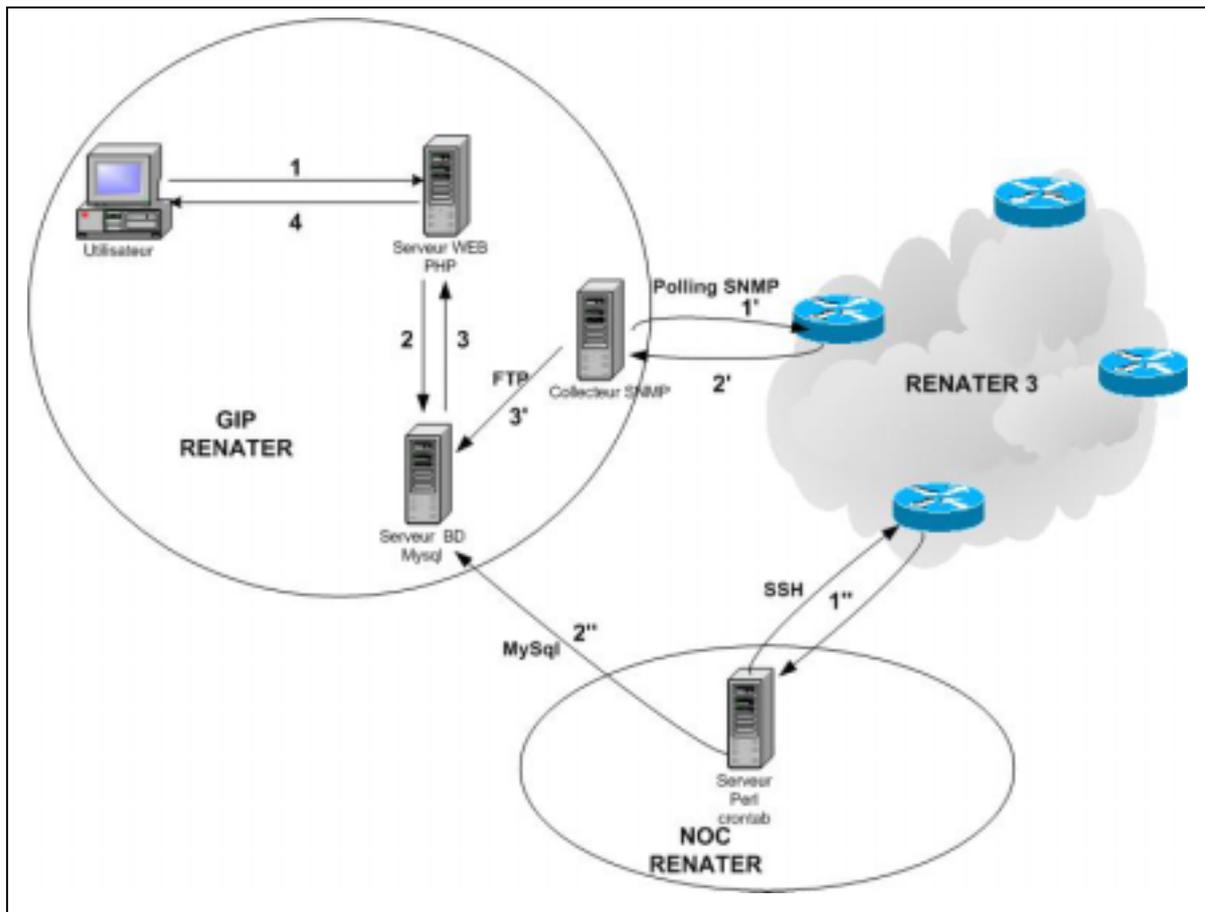
Voici la structure de la base de données avec les modifications réalisées:



La table peering contient les informations principales concernant les peerings (adresse IPv6 de l'extrémité, description, état, le numéro d'AS...). La table AS contient le numéro d'AS et le nom de l'AS.

3.2.3.5 Architecture de l'application

Voici un schéma décrivant l'architecture de l'application:



Consultation WEB:

L'utilisateur accède à travers l'interface web à l'application et effectue son choix (1). Alors le serveur web interroge à travers des pages PHP la base de données MySQL qui renvoie les informations au serveur web (2,3). Le serveur web est une distribution Linux Debian avec un serveur WEB apache 2.0 et la version 4 de PHP. Finalement, la page html est générée puis envoyée à l'utilisateur (4).

Collecte SNMP:

Des scripts écrits en C interrogent régulièrement les équipements du backbone en utilisant le protocole SNMP (1' et 2') pour récupérer entre autres des informations sur les interfaces. Un autre script stocke ces informations dans la base de données MySQL (3').

Collecte SSH:

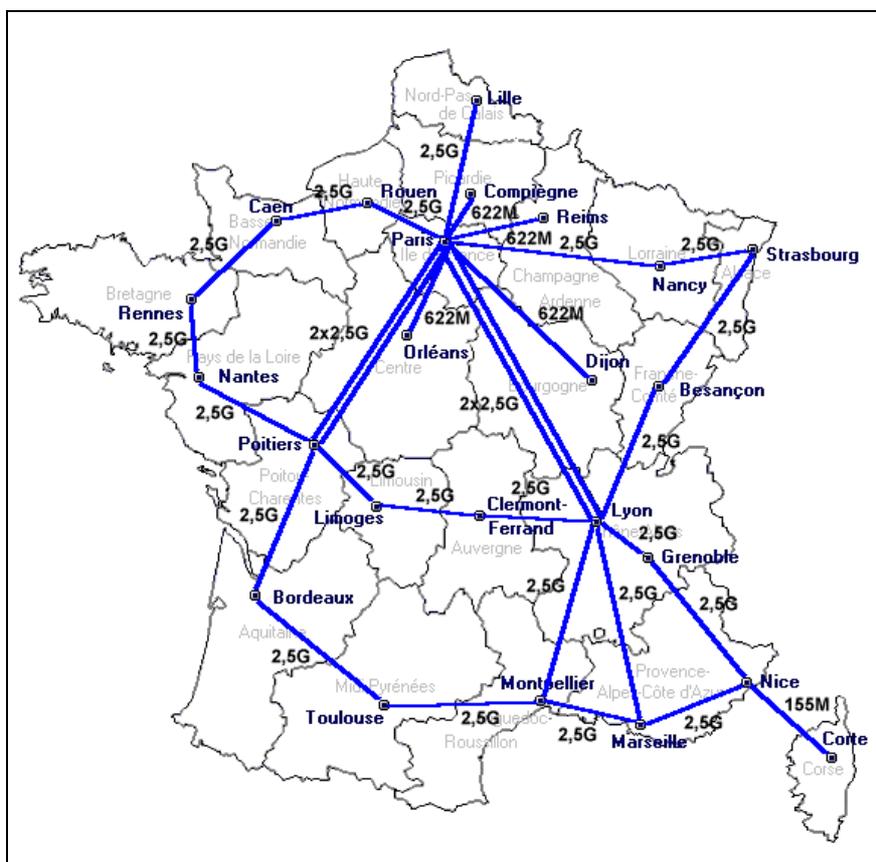
Des scripts écrits en perl permettent de se connecter aux routeurs et récupérer les peerings BGP IPv6 (1"). Ensuite, ceci est stocké dans la base de données (2"). Un module perl permettant d'interagir avec les bases de données ainsi que les dépendances ont été installés. Les modules perl permettant de se connecter en SSH ont été aussi installés sur ce serveur.

Remarque : Le nom de l'AS n'est pas présent parmi les informations récupérées sur le routeur. Afin de compléter la table AS, la base RIPE est consultée à travers la commande "whois". RIPE (Réseaux IP Européens) Network Coordination Centre (NCC) est l'un des quatre organismes dans le monde qui fournit des services d'attribution et enregistrement en accord avec l'Internet mondial.

Quotidiennement, un script en perl interroge la base RIPE pour récupérer les noms d'AS manquants dans la table AS. Afin que les noms d'AS soient mis à jour, une interrogation de la base RIPE est faite une fois par mois pour tous les numéros d'AS présents dans la table AS.

3.2.3.6 Utilisation de l'outil

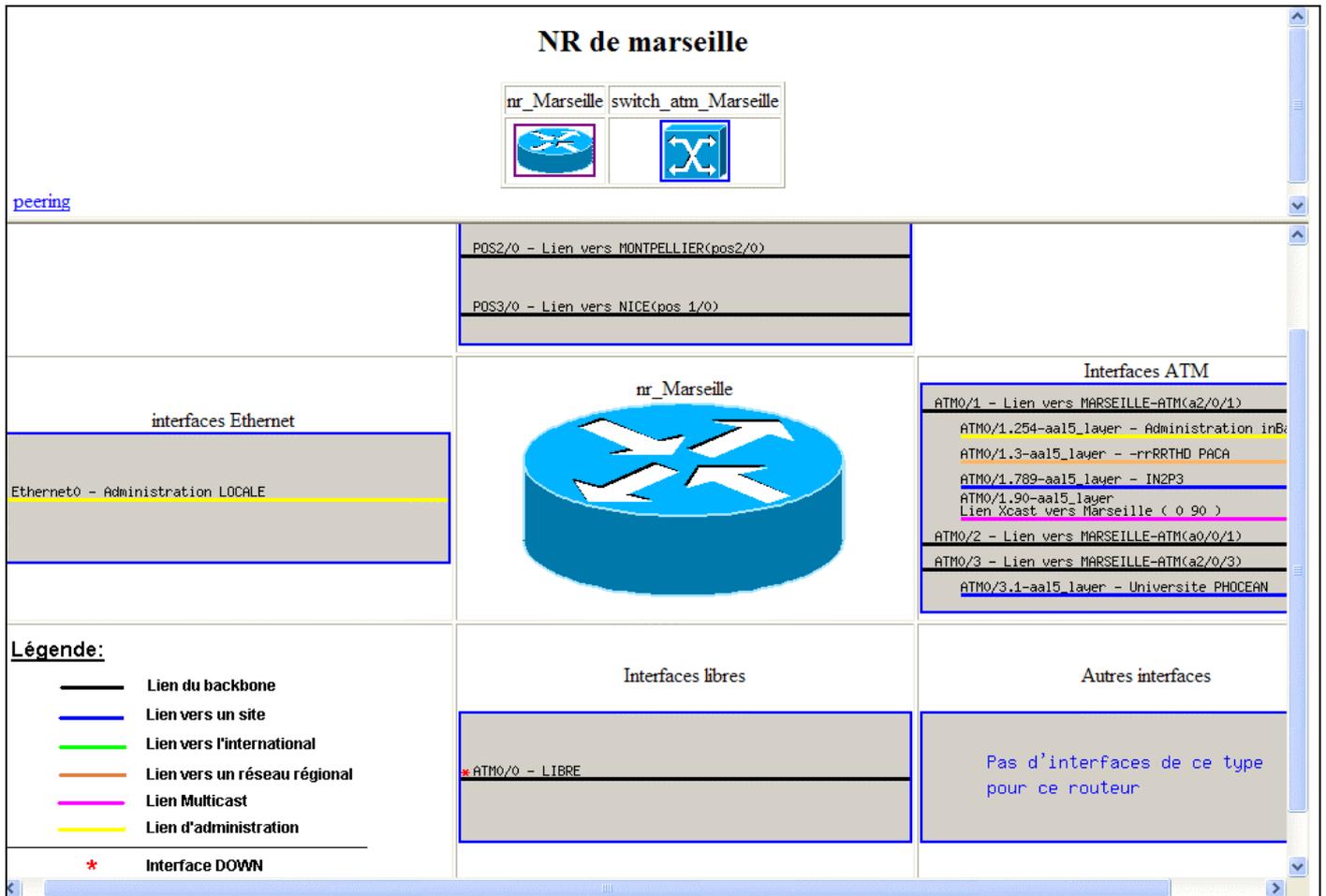
L'utilisateur dispose d'une carte de France où est représenté l'ensemble des NR ainsi que les liens physiques. Cette carte est "cliquable" ce qui permet d'accéder rapidement aux informations sur un NR.



En cliquant sur un NR, l'utilisateur peut alors visualiser soit un schéma avec les interfaces, soit les peerings BGP. L'application permet de choisir parmi les équipements constituant le NR.

Interfaces des équipements:

- Les routeurs: Afin de rendre plus lisible l'ensemble du schéma, l'affichage se fait par type d'interface.



Une image au format PNG (Portable Network Graphic) est générée par type d'interface. Pour ceci, un module php a été installé sur le serveur WEB. Nous pouvons remarquer que les interfaces libres sont immédiatement aperçues et que des couleurs permettent de distinguer le type de lien. Les interfaces qui sont précédées d'une étoile rouge sont down.

- Les switches: Ils ont un seul type d'interface ce qui simplifie la présentation. Uniquement sont différenciées les interfaces libres des interfaces utilisées:



NR de Toulouse

nr_Toulouse switch_atm_Toulouse Toulouse_3640

switch_atm_Toulouse

Interfaces ATM

- ATM0/1 - Lien vers BOSTERON-ATM(a1/1)
- ATM0/2 - Lien vers TOULOUSE(a0/0)
- ATM0/2 - Lien vers TOULOUSE(a0/1)
- ATM0/2 - Lien vers (Tres-1a-951/12)ansteer-atm(a0/1/2)
- ATM0/0 - Lien vers le 3640 Toulouse2
- ATM0/3 - Lien vers TOULOUSE (a0/2)

Interfaces libres

- ATM0/0 - LIBRE
- ATM0/2 - LIBRE
- ATM0/3 - LIBRE
- ATM0/0 - LIBRE
- ATM0/1 - LIBRE
- ATM0/2 - LIBRE
- ATM0/1 - LIBRE
- ATM0/2 - LIBRE

Légende:

- Lien du backbone
- Lien vers un site
- Lien vers l'international
- Lien vers un réseau régional
- Lien Multicast
- Lien d'administration
- ★ interface DOWN

Peering des équipements:

Les peerings sont divisés en deux groupes: les peerings iBGP et eBGP:



NR de PROJETS

PROJETS_GSR-NIO PROJETS_GSR-ENET PROJETS_7200-MICAST PROJETS_M5

Routeur PROJETS_GSR-NIO

Peering BGP

peering iBGP

- Established *** Peer-group de tous les routeurs iBGP *** AS 1717 - FR-RENATER-PROJETS
- Established *** Peer-group de tous les routeurs iBGP *** AS 1717 - FR-RENATER-PROJETS
- Established *** Peer-group de tous les routeurs iBGP *** AS 1717 - FR-RENATER-PROJETS

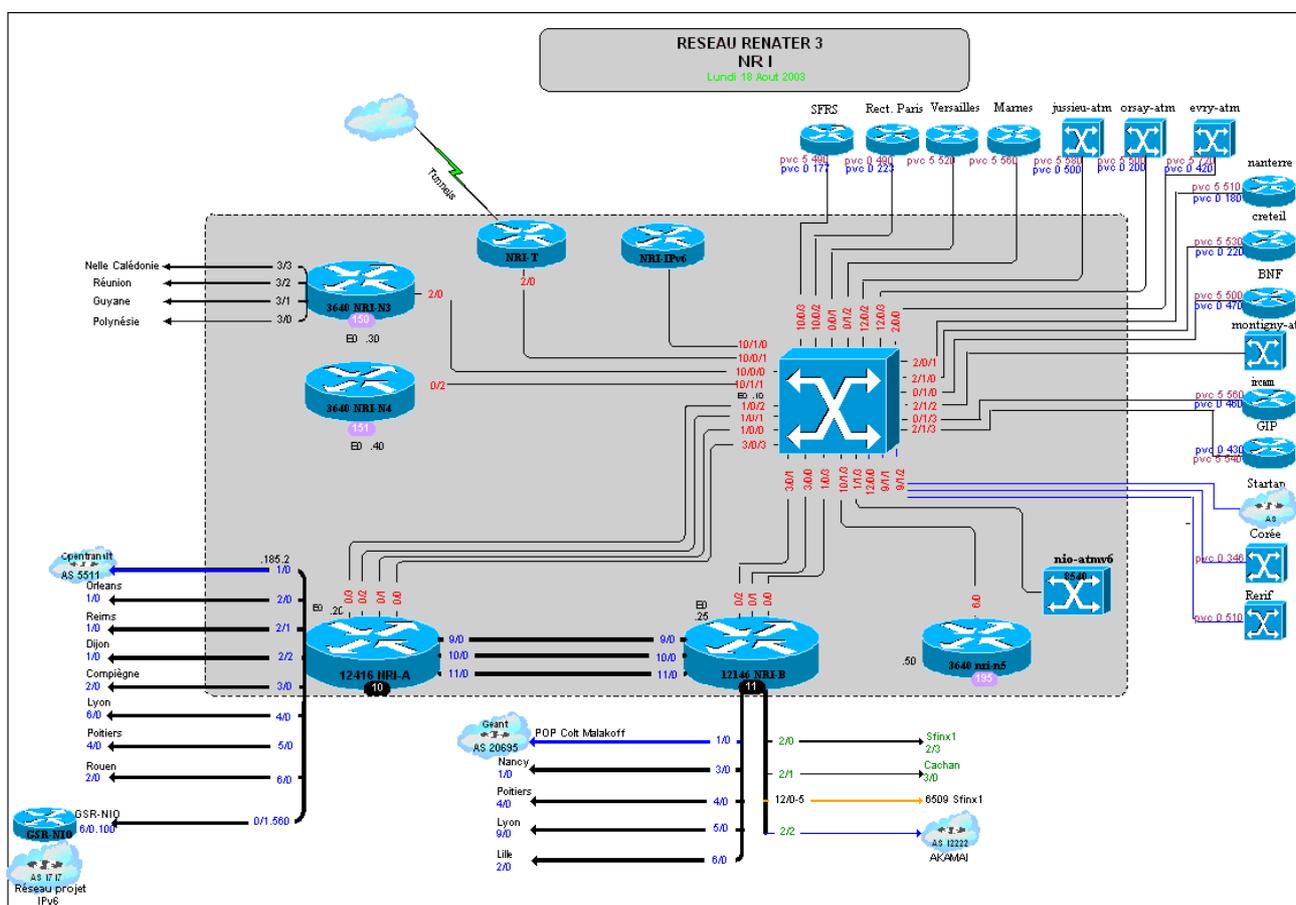
peering eBGP

- Established *** eBGP NRI-A RENATER1 *** AS 2200 - FR-RENATER
- Established *** eBGP RENATER1 IPv4 *** AS 2200 - FR-RENATER
- Active *** eBGP @IRS++ KWAK | shand@renater.fr *** AS 65004 -
- Active *** eBGP @IRS++ PIETRA | shand@renater.fr *** AS 65004 -

Il est possible de voir l'état du peering ainsi qu'un ensemble d'information (adresse IPv6 du voisin, temps depuis lequel le peering est Up ou Down) en cliquant sur le descripteur du peering.

Cas particulier du NRI de Paris (Nœud Renater-3 International):

Nous avons vu que les NR étaient constitués généralement de deux ou trois équipements. Cela rend facile la compréhension de l'architecture lorsqu'un schéma est généré automatiquement. Vu le nombre d'équipements qui constitue le NRI de Paris, un schéma généré serait plus difficile à analyser, surtout si l'utilisateur ne connaît pas exactement l'architecture. Pour cette raison, un schéma a été fait détaillant les liens physiques.



L'utilisateur peut cliquer sur l'un des équipements afin de voir le détail des interfaces ou des peerings comme précédemment pour un NR.

Bien qu'il soit pratique d'avoir des cartes de ce type, elles présentent un grand inconvénient: la mise à jour. En effet, des modifications sont effectuées fréquemment, ce qui oblige de maintenir les cartes à jour afin d'avoir une vision correcte de l'architecture. Ceci demande un temps considérable alors que la génération automatique n'exige pas un suivi.

3.3 Conclusion

La réalisation de ces deux applications m'a permis de travailler dans des environnements techniques différents. J'ai utilisé différents systèmes d'exploitation et divers langages de programmation selon les besoins. Le fait de travailler avec différentes équipes m'a permis de voir que des améliorations pouvaient être apportées aux applications.

4. Evolutions possibles

4.1 Evolutions à court terme

Concernant l'application permettant de faire l'inventaire des interfaces ainsi que celui des peerings, des évolutions peuvent être apportées.

En effet, nous avons vu pour le NRI de Paris que l'entretien des cartes demandait beaucoup de temps. Il a donc été envisagé de généraliser l'outil pour le NRI de Paris. Il est vrai que l'on perd de la visibilité sur l'architecture car il est difficile de voir rapidement les interconnexions entre chaque équipement. Cependant cet outil est destiné à des utilisateurs connaissant globalement l'architecture de Renater. Il est donc préférable de faire un outil générique qui peut évoluer au cours du temps sans avoir à faire de mise à jour importante. Une raison supplémentaire pour généraliser l'outil à l'ensemble des NRI, est la migration prévue sur l'Ile de France. En effet, l'architecture ATM va être remplacée par une architecture reposant sur la technologie GigaEthernet. Avec cet outil, un suivi pourra être fait tout au long de la migration.

En ce qui concerne les peerings BGP, des compléments peuvent être apportés. Lorsque des problèmes de routage sont présents dans le réseau, il est souvent nécessaire de connaître les routes reçues (received routes) ainsi que les routes annoncées (advertised routes) sur un peering. Pour cela, il faudra faire une capture de la table de routage ce qui en IPv6 est concevable (500 routes sur les routeurs du backbone). En IPv4 cela n'aurait pas été envisageable puisque les routeurs du backbone ont environ 120 000 routes. Il est vrai que le réseau IPv4 mondial est beaucoup plus important que le réseau IPv6, mais nous voyons déjà ici l'intérêt de l'agrégation dans l'adressage en IPv6 (tables de routages beaucoup plus petites).

4.2 Evolutions à moyen et long termes

L'absence de MIB permettant de connaître les peering BGP IPv6, empêche de faire une interrogation régulière en SNMP sur les équipements. Nous pouvons envisager, lorsque les constructeurs implémenteront sur ses équipements ces MIB, de superviser les peerings BGP IPv6. Lorsqu'une perte de la session TCP du peering se produit, le client appelle pour signaler le problème. Afin d'être proactif et anticiper la plainte du client, un système d'alarmes pourrait être mis en place permettant d'envoyer des messages au NOC ainsi qu'au SSO si une anomalie se produit.

5. Conclusion

Pendant le déroulement de mon stage, j'ai eu l'opportunité de travailler sur différents aspects avec deux équipes différentes. Le travail réalisé s'est avéré très enrichissant pour mon expérience professionnelle aussi bien en ce qui concerne le domaine technique que l'aspect humain. Le fait de travailler avec deux entités différentes (GIP et NOC Renater) m'a permis d'avoir une vision détaillée de la supervision et de la gestion de réseaux.

En effet, la première partie du stage au NOC RENATER, m'a permis de savoir comment un réseau comme RENATER était opéré par un groupe d'expert.

Pendant la deuxième partie du stage au GIP RENATER, j'ai découvert comment était assurée la maîtrise d'ouvrage du réseau RENATER. Dans les travaux réalisés, j'ai pu apporter mes connaissances théoriques et approfondir certains domaines que je ne connaissais pas encore; j'ai pu découvrir un ensemble d'outils employés dans l'administration de réseaux. J'ai pu aussi me familiariser avec le matériel constructeur qu'utilise RENATER pour constituer son backbone.

Le fait de travailler en équipe et utiliser des applications existantes m'a permis de m'intégrer dans un groupe de travail et de voir en quoi consistait le travail d'ingénieur au sein d'une structure comme RENATER.

6. Glossaire

AS : Autonomous System
ATM : Asynchronous Transfer Mode
BdC : Boucle des Contenus
BGP : Border Gateway Protocol
CoS: Class of Service
GIP : Groupement d'Intérêt Public
ICMP : Internet Control Message Protocol
IETF : Internet Engineering Task Force
MIB : Management Information Base
MRTG : Multi Router Traffic Grapher
NOC : Network Operations Center
NR: Nœud Renater
NRI : Nœud Renater International
PKI : Public Key Infrastructure
RdC : Réseau de Collecte
RIPE : Réseaux IP Européens
SNMP : Simple Network Management Protocol
SSH : Secure Shell
TCP : Transmission Control Protocol
ToS: Type of Service
UDP: User Datagram Protocol

7. Références bibliographiques

Références Internes à CS et au GIP RENATER:

<http://sem2.renater.fr> : Site web technique IPv6 de RENATER

Adresses Web:

<http://www.renater.fr>

<http://tools.6net.net>

<http://www.sunfreeware.com>: Téléchargement des logiciels (UCD-SNMP, ...)

<http://www.perl.com> : Documentation sur le langage perl

<http://www.perl.com/CPAN-local/modules/by-module>: Téléchargement des modules perl

<http://www.cisco.fr> : Documentation sur les MIB IPv6.

<http://www.juniper.net> : Documentation

Documentation:

IPv6, Théorie et Pratique - Gisèle Cizault – O'Reilly Edition 03/2002

RFC :

RFC 1303-1351-1352-1353: SNMP v1 - Description du modèle

RFC 1442 à 1446 : SNMP v2 - Description du modèle

RFC 2271 à 2273 : SNMP v3 – Description du modèle

RFC 2452: MIB IPv6 TCP

RFC 2454: MIB IPv6 UDP

RFC 2465: MIB IPv6

RFC 2466: MIB ICMPv6

RFC 1657: MIB BGP-4

DRAFT :

draft-ietf-ipv6-rfc2011-update-03.txt : draft sur la MIB IP

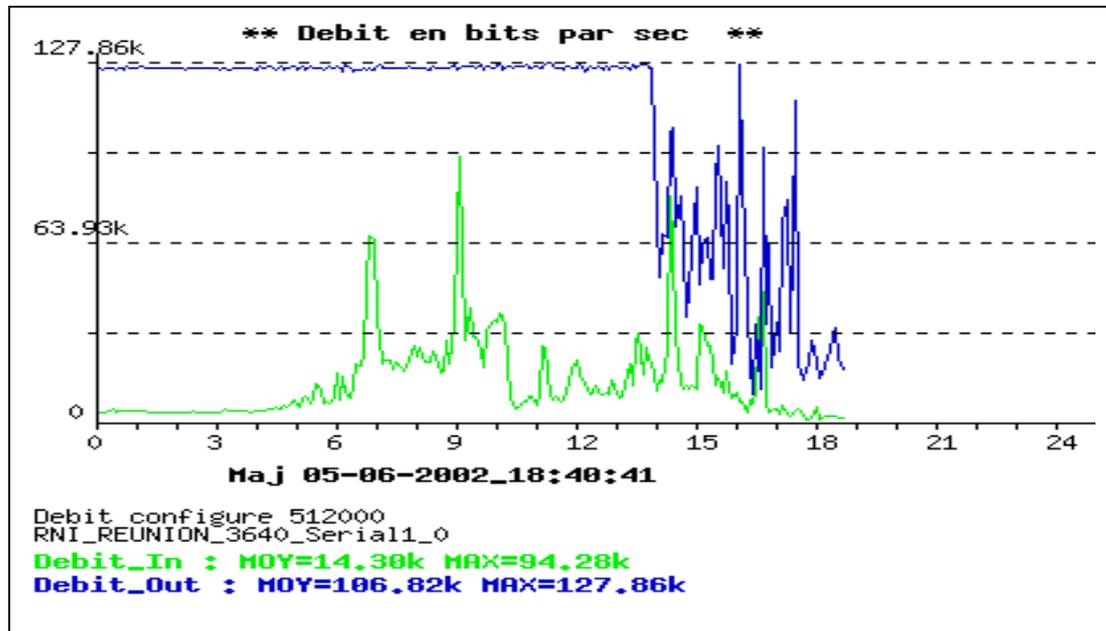
draft-ietf-ipv6-rfc2012-update-03.txt : draft sur la MIB IP TCP

draft-ietf-ipv6-rfc2013-update-03.txt : draft sur la MIB IP UDP

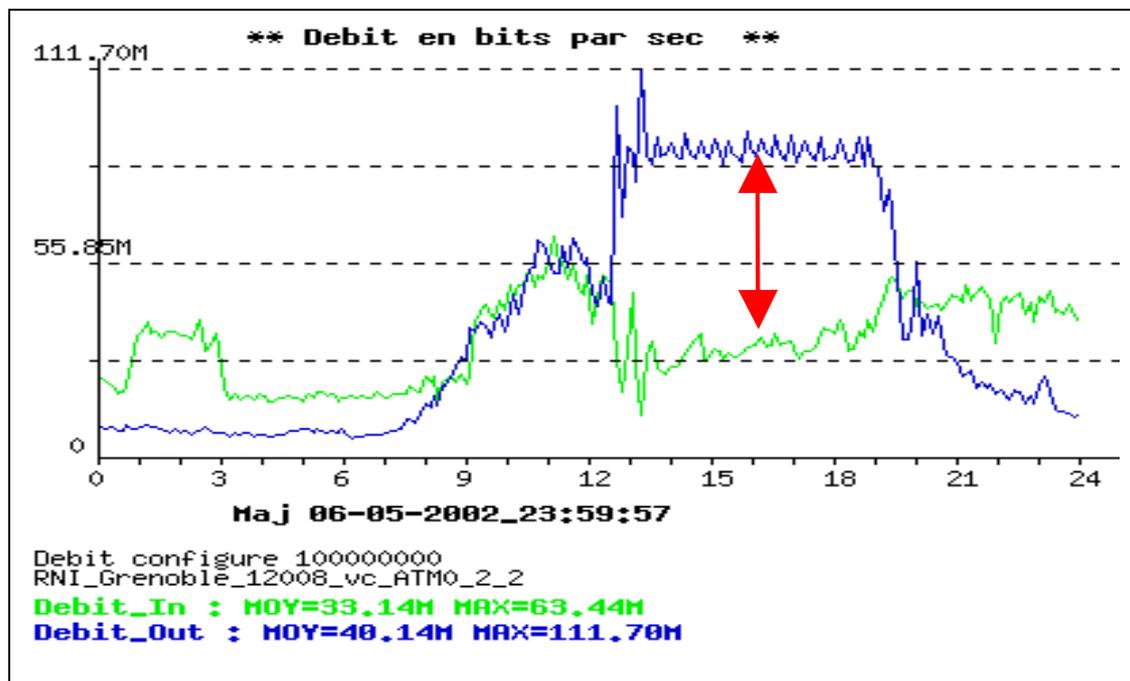
draft-ietf-ipv6-rfc2096-update-04.txt : draft sur la MIB IP Forwarding Table

8. Annexes

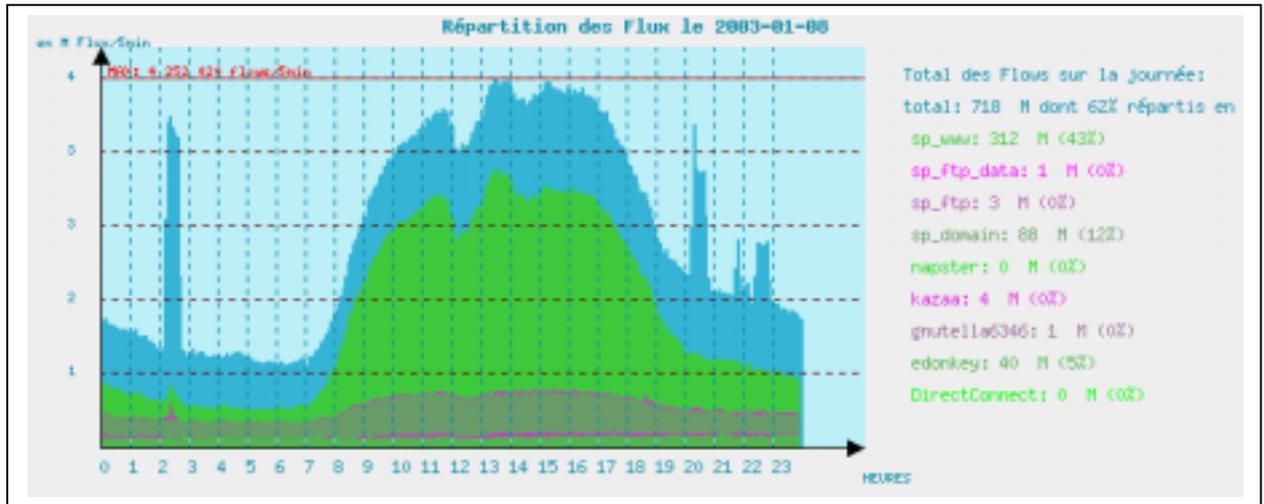
Annexe I: Liaison Saturée



Annexe II: Détection d'un déni de service avec la métrologie



Annexe III: Répartition des flux



Annexe IV: Quelques champs de la MIB CISCO-IETF-IP

```

ciscoIetfIpMIBObjects OBJECT IDENTIFIER ::= { ciscoIetfIpMIB 1 }

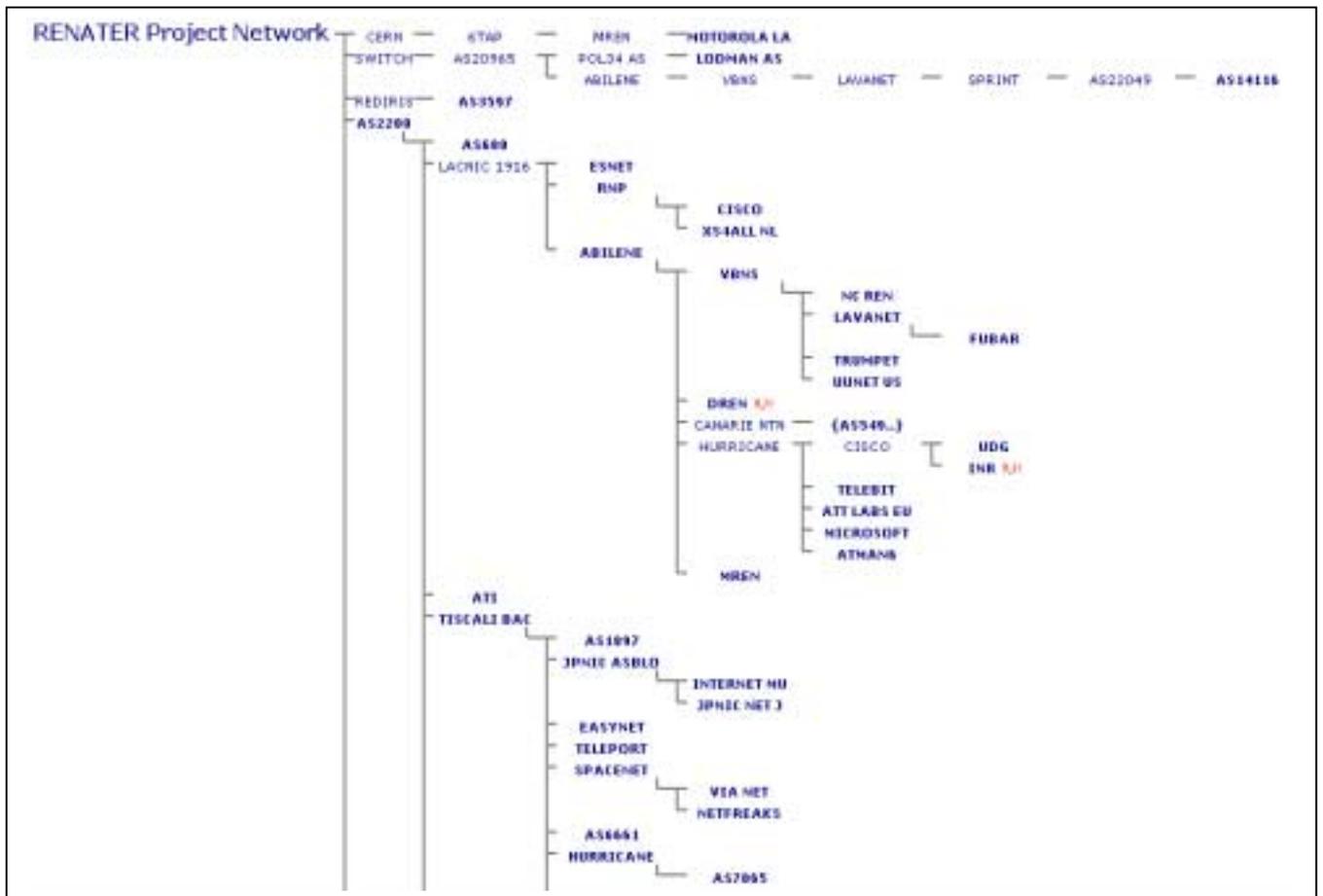
-- the IP general group
cIp      OBJECT IDENTIFIER ::= { ciscoIetfIpMIBObjects 1 }
-- the IPv6 specific group
cIpv6    OBJECT IDENTIFIER ::= { ciscoIetfIpMIBObjects 2 }
-- the ICMP group
cIcmp    OBJECT IDENTIFIER ::= { ciscoIetfIpMIBObjects 3 }

--
-- Textual Conventions
--
Ipv6AddrIfIdentifier
--
-- Object definitions
--
cIpv6Forwarding OBJECT-TYPE
    ::= { cIpv6 1 }
cIpv6DefaultHopLimit OBJECT-TYPE
    ::= { cIpv6 2 }

--
-- IPv6 Interface table
--
cIpv6InterfaceTable OBJECT-TYPE
    ::= { cIpv6 3 }
cIpv6InterfaceEntry OBJECT-TYPE
    ::= { cIpv6InterfaceTable 1 }
cIpv6InterfaceEntry ::= SEQUENCE {
    cIpv6InterfaceIfIndex      InterfaceIndex,
    cIpv6InterfaceEffectiveMtu Unsigned32,
    cIpv6InterfaceReasmMaxSize Unsigned32,
    cIpv6InterfaceIdentifier  Ipv6AddrIfIdentifier,
    cIpv6InterfaceIdentifierLength INTEGER,
    cIpv6InterfacePhysicalAddress PhysAddress
}

cIpv6InterfaceIfIndex OBJECT-TYPE
    ::= { cIpv6InterfaceEntry 1 }
cIpv6InterfaceEffectiveMtu OBJECT-TYPE
    ::= { cIpv6InterfaceEntry 2 }
cIpv6InterfaceReasmMaxSize OBJECT-TYPE
    ::= { cIpv6InterfaceEntry 3 }
cIpv6InterfaceIdentifier OBJECT-TYPE
    ::= { cIpv6InterfaceEntry 4 }
cIpv6InterfaceIdentifierLength OBJECT-TYPE
    ::= { cIpv6InterfaceEntry 5 }
cIpv6InterfacePhysicalAddress OBJECT-TYPE
    ::= { cIpv6InterfaceEntry 6 }
    
```

Annexe V: ASPath-tree sur le réseau projet de RENATER



Annexe VI : Liste des commandes du looking glass :

- show BGP ipv6
- show BGP ipv6 neighbors
- show BGP ipv6 summary
- show BGP ipv6 regexp \$regexp où \$regexp est une expression régulière
- show BGP ipv6 quote_regexp \$regexp
- show BGP ipv6 paths \$regexp
- show ipv6 traffic
- show ipv6 interface
- show ipv6 neighbors
- show ipv6 tunnel
- show ipv6 route
- ping ipv6 \$adresse - ping \$adresse où \$adresse est une adresse IPv6 ou IPv4
- traceroute ipv6 \$adresse - traceroute \$adresse
- show ip bgp sum
- show ip bgp \$adresse - sh bgp ipv6 \$adresse
- show ip bgp dampening dampened-paths
- show ip mroute summary
- show ip mroute active
- show ip mbgp summary
- show ip mbgp \$adresse

Annexe VII: Liste des bibliothèques et modules perl à installer pour SSH

- **Net-SSH-Perl-1.23** : Permet de se connecter à un équipement en SSH.

Dépendances:

- *gmp-4.1.2.tar.gz* :Librairie permettant de faire des calculs arithmétiques de précision
- *Math::GMP* (1.04 ou plus) (pour SSH1) : Utilisé pour le calcul lors du chiffrement
- *String::CRC32* (1.2 ou plus) (pour SSH1) : Permet de faire des checksums (utile lors de l'authentification)
- *Digest::MD5* (pour SSH1): à partir d'un message en entrée, cet algorithme produit une empreinte de 128 bits sur ce message qui permet de vérifier l'intégrité des données.
- *IO::Socket* (pour SSH1): Nécessaire pour établir une communication en IPv4.
- *IO::Socket6* (pour SSH1): Nécessaire pour établir une communication en IPv6.

Les modules suivants permettent d'utiliser les différents algorithmes de chiffrements (ciphers) lors de la connexion SSH :

- *Crypt::DSA* (0.03 ou plus) (pour SSH2)
- *Crypt::DH* (0.01 ou plus) (pour SSH2)
- *Math::Pari* (2.001804 ou plus) (pour SSH2)
- *MIME::Base64* (pour SSH2)
- *Digest::SHA1* (pour SSH2)
- *Digest::HMAC_MD5* (pour SSH2)
- *Digest::HMAC_SHA1* (pour SSH2)
- *Convert::PEM* (0.05 or greater) (pour SSH2)

Annexe VIII: Modifications principales sur la librairie Perl.pm

```
#Utilisation de Socket6
use Socket6;
...
# On vérifie si c'est une adresse IPv4 ou IPv6
## Lookup server's IP address.
if ( $raddr = inet_pton(AF_INET6, $ssh->{host}))
{
    $version = 6;
}
elsif ($raddr = inet_aton( $ssh->{host}))
{
    $version = 4;
}
else { die "unknown remote host: $ssh->{host}\n"; }
...
# Création de la socket en v4 ou v6
my $sock = $ssh->_create_socket;

if ($version == 6)
{
    socket($sock, AF_INET6, SOCK_STREAM, $proto) ||
        croak "Net::SSH: Can't create socket v6: $!";
}
elsif ($version == 4)
{
    socket($sock, AF_INET, SOCK_STREAM, $proto) ||
        croak "Net::SSH: Can't create socket v4: $!";
}

# Connexion en IPv6
if ($version == 6)
{
    # Connexion en IPv6
    connect($sock, sockaddr_in6($rport, $raddr))
        or die "Can't connect to $ssh->{host}, port $rport: $!";
}
elsif ($version == 4)
{
    # Connexion en IPv4
    connect($sock, sockaddr_in($rport, $raddr))
        or die "Can't connect to $ssh->{host}, port $rport: $!";
}
}
```

Annexe IX: Configuration de Tacacs+ (serveur et équipements)

Configuration du routeur Cisco :

Voici la configuration qui est présente sur l'ensemble des routeurs de RENATER-3

```
enable secret local_enable_password
aaa new-model
tacacs-server host XX.XX.XX.XX #adresse IP du serveur tacacs
aaa authentication login default tacacs+
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+
```

Configuration du compte Looking-glass :

Extrait du fichier /etc/tacacs.conf

```
key = "la_cle"

accounting file = /var/log/tac.log

default authorization = permit

user=normal_user{
    login = des N75frezREER/LI
}

user=looking_glass
{
    login = cleartext mot_de_passe_en_clair
    cmd = show
    {
        permit "bgp ipv6 neigh"
        permit "ipv6 traffic"
        ...
        ...
    }
}
```

Annexe X: Interface du Looking Glass IPv6

RENATER Looking Glass

<p>BGP tables</p> <p><input checked="" type="radio"/> show bgp IPv6 <input type="text" value="routing_table"/></p> <ul style="list-style-type: none"> <input type="text" value="routing_table"/> <input type="text" value="summary"/> <input type="text" value="neighbors"/> 	<p>BGP with regular expression</p> <p><input type="radio"/> show bgp IPv6 <input type="text" value="regex"/></p> <p>regular expression : <input type="text"/></p> <p><small>Don't use the character '\$'</small></p>
<ul style="list-style-type: none"> <input type="radio"/> IPv6 traffic <input type="radio"/> IPv6 interface <input type="radio"/> IPv6 tunnels <input type="radio"/> IPv6 neighbors <input type="radio"/> IPv6 route 	<ul style="list-style-type: none"> <input type="radio"/> Ping XXXX <input type="radio"/> Traceroute XXXX <input type="radio"/> show ip bgp XXXX <input type="radio"/> show ip bgp summary <input type="radio"/> show ip bgp dampening dampened-paths <input type="radio"/> show ip mroute summary <input type="radio"/> show ip mroute active <input type="radio"/> show ip mbgp summary <input type="radio"/> show ip mbgp XXXX <p><input type="radio"/> IPv4 address <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></p> <p><input type="radio"/> IPv6 address <input type="text"/></p> <p><input type="radio"/> name address IPv4 <input type="text"/></p> <p><input type="radio"/> name address IPv6 <input type="text"/></p>
<p>Router: <input type="text" value="Toulouse"/></p> <p><input type="button" value="submit"/> <input type="button" value="Reset"/></p>	

Annexe XI: fichier de configuration pour le looking glass

Ceci est un extrait du fichier contenant la liste des équipements du backbone et leurs caractéristiques : Adresse, description, login et mot de passe pour Tacacs

```
#
# lg.cfg Configuration file for the looking glass.
#

package config;

#
# Common variables.
#
$Company = 'RENATER';
$Logo = 'Renater.gif';
$Email = 'noc-ipv6@cssi.renater.fr';

#
# List of routers (detailed info below). This is the order they
# will appear in the pull-down menu.
#
@Routers = ( 'besancon','compiegne',...,'toulouse' );

#
# Per-cisco variables.
#

$cfg{besancon} = {
    Host => '2001:660:X:X::X',
    Login => '***',
    Pass => '***',
    IXPoint => 'Routeur C12000 ',
};

$cfg{compiegne} = {
    Host => '193.X.X.X',
    Login => '***',
    Pass => '***',
    IXPoint => 'Routeur C12000 ',
};
...
...
$cfg{toulouse} = {
    Host => '2001:660:X:X::X',
    Login => '***',
    Pass => '***',
    IXPoint => 'Routeur C12000 ',
};
```