La métrologie au GIP RENATER

François-Xavier Andreu
GIP RENATER
151, bd de l'hôpital
75013 Paris
andreu@renater.fr

Résumé

Aujourd'hui, l'utilité de la métrologie n'est plus à prouver : depuis deux ans les solutions existantes sur RENATER ont démontré leur efficacité. C'est une aide à la supervision du réseau, à la sécurité, au dimensionnement... Après un rappel indispensable des caractéristiques du réseau, cet article fait un point sur l'état du système de métrologie au GIP RENATER. Les solutions opérationnelles sont présentées ainsi que leurs évolutions et limites, limites que le GIP RENATER souhaite repousser en étudiant de nouveaux systèmes de mesures (mesures actives). Cette approche implique une redéfinition des besoins. Certains de ces besoins sont contraignants et s'appuient sur des technologies de plus en plus complexes. L'utilisateur final (site RENATER) est lui aussi intégré dans la spécification d'un tel système afin d'obtenir les mesures les plus représentatives sur l'état du réseau. Les solutions étudiées sont présentées dans la dernière partie.

Mots clefs

Métrologie, mesures de bout en bout, SNMP, NetFlow

1 Introduction

La métrologie est utilisée pour améliorer la supervision du réseau, fournir une aide au diagnostic et au dimensionnement du réseau (conception d'architecture). La sécurité est également partie prenante avec la détection des attaques. Les réseaux étant en constante évolution, tant au niveau matériel qu'au niveau des services, les solutions de métrologie doivent être évolutives et sont donc généralement remaniées. C'est le cas sur le réseau RENATER avec la maintenance de l'existant. Mais l'apparition de nouveaux services (par exemple la mise en place d'IPv6 ou des classes de services) nécessite d'effectuer d'autres mesures qui ne s'intègrent pas forcément dans les systèmes actuellement exploités, d'où la recherche de nouvelles solutions.
Après une brève description du réseau RENATER, cet article présente les solutions opérationnelles mises en place au GIP RENATER (classées dans la catégorie des mesures passives : capture du trafic). La dernière partie expose l'étude de la prochaine solution, complémentaire à la précédente, et s'appuyant sur des mesures actives (étude d'un trafic généré).

2 Le backbone RENATER

Avant d'expliquer les techniques de mesures déployées ou en passe de l'être, la connaissance de ce que l'on va mesurer est primordiale. Il faut donc présenter le réseau RENATER-3 : il est composé d'une partie métropolitaine (appelée dans la suite du document "backbone") avec les nœuds RENATER (NR) qui permettent l'interconnexion avec les réseaux de collecte. Les DOM-TOM sont également reliés et les réseaux nationaux européens pour l'éducation et la recherche sont accessibles via GEANT. La connectivité avec l'Internet de commodité est réalisée avec le point d'échange SFINX et via un double accès vers OpenTransit.
Des équipements et technologies hétérogènes cohabitent afin de constituer ce réseau. Son architecture matérielle est composée de routeurs et commutateurs CISCO (C124xx, C12xxx, C7500, C7200, C3640, C3550, C8540). Le cœur du réseau s'appuie sur une technologie DWDM sur laquelle repose une couche POS[1] puis la couche IP. La plupart des liens sont des liens à 2,5Gbit/s à l'exception de certaines liaisons pendulaires en 622Mbits/s (SDH). Le raccordement des réseaux de collecte se fait via des interfaces Giga-Ethernet (avec encore certains raccordements en ATM, reliquats de RENATER-2). Les protocoles de routage sont IS-IS[2] pour l'IGP et BGP pour l'EGP (interconnexions avec les éléments extérieurs). Les services opérationnels sont :

[1] POS : Packet Over SDH (Synchronous Digital Hierarchy)
[2] IS-IS: Intermediate System to Intermediate System

- IPv4 Unicast
- IPv4 Multicast
- IPv6 Unicast
- MPLS[1] VPN[2] (niveau 2 et 3)

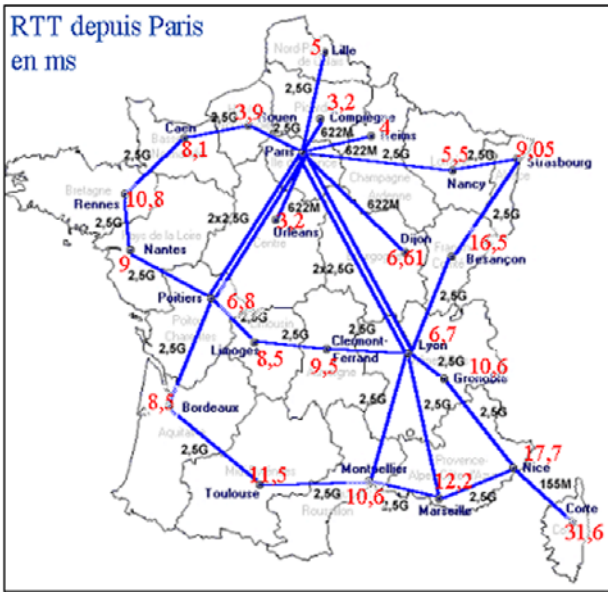

Figure 1 - *RTT dans RENATER 3 depuis Paris*

Cette diversité d'équipements et de services a de fortes implications sur les méthodes de mesures. Les temps de transit d'un paquet IP sont aujourd'hui très faibles d'un bout à l'autre du réseau. La figure 1 donne un ordre de grandeur des temps "aller-retour" entre un site parisien et les différents NR. Bien que ce test ait été effectué avec le protocole ICMP, qui n'est pas forcément traité de manière prioritaire au niveau des équipements, on peut déjà remarquer que les temps "aller-retour" sont très faibles, par déduction les délais unidirectionnels le sont également (il peut parfois y avoir une légère asymétrie). Cette caractéristique du réseau (temps de transit très faibles) a une forte influence sur la finesse des mesures : une précision de cinq pourcents sur un temps de deux secondes nécessite une incertitude de la mesure d'au plus cent millisecondes. Lorsque l'observation consiste à surveiller les fluctuations des temps de transit l'incertitude de l'outil doit être encore inférieure à cela. En plus des équipements, la diversité des protocoles (IP, MPLS) et bientôt les classes de services contribuent à la complexité d'un système de métrologie complet.

3 Les besoins élémentaires

Il y a déjà plusieurs années le GIP RENATER a mis en place une politique de mesures sur le backbone afin de répondre aux principaux besoins de la gestion d'un réseau : disponibilité des liens, débits, dimensionnement, sécurité. Bien entendu l'évolution de ces technologies suit celle du réseau tant au niveau du matériel qu'au niveau des services.
Les techniques choisies sont classées dans la catégorie de la métrologie passive : celle-ci consiste à observer le trafic sans modifier ou altérer le réseau. Pour cela deux fonctionnalités présentes dans les routeurs sont utilisées : les MIB (Management Information Base) et le NetFlow (développé chez CISCO mais aujourd'hui présent chez les autres constructeurs).

3.1 Les MIB et SNMP

Les équipements réseaux possèdent des MIB qu'ils mettent à jour toutes les dix secondes environ. La manipulation de ces données est réalisée par le protocole SNMP (Simple Network Management Protocol). L'équipement est sollicité pour une interrogation ("get") ou mise à jour ("set") d'une variable. Cette technique permet d'observer les équipements mais aussi de les configurer (dans une certaine mesure).

[1] MPLS : Multi Protocol Label Switching
[2] VPN : Virtual Private Network

Il existe de nombreuses MIB, certaines sont standardisées, d'autres propres aux constructeurs. Elles représentent l'état du système, des interfaces, mais il existe aussi de nombreuses variables sur le comportement des protocoles des couches réseau et transport.
Cette technique est principalement utilisée aujourd'hui au GIP dans un but de supervision, d'aide au diagnostic et d'aide au dimensionnement. Les principaux indicateurs observés sont :

- l'état (up/down) des interfaces (ce qui permet de dresser une carte de disponibilité du réseau)
- le taux de charge de la CPU et l'utilisation de la mémoire
- le nombre d'octets et de paquets par interface (physique et logique)
- les pertes de paquets et les erreurs

Les outils permettant d'exploiter les MIB sont nombreux, les plus connus étant MRTG[1] et Cricket pour les solutions libres et HP Openview ou Tivoli pour les solutions commerciales. Le GIP a décidé de développer son propre outil de mesures afin que celui-ci s'adapte parfaitement au réseau et puisse être maintenu facilement lors des évolutions majeures de l'infrastructure, et il se rapproche du logiciel RTG[2] pour les techniques employées.
L'outil est écrit en C pour des raisons de performances et s'appuie sur la librairie Net-SNMP[3]. Il doit interroger plus de 80 équipements (routeurs, commutateurs) dans un temps assez court, d'où le choix du langage. L'intervalle de temps entre deux interrogations peut être très faible, de l'ordre de quelques dizaines de secondes (d'où la possibilité d'effectuer des campagnes de mesures plus précises). L'interrogation de l'ensemble des équipements est réalisée en 10 secondes environ grâce à une gestion asynchrone des communications, chaque équipement étant interrogé en même temps. Par contre, pour des raisons de charge et de simplicité, les interrogations sont séquentielles pour un même équipement. Le logiciel ne se base pas sur les indices des interfaces, ce qui facilite la gestion des problèmes liés à des reconfiguration des équipements. Il découvre automatiquement les nouvelles interfaces : celles-ci ne sont donc pas à gérer à la main ou par un script dans un fichier de configuration (cette caractéristique est appréciable dès que le réseau est de taille significative), et il suffit de définir un équipement par son nom, son adresse IP, sa communauté SNMP, l'intervalle de "polling" et son groupe. Ce dernier paramètre permet de relever les indicateurs appropriés pour chaque équipement suivant les types définis par l'utilisateur. Cette définition peut se faire en fonction de l'équipement (routeurs C12xxx, C7200, C3640, commutateurs...), ou en fonction d'autres règles puisqu'un groupe est défini par une liste d'OID[4]. Le nombre minimum de requêtes par équipement est de 1+(4*nombres d'interfaces) soit environ 4000 requêtes (paquets UDP), mais l'impact est toutefois faible sur la charge des équipements. Les données collectées sont ensuite enregistrées dans une base de données MySQL : cela permet d'effectuer des requêtes complexes lors d'études sur plusieurs paramètres. Chaque nuit les données sont agrégées dans une table différente afin d'obtenir des statistiques sur des échelles de temps variées. La visibilité par tranche de 24h est possible jusqu'aux quatre derniers jours (cela représente environ 100Mo de données). Les statistiques sont disponibles en interne au GIP via une interface WEB. La communication avec la base de données est gérée par des scripts PHP (API MySQL et librairie graphique GD).

Un tel système de mesure a bien sûr ses limites. Les courbes sont généralement moyennées sur 5 minutes (même si la collecte a une fréquence plus élevée), d'où un effet de lissage : les pics de trafic ("bursts" sur quelques dizaines de secondes) sont alors très atténués. D'un autre côté, la visualisation d'un débit moyenné sur une minute fait apparaître une courbe en dents de scie qui n'est plus lisible.
La vision du trafic est aujourd'hui exclusivement IP, or le trafic sur RENATER se décompose en IPv4 et IPv6, et la MIB permettant de comptabiliser le trafic exclusivement IPv6 n'est toujours pas standardisée, il est néanmoins possible de connaître la part des flux IPv6 au niveau des interfaces physiques. Néanmoins les constructeurs mettent généralement à disposition une MIB (propriétaire) pour chaque nouvelle technologie, comme par exemple les MIB pour MPLS, IPv6 et les classes de services.
Même si les MIB permettent une bonne vision de la couche réseau, il y a toutefois une lacune pour une visibilité au niveau des couches supérieures. Il est donc nécessaire d'utiliser en parallèle d'autres techniques.

3.2 Netflow

Le NetFlow est une technologie qui permet d'observer le réseau au niveau des flux ("level-flow"). Conçu à l'origine pour accélérer le routage dans les équipements, il est aujourd'hui toujours présent mais est utilisé dans un but de mesure. Le

[1] Multi Router Traffic Grapher : http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
[2] Real Traffic Grabber : http://www.caida.org/tools/measurement/rtg/
[3] Net-SNMP : http://net-snmp.sourceforge.net/
[4] OID : Object Identifier Descriptor

"capteur" est situé dans l'équipement (routeur, commutateur). La capture est effectuée sur les flux entrant dans l'équipement ("incoming traffic" ou "ingress"). Les informations collectées pour un flux sont les suivantes :

- adresses IP source et destination
- port (couche 4) source et destination
- protocole
- type de service
- index des interfaces logiques d'entrée et de sortie
- nombre de paquets et d'octets
- date de début et de fin
- AS source et destination
- masque des adresses IP

Cette liste permet déjà d'entrevoir les possibilités de traitement, les agrégations des flux sont possibles pour un routeur, une interface, un bloc d'adresse, une adresse IP, un (ensemble de) port(s) (Figure 2), d'AS, etc.

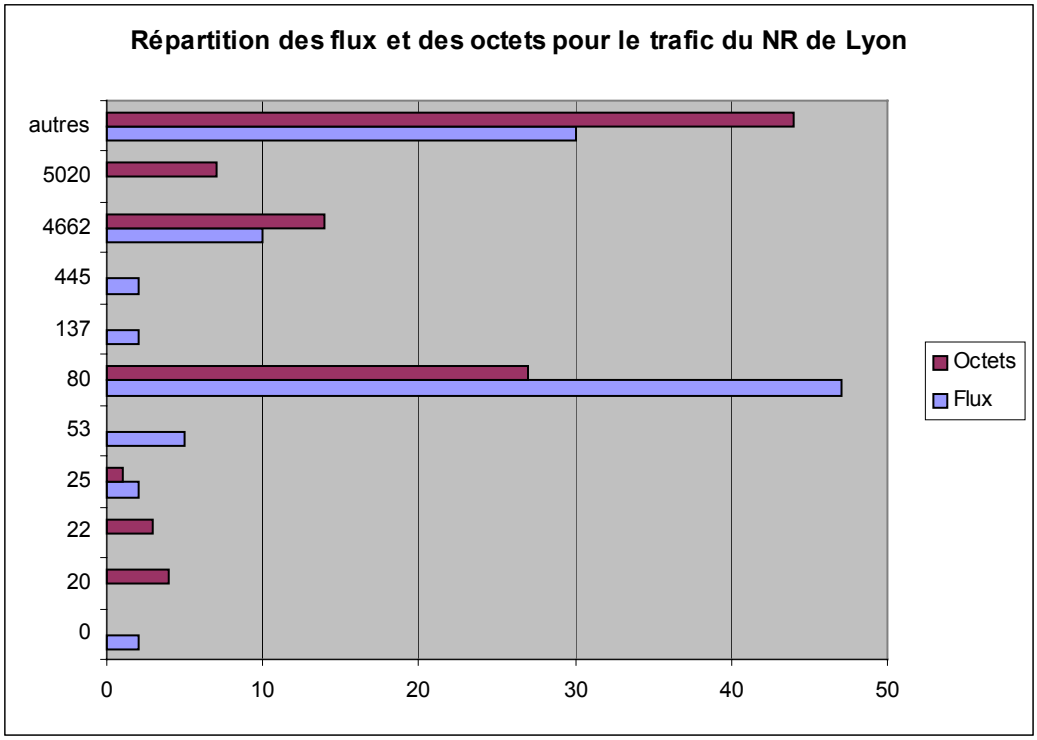

Figure 2 – *Répartition suivant les ports*

Le NetFlow est utilisé au GIP pour :

- mesurer les débits en flux et octets des blocs d'adresses (donc le débit des sites)
- superviser le trafic correspondant à l'adressage du backbone
- contrôler le respect de la charte RENATER (cela n'est pas possible de façon directe)
- déterminer les attaques de type deni de service (DoS)

Nous obtenons donc pour chacun des blocs d'adresses alloués aux sites son débit en nombres de flux par tranches de 5 minutes (Figure 3), son débit en octets par seconde (Figure 4) et en paquets par secondes.

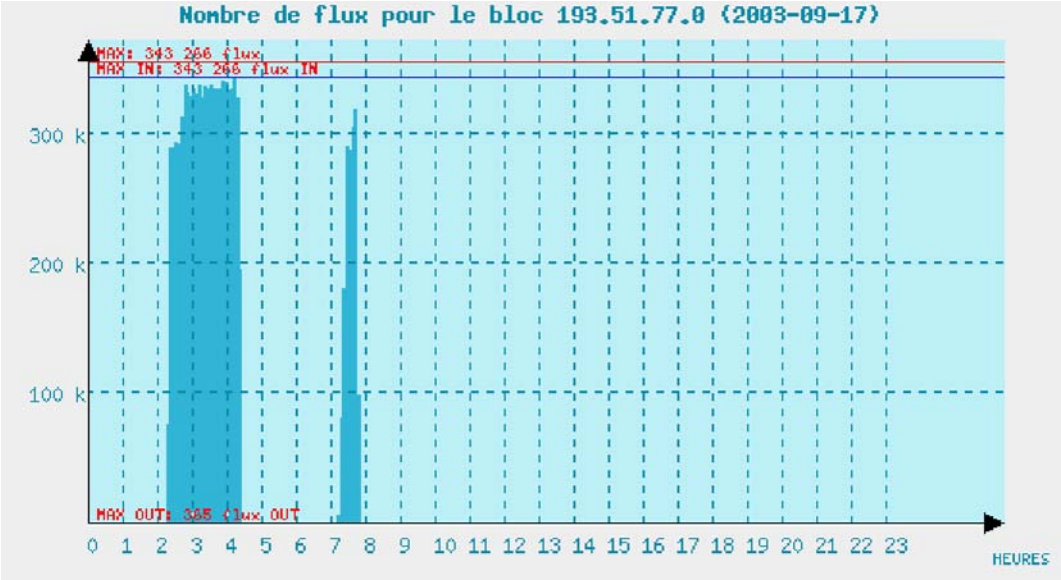

Figure 3 – *Débits d'un bloc d'adresses en Flux/5min*

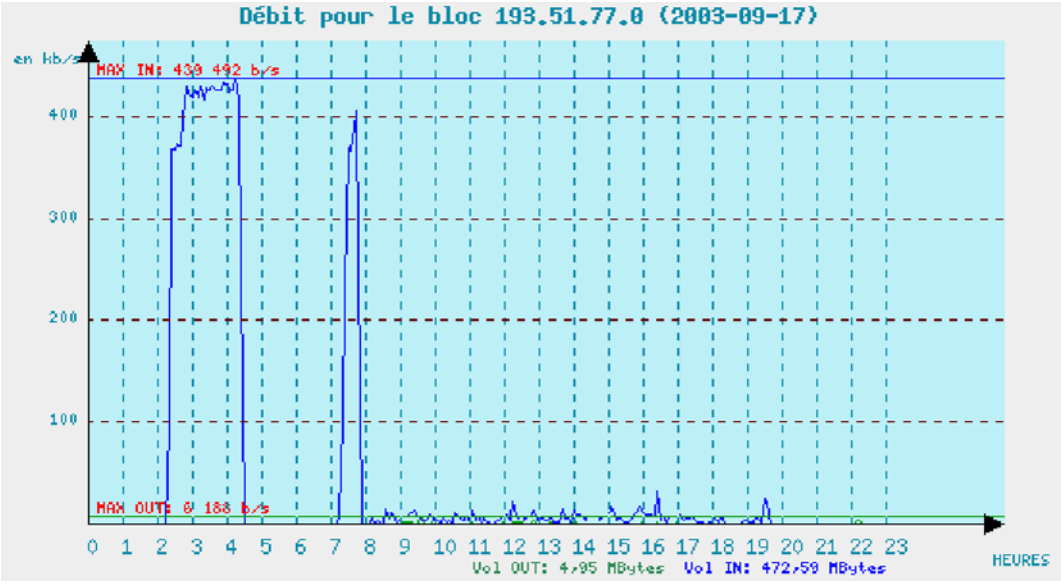

Figure 4 – *Débits d'un bloc d'adresses en kb/s*

Il est possible de générer des alarmes lorsque des seuils sont dépassés : cela permet de signaler certaines attaques de type DoS. L'attaque, visible sur les deux figures précédentes, se remarque également sur le nombre de flux observés globalement sur le backbone (Figure 5).

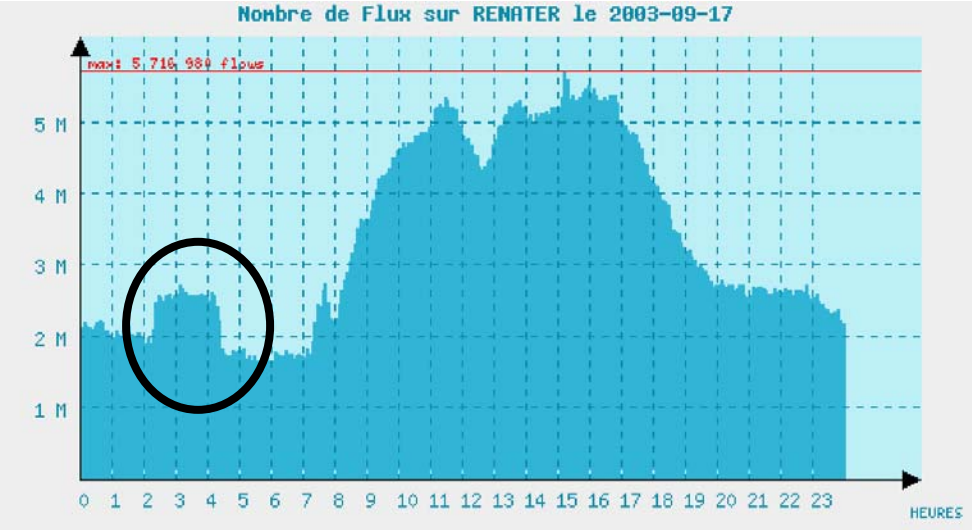

Figure 5 – *Débit RENATER en millions de flux/5min*

Le contrôle du respect de la charte RENATER est effectué en définissant des signatures : certains flux correspondant à des transferts de fichiers "warez" peuvent être caractérisés par leur taille, et une partie des flux Peer-to-Peer le sont par les ports. Il reste néanmoins une part d'interprétation réalisée par le CERT-RENATER qui reçoit les informations relatives à ce type de trafic chaque jour. La mise en évidence, grâce à ces mesures, de machines dont la plupart étaient piratées, a permis de faire baisser le trafic "illégal" de moitié depuis la mise en place de la reconnaissance des flux par l'analyse des signatures en juin 2002.
Les flux comportant une adresse appartenant aux équipements du backbone sont eux aussi analysés afin de détecter les éventuelles attaques dirigées sur l'infrastructure. Un seuil est défini d'après le nombre de flux moyen en provenance et en direction des équipements (adresses des routeurs, des interfaces et des interconnexions).
Les problèmes de routage - comme une boucle entre deux routeurs voisins - sont facilement détectables. Ce phénomène, souvent dû à une mauvaise configuration des routeurs, est peu fréquent mais peut engendrer de grosses perturbations sur le lien (un flot continu de quelques kb/s se transforme tout simplement en un trafic de plusieurs centaines de Mbits entre les deux routeurs).

Le NetFlow est configuré sur tous les équipements du backbone RENATER qui le supportent, soit sur 47 routeurs. Ces derniers transmettent les informations sur un unique collecteur qui traite en temps réel les informations reçues : cela représente un trafic de 8Mb/s au niveau du collecteur. Avant d'être agrégés au niveau d'une base de données MySQL, les flux sont contrôlés suivant des règles persistantes et/ou ponctuelles afin de générer des remontées d'alarmes (visualisables ensuite au niveau d'un serveur Web). La figure 6 représente l'architecture globale de l'outil.

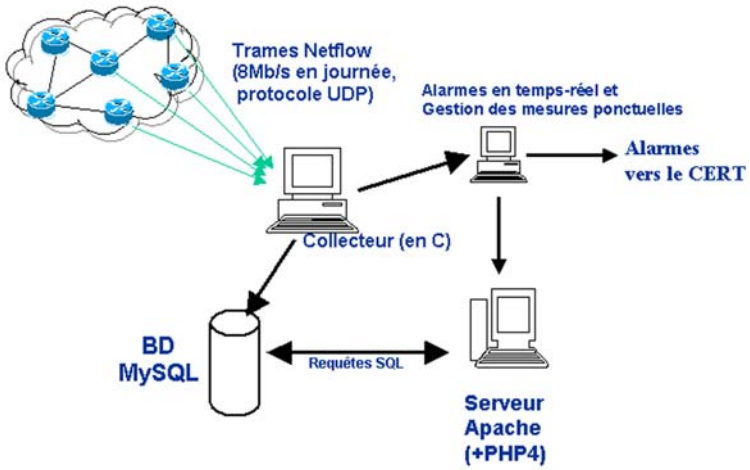

Figure 6 – *Traitement du Netflow : architecture matérielle*

Depuis sa mise en place dans le backbone, l'évolution majeure de la technologie NetFlow fut le passage du mode "full-flow" à un mode "échantillonné". À la vue des débits croissants des interfaces, les constructeurs ont choisi d'opter pour une capture par échantillonnage afin de ne pas pénaliser les équipements. Au lieu de reconstruire les flux en fonction de tous les paquets qui transitent sur le lien, le cache NetFlow est rempli avec une partie des paquets (1 sur X) : la valeur actuellement utilisée pour X sur les équipements du backbone est 10, les flux sont donc construits à partir d'un paquet sur dix.
Une alternative à ce "problème" est l'utilisation du NetFlow agrégé : cette technique consiste à observer le réseau selon les AS, les sous-réseaux, les ports. Le travail d'agrégation est alors effectué par le routeur, mais cela signifie la perte des informations au niveau d'un flux : les clés essentielles pour la sécurité, tels que les adresses sources/destinations ou les ports ne sont plus observables pour un flux, et le traitement des problèmes de sécurité n'est alors plus possible tel qu'il avait été mis en place. Le choix de l'agrégation n'a donc pas été retenu sur RENATER.
Il faut également noter que les différentes méthodes d'échantillonnage ne sont pas toutes aussi précises les unes que les autres surtout lorsque X est grand ("Uniform Sampling" contre "Smart Sampling" [1]). CISCO travaille aujourd'hui sur des modes d'échantillonnage non déterministes : méthodes aléatoires ou basées sur le temps [2].
En pratique, l'observation sur RENATER avec la valeur 10 paramétrée montre qu'environ la moitié des flux n'est pas capturée : il s'agit principalement de petits flux composés de peu de paquets. On pourrait donc penser que la détection des attaques DoS ne fonctionne plus, mais ce n'est pas le cas, car pendant une attaque le nombre de paquets est tellement important que ceux qui sont capturés suffisent à déclencher les alarmes. Le calcul du débit d'un site n'est quant à lui pas gêné par l'échantillonnage : il suffit de multiplier la moyenne par 10 dans notre cas pour connaître la valeur réelle. Mais si l'échantillonnage augmente (X=100 au lieu de 10 par exemple) les valeurs obtenues peuvent être mal interprétées lorsqu'elles ne sont pas moyennées sur une période conséquente. Lors du passage au "Sampled" NetFlow sur RENATER, les valeurs obtenues par extrapolation (valeur observée*X) ont été comparées aux valeurs relevées par SNMP pour vérification, et le résultat a été satisfaisant.
La figure 7 est l'observation du débit en nombre de flux pour un bloc d'adresse le jour où l'interface renvoyant les flux exportés du site est passée du "Full Netflow" au "Sampled Netflow" (à 13h) : on observe nettement une diminution du nombre de flux capturé.

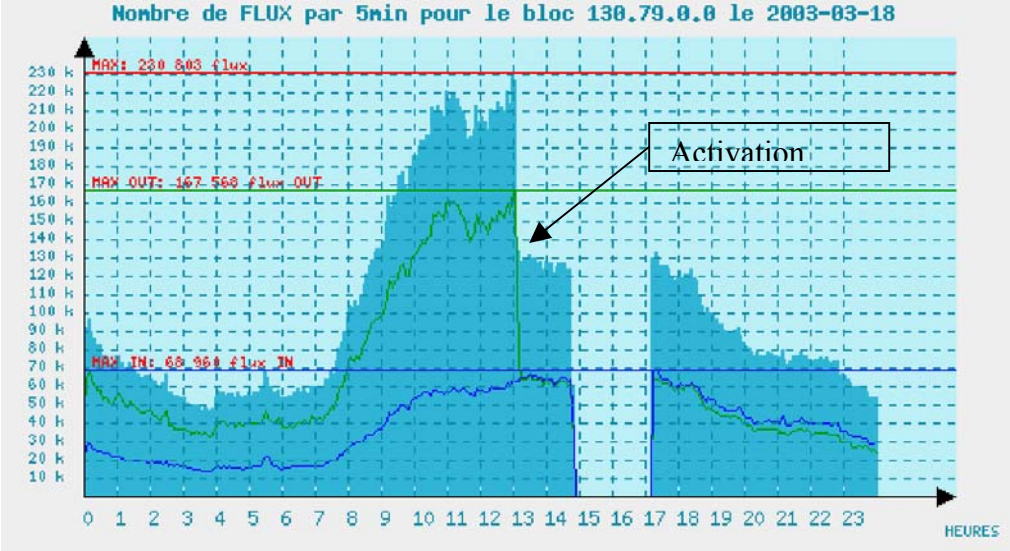

Figure 7 – *Activation du Sampled NetFlow sur une interface (courbe verte)*

Une autre évolution du NetFlow concerne son format d'exportation. Au lieu de recevoir au niveau du collecteur des paquets UDP identiques en provenance de tous les routeurs, l'utilisateur peut aujourd'hui choisir le type d'information que contiendra un paquet (utilisation de "templates"). A chaque redémarrage de l'équipement, puis à intervalles réguliers, le format des trames choisies (et enregistrées dans le fichier de configuration des routeurs) est envoyé au collecteur qui dispose ainsi de l'information nécessaire pour analyser les paquets Netflow. Cette technique permet de transporter avec le même protocole (version 9) les différentes versions de NetFlow : "normal" ou "full" (version 5) et le NetFlow agrégé (version 8). Ce format permet également la prise en compte de l'IPv6, du MPLS et du Multicast.

Une version Bêta d'IOS[1] pour le traitement NetFlow des flux IPv6 existe. L'observation des flux IPv6 est actuellement en cours d'implémentation au GIP.
Le NetFlow peut prendre aujourd'hui en compte le multicast. Plusieurs configurations sont possibles : observation du flux entrant sur le routeur (méthode traditionnelle), observation du flux entrant avec comptabilisation des octets sortants (méthode "Ingress"), ou observation des flux sortants (méthode "Egress").
Une dernière nouveauté est la possibilité de configurer un NetFlow Egress sur les cartes ISE (IP Services Engine, cartes spéciales sur les GSR (Gigabit Switch Router) qui ont des caractéristiques supplémentaires -équivalent des NPE-G1 pour les C7200-). Par rapport au NetFlow traditionnel ("ingress") l'"Output Sampled Netflow" observe le trafic sortant sur une interface. Cela permet de surveiller des flux provenant d'un lien MPLS ou IPv4 et qui sortent sur un lien IPv4. Pour l'instant cette possibilité n'est pas appliquée sur le réseau [3].
La prochaine intégration au niveau du collecteur utilisé au GIP est la prise en compte de la version 9 du format de transport, ceci dès que les versions d'IOS seront disponibles (ces versions devant bien sûr inclure les services déjà disponibles dans RENATER-3 : IPv4, IPv6, Multicast). Les spécificités du NetFlow dépendent entièrement des versions d'IOS (pour CISCO).

SNMP permet de signaler les problèmes et/ou anomalies qui durent un certain temps. Par contre les petits phénomènes ou perturbations sont dissimulés. Il est donc nécessaire de disposer d'outils de mesures complémentaires une fois les anomalies détectées (comme ping, traceroute, pchar, etc). Mais ces différents outils bien que complémentaires ne suffisent pas aujourd'hui pour avoir une supervision complète du réseau.

4 De nouvelles mesures... pour de nouveaux besoins

Après une politique de surdimensionnement et de "best-effort", la qualité de service (QoS[2]) apparaît de plus en plus dans les réseaux. Des classes de services vont être mises en place dans RENATER-3 [6]. Il sera donc nécessaire de mesurer et de contrôler ces classes. Les outils actuellement opérationnels au GIP ne gérant pas cette technologie il faut donc se tourner vers d'autres solutions.
De plus, la communauté RENATER, à travers l'utilisation d'applications exigeantes (visioconférences, grilles de calcul...) est de plus en plus intéressée par des indicateurs précis et accessibles représentant l'état du réseau de bout en bout. Les besoins, contraintes et solutions répondant à ces questions et présentés dans la suite de l'article, sont traités dans le cadre du projet RNRT METROPOLIS[3].

4.1 Les besoins et contraintes

Les besoins, en termes de mesures sur un réseau IP, ont été étudiés par l'IETF[4] dans le groupe IPPM[5]. Les mesures de base sont le délai unidirectionnel (ou OWD[6]), le délai aller-retour (RTT[7]), la gigue et le taux de perte. Les contraintes qui apparaissent au niveau d'un outil effectuant ces mesures actives sont la nécessité de traiter les résultats en temps réel, l'activation en continu, la précision des mesures et le facteur d'échelle.
Le traitement à la volée des données collectées permet une supervision quasi temps réel. Cette propriété est utile dans le cas de la surveillance de SLA[8] (pour les classes de services notamment). Une activation permanente de l'outil est aussi obligatoire pour une supervision du réseau. Les temps de traversée du backbone n'étant que de quelques millisecondes, les mesures seront fines et précises (une incertitude de l'ordre de la centaine de microsecondes est nécessaire pour la mesure des délais unidirectionnels). Cette précision est aujourd'hui obtenue sur de nombreux outils avec des antennes GPS, mais cette caractéristique introduit des contraintes supplémentaires (problèmes d'installation, de coût et de maintenance) : le passage à l'échelle est un facteur essentiel compte tenu des futures évolutions du réseau.
La visualisation des résultats devra être orientée "utilisateur final" : l'interface pourra s'inspirer de Beacon[7], outil déjà utilisé par le NOC-RENATER-3[9] afin de superviser l'état du trafic Multicast. Ce dernier mesure les délais, gigues et pertes entre différents clients logiciels et présente les résultats sous forme de matrices sur des pages HTML.

---

[1] IOS : Internetwork Operating System
[2] QoS: Quality of Sevices
[3] METROPOLIS: Métrologie pour l'Internet et ses Services (présentation sur le site: http://www.telecom.gouv.fr/rnrt/projets/res_01_57.htm)
[4] IETF: Internet Engineering Task Force
[5] IPPM: IP Performance Metrics
[6] OWD: One Way Delay
[7] RTT: Round Trip Time
[8] SLA: Service Level Agreement
[9] NOC: Network Operation Centre

L'utilisateur devra pouvoir, à terme, effectuer ses propres mesures "End-to-End" (E2E). L'ouverture de la solution vers l'utilisateur est un réel besoin, mais également une forte contrainte (problèmes d'échelle car fonction du nombre d'utilisateur). Le dernier besoin est la mise en place d'une telle solution parmi tous les acteurs réseaux. Les sites RENATER étant connectés via les réseaux de collecte, il est nécessaire de disposer de sondes (matérielles ou logicielles) au niveau de ces réseaux car les mesures intra-backbone ne sont pas représentatives à elles seules des mesures de bout en bout.

4.2 Les solutions existantes

	SAA	RIPE TTM	Saturne	Rude/Crude	NIMI	QOS Metrix
Matériel	routeur	boîtier (pc/FreeBSD)	PC (FreeBSD)	PC (linux)	PC (divers OS)	boîtier
GPS intégré	non	oui	Non	non	non	Selon modèle
Sécurité	Authentification sondes par MD5 possible	Aucune	Aucune	Paquets numérotés	Chiffrement	Intégrée
Réception des paquets sondes	Non précisée	Capture (pcap) + socket	Capture (bpf)	Socket	Dépend de l'outil utilisé	matérielle
Estampillage	Non précisé	Avant envoi sur socket	Kernel	Avant envoi sur socket		matériel
Paramétrage du DSCP des paquets sondes	oui	non	Oui	oui		oui
Collecte	Distante, par SNMP	Logs locaux envoyés au site central quotidiennement	Logs locaux, envoi au site central par RPC de chaque mesure	Logs locaux	Logs locaux	Vers site central en temps réel
Présentation des résultats	Non intégrée	Très complète, sur serveur web local et central (à Amsterdam)	Non intégrée	Non intégrée	Non intégrée	Site web central
Modification/ adaptation de l'outil	Impossible	Possible (mais nécessite demande à RIPE)	Possible	Possible	Possible (mais code source imposant)	Impossible
Licence	commerciale	commerciale	non définie actuellement	GPL	GPL	commerciale

Tableau 1 – *Caractéristiques des outils étudiés (source [5])*

Il existe de nombreuses solutions, commerciales ou non, répondant plus ou moins aux critères précédents. Le tableau 1 présente les principales caractéristiques des outils étudiés. SAA[1], Rude/Crude[8], Saturne[9], ont été testés au GIP ; RIPE TTM[2] et NIMI[3] sont actuellement déployés au sein de la plate-forme de mesures de METROPOLIS.

L'utilisation de la technologie SAA n'est pas envisageable sur le backbone en raison de sa faible précision. NIMI représente une architecture sur laquelle l'installation de "plugins" est possible mais son développement n'est toutefois pas terminé.
De plus, sur les outils testés au GIP, un phénomène de mesures aberrantes a été remarqué : ponctuellement, certaines mesures étaient bien supérieures aux autres (plusieurs dizaines de millisecondes au lieu de quelques millisecondes). Ce phénomène est en fait dû aux systèmes d'exploitation non temps réel : le processus de mesure est parfois interrompu inopinément par le système, faussant ainsi la mesure du temps, et cela se révèle très gênant dans le cas d'une surveillance basée sur un dépassement de seuil. La première solution pour résoudre ce problème est l'utilisation d'un système d'exploitation temps réel ;

[1] SAA: Service Assurance Agent (CISCO)
[2] RIPE TTM : http://www.ripe.net/ttm/
[3] NIMI: National Internet Measurement Infrastructure

mais il faut souvent réécrire une partie du code de l'outil. La deuxième solution consiste à traiter ces valeurs aberrantes par un processus logiciel, mais ce dispositif n'est pas actuellement disponible dans les outils étudiés.

4.3 Une architecture ouverte

Pour l'instant l'architecture retenue est hétérogène. Des mesures très fines sur le backbone sont nécessaires à la vue des performances de ce dernier. Par contre les mesures "E2E" n'ont pas besoin d'un tel niveau de précision. Des sondes sur les nœuds RENATER permettront d'effectuer des mesures permanentes entre elles alors que les mesures "E2E" ne seraient que ponctuelles (figure 8).

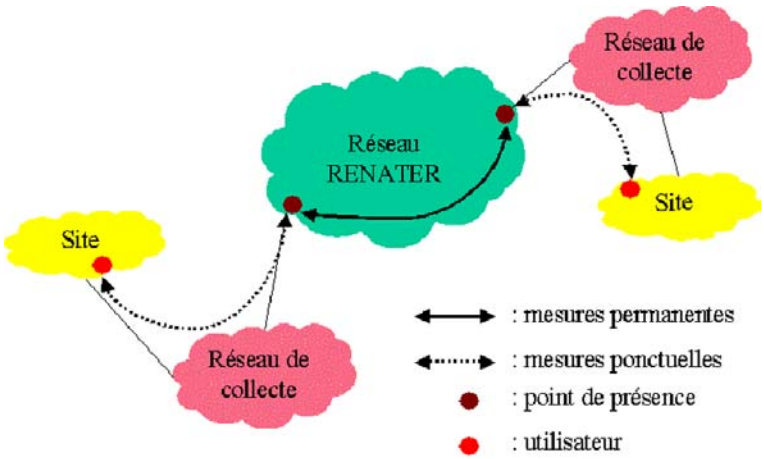

Figure 8 – *Mesures "E2E" (source [5])*

Les solutions libres qui sont utilisables dans le cadre d'une telle architecture sont malheureusement trop difficiles à adapter en termes de développement, ou pas assez précises. Les sondes commerciales (qui sont souvent plus abouties) sont quant à elles « propriétaires » et ont un coût plus élevé. Le choix n'est aujourd'hui pas arrêté.

5 Conclusion

La liste des outils présentés dans cet article ne se veut pas exhaustive. Pour plus d'information sur les outils de métrologie existants, vous pouvez lire les « états de l'art » du projet METROPOLIS et du projet IST[1] SCAMPI[2][10] et/ou visiter le site de CAIDA[3][11].
Cet article n'a pas traité des outils de mesures passives d'analyse/capture de trafic. Non pas parce qu'ils sont moins utiles que les autres mais tout simplement parce qu'ils ne sont pas employés aujourd'hui sur le backbone (pour des raisons de difficulté d'installation, de coût, et de capacité de traitement des informations). Par contre la plate-forme de mesures du projet METROPOLIS exploite actuellement ces outils, indispensables pour certaines études du trafic Internet.
Comme on a pu le voir, la métrologie évolue en fonction des changements du réseau, mais aussi avec les souhaits des utilisateurs. Nous espérons au GIP RENATER contribuer, grâce à la métrologie, à une meilleure qualité du réseau (aspects supervision, dimensionnement, politique de routage, sécurité) ainsi qu'à une meilleure connaissance/visibilité de celui-ci de la part des sites RENATER. Mais les mesures de bout en bout ne dépendent pas seulement de la mise en place de la métrologie sur RENATER-3, mais également d'une infrastructure de métrologie au sein des réseaux de collectes.

Références

[1] N.G. Duffield and C. Lund, Predicting Resource Usage and Estimation Accuracy in an IP Flow Measurement Collection Infrastructure. Dans *ACM SIGCOMM Internet Measurement Conference*, Miami Beach, Octobre 2003.
[2] NetFlow Overview : http://www.cisco.com/warp/public/732/Tech/nmp/netflow/netflow_presentations.shtml

[1] IST : Information Society Technologies
[2] SCAMPI: Scaleable Monitoring Platform for the Internet
[3] CAIDA: Cooperative Association for Internet Data Analysis

[3] Output Sampled NetFlow :
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/12soutfl.htm
[4] GGF Network Measurements Working Group : http://www-didc.lbl.gov/NMWG/NM-WG-tools.html
[5] G. Yonnet, E. Da Costa, Définition et Spécifications d'un système de métrologie active. *Rapports de stages* effectués au GIP RENATER, 2003
[6] Franck Simon, Implémentation des classes de services dans RENATER 3. Dans *Actes du congrès JRES2003*
[7] Multicast Beacon : http://dast.nlanr.net/Projects/Beacon/
[8] Rude & Crude : http://rude.sourceforge.net/
[9] J. Corral, M. Ourraou, G. Texier, L. Toutain, Platform Implementation for Measurement QoS Parameters in the Internet Network. *Rapport Saturne* ENST Bretagne, 2002
[10] Arne Oslebo, "Description and analysis of the state of the art". *Document 0.1* du projet SCAMPI, août 2002
[11] CAIDA http://www.caida.org