netMAT : network's MATrix, la matrice des flux des réseaux

Karol PROCH
CIRIL - Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault
54500 VANDOEUVRE LÈS NANCY - FRANCE
Karol.Proch@ciril.fr

Alexandre SIMON
CIRIL - Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault
54500 VANDOEUVRE LÈS NANCY - FRANCE
Alexandre.Simon@ciril.fr

Sébastien MOROSI
CIRIL - Centre Interuniversitaire de Ressources Informatiques de Lorraine
Rue du Doyen Roubault
54500 VANDOEUVRE LÈS NANCY - FRANCE
Sebastien.Morosi@ciril.fr

Résumé

Depuis 2000 le CIRIL utilise netMET, developpé par Alexandre Simon, pour quantifier et qualifier le trafic entre Lothaire et Renater. Les services rendus par cet outil ont fait émerger le besoin de mieux connaître la nature du trafic interne à Lothaire non couvert par netMET. Le projet netMAT a été initié en septembre 2005 afin de satisfaire cette demande. L'étude a commencé par une évaluation de la faisabilité du projet. Les informations disponibles sur le trafic interne à Lothaire étant de même nature que celles utilisées par netMET (les NetFlows envoyés par les routeurs Cisco), une première version de netMAT réutilisant le collecteur de netMET couplé à une exploitation spécifique des données collectées a été développée. Dans un deuxième temps le collecteur a été modifié pour faciliter sa configuration et permettre entre autre la prise en compte de nouveaux formats de NetFlows (v9). Ces modifications fonctionnelles du collecteur ont conduit à mettre en chantier une nouvelle version ; son développement est en cours.

Mots clefs

Métrologie, matrice de flux, NetFlow Cisco.

1 Introduction

Lothaire fédère les réseaux des quatre Universités de Lorraine, l'ensemble des établissements scolaires du second degré (hors collèges) et de l'enseignement supérieur ainsi que les centres de recherche du CNRS, de l'INSERM, de l'INRA et de l'INRIA. Lothaire est l'agrégation des réseaux métropolitains des villes de Nancy et Metz (réseaux StanNet et AmpereNet), du réseau des lycées lorrains eLorraine et de tous les autres sites académiques délocalisés. Au total, près de 230 000 utilisateurs sont potentiellement amenés à se connecter à ce réseau. Le CIRIL[1] administre aujourd'hui l'intégralité de ces réseaux, à l'exception du réseau métropolitain de Metz (AmpereNet).

Lothaire propose à ses utilisateurs une connexion au réseau Renater, dont l'ensemble des échanges représente plus de 3.5 To par jour avec un débit dépassant les 700 Mbit/s. Le CIRIL ne pouvait se satisfaire de ces ordres de grandeur et a eu besoin de quantifier et de qualifier les trafics entre Lothaire et Renater :

- pour dimensionner au mieux les matériels et les liaisons ;
- pour ajuster les classes de service (*CoS*) et configurer la qualité de service (*QoS*) ;
- pour satisfaire les besoins de sécurité (détection d'attaques et de tentatives d'intrusion) ;
- pour affiner la gestion financière.

Depuis plusieurs années, le trafic entre Lothaire et Renater est mesuré avec la technologie NetFlow de Cisco[2] et le logiciel netMET (*network's METrology)* développé par Alexandre SIMON [1] [2]. En exploitation depuis 2000, cette solution a montré sa robustesse et donne entière satisfaction ; les réponses aux besoins exprimés sont fournies par les informations de métrologie suivantes :

- top N par organisme (université, centre de recherche...), par machine ;
- volumétrie pour chaque organisme, par protocole, par service/protocole ;
- débits instantanés, moyens, maximums ;
- rapports de sécurité concernant les « scans » de réseaux.

Il est rapidement apparu nécessaire de quantifier et de qualifier le trafic interne à Lothaire pour répondre aux mêmes questions de dimensionnement, de qualité de service ou de sécurité sur ce réseau. netMET n'ayant pas

[1] Centre Interuniversitaire de Ressources Informatiques de Lorraine

[2] http://www.cisco.com/go/netflow

été conçu à cette fin, il ne permet pas l'analyse du trafic interne à Lothaire. Le CIRIL a donc initié en septembre 2005 le projet netMAT (*network's MATrix)* pour répondre à cette problématique nouvelle en exploitant la matrice des flux du réseau Lothaire.

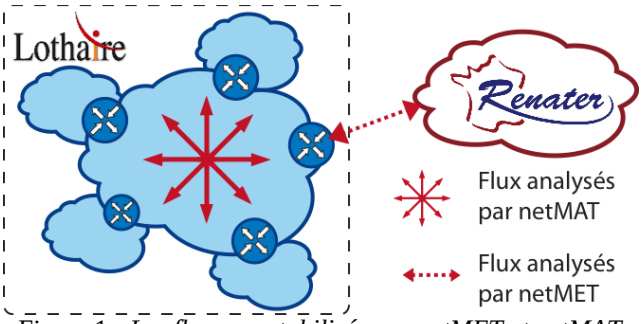

Figure 1 - *Les flux comptabilisés par netMET et netMAT*

Comme l'illustre la Figure 1, les applications netMET et netMAT sont complémentaires, la première prenant en compte les flux entre Lothaire et Renater, la seconde les flux internes à Lothaire.

2 De netMET à netMAT

netMAT a été d'emblée perçu comme un « héritier » de netMET avec le souhait de profiter de l'expérience acquise et si possible de réutiliser des codes déjà développés. Pour cela, il fallait que l'architecture globale de netMAT puisse être calquée sur celle de netMET présentée dans [1]. Comme netMET, netMAT se base sur les informations de routage reçues des équipements (NetFlows).

Rappelons que l'architecture de netMET comporte deux grandes parties. L'une réalise la collecte des NetFlows et le stockage des informations pertinentes, l'autre réalise l'exploitation de ces informations. L'exploitation n'est pas faite « au fil de l'eau » mais est relative à une période donnée.

Lors de la collecte, les datagrammes NetFlows sont analysés et les flux extraits sont pré-traités pour les synthétiser puis les enregistrer dans des fichiers. Ces fichiers ne contiennent donc pas l'information brute, mais seulement l'information nécessaire et suffisante à la métrologie netMET.

Lors de l'exploitation les informations conservées par le collecteur sont traitées et mises en forme pour obtenir les résultats souhaités sous forme d'un ensemble de pages XML.

Lors du lancement du projet netMAT, notre volonté était de reprendre le collecteur de netMET et de pouvoir ainsi travailler en deux phases :

- valider la faisabilité de l'exploitation netMAT : était-il possible de traiter les informations dans un délai raisonnable et surtout trouver un mode de représentation adapté ?
- reprendre le développement du collecteur afin de supporter les nouveaux standards.

Cette volonté d'avoir une architecture commune et des éléments communs nous garantissaient par la même occasion une évolution des deux solutions en parallèle et une maintenance plus facile.

Notons enfin que netMET base l'ensemble de ses représentations sur une notion d'organisme qui ne modélise pas la structure hiérarchique des établissements et de leurs réseaux. Un des défis de la conception de netMAT était donc de trouver une solution permettant de présenter des informations de métrologie en tenant compte des hiérarchies existantes.

3 La matrice des flux internes à Lothaire

Pour simplifier, la question posée est de savoir qui dialogue avec qui au sein de Lothaire et sous quelle forme. Les personnes en charge de Lothaire souhaitent connaître :

- la liste des organismes ayant le plus utilisé le réseau durant une période donnée ;
- la répartition entre les organismes des flux émis (sortant) ou reçus (entrant) ;
- la part de chaque service/protocole dans le trafic ;
- l'évolution du débit « instantané » au cours de la période d'observation ;
- les volumes échangés dans chaque sens par chaque couple d'organismes et leur répartition en services.

Les quatre premiers items se prêtent à des représentations graphiques (histogrammes, « camemberts » et courbes) complétées par des tableaux. Le dernier nécessite de construire, pour la période concernée, une matrice de flux dont les lignes et les colonnes sont indicées par les organismes, chaque case contenant le volume des échanges par couple d'organismes, avec le détail par service. Le nombre potentiellement important d'organismes connectés, une trentaine dans le cas de Lothaire (donc le nombre de lignes et de colonnes de cette matrice) et le nombre important de services posent le problème de sa mise en page.

Celle-ci doit de plus intégrer la structure hiérarchique des organismes connectés à Lothaire.

3.1 La hiérarchie des organismes connectés

Les organismes connectés à Lothaire (universités, grandes écoles, laboratoires...) sont eux-mêmes structurés en composantes diverses telles que U.F.R[3], équipes de recherche, départements. Celles-ci sont à leur tour composées d'entités plus petites. Parallèlement, les équipements informatiques de ces diverses entités sont connectés à des sous-réseaux distincts. Cette structuration

[3]Unité de Formation et de Recherche

des organismes et de leurs sous-réseaux forme une arborescence à trois niveaux et les administrateurs « informatiques » des différents nœuds de l'arbre ont besoin d'informations similaires à chacun de ces nœuds. Il faut dès lors avoir la possibilité de « zoomer » sur le trafic d'un organisme particulier pour fournir les informations le concernant en distinguant les échanges entre composantes de l'organisme des échanges entre ces composantes et les organismes extérieurs.

3.2 Les informations disponibles aux feuilles de l'arborescence des organismes

Considérons les départements *da1* et *da2* de l'IUT *iutA* et le département *db1* rattaché à l'IUT *iutB* (Figure 2).

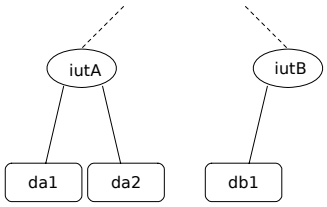

Figure 2 - *Arborescence des organismes (extrait)*

Pour connaître le détail de la répartition en services/protocoles des flux échangés entre *da1* et ses pairs[4] durant une période donnée, il faut lister pour chaque couple (*da1, da2*) et (*da1, db1*) et pour les services utilisés : le total des octets transmis dans chaque sens, éventuellement les pourcentages que cela représente (Figure 3).

Échanges entre da1 et da2

service/ protocole	da1->da2	% du total da1->da2	da2->da1	% du total da2->da1	da1<->da2	% du total
www-http/tcp	10.7 Mo	74.15%	9,8 Mo	75.44%	20,5 Mo	74,76%
smtp/tcp	2.1 Mo	14.55%	1.7 Mo	13.09%	3.8 Mo	13,86%
ssh/tcp	0.88 Mo	6.10%	0.77 Mo	5.93%	1.65 Mo	6,02%
domain/udp	0.75 Mo	5.20%	0.72 Mo	5.54%	1.47 Mo	5,36%
Total	14.4 Mo	100.00%	13.0 Mo	100.00%	27.4 Mo	100.00%

Échanges entre da1 et db1

service/ protocole	da1->db1	% du total da1->db1	db1->da1	% du total db1->da1	da1<->db1	% du total
www-http/tcp	10.3 Ko	55.68%	17.0 Ko	88.55%	27.3 Ko	67.91%
https/tcp	5.8 Ko	31.35%	2.3 Ko	8.81%	8.1 Ko	20.25%
smtp/tcp	2.4 Ko	12.97%	1.7 Ko	2.64%	4.8 Ko	11.94%
Total	18.5 Ko	100.00%	21.7 Ko	100.00%	40.2 Ko	100.00%

Figure 3 - *Les échanges de da1 avec ses pairs*

Pour avoir une vue complète sur l'activité de *da1* il faut ajouter à ces tableaux celui décrivant le trafic interne à ce département (Figure 4). Attention de ne pas se méprendre sur la signification du terme « interne ». Les informations de trafic étant fournies par les routeurs, seul le trafic routé est mesuré. Une partie des échanges entre utilisateurs reste à jamais ignorée (i.e. le trafic dans un même sous réseau non routé est ignoré).

Un tableau montrant la répartition en services/protocoles de l'ensemble des flux entrant ou sortant de *da1* (Figure 5) (qui est en quelque sorte la « fusion » des précédents) complète le dispositif par une vue synthétique de l'ensemble des flux.

Échanges internes à da1

service/ protocole	Nombre d'octets	% du total
tina/tcp	1.3 Go	92.84%
nfs/tcp	60 Mo	4.28%
ssh/tcp	40 Mo	2.86%
www-http/tcp	263.4 Ko	0.02%
Total	1.4 Go	100.00%

Figure 4 - *Les échanges internes à da1*

Ces informations « brutes » peuvent de plus faire l'objet de graphiques : des « camemberts » pour représenter les répartitions en pourcentages, des histogrammes pour visualiser rapidement les principaux interlocuteurs.

Répartition de l'ensemble des flux depuis ou vers da1

service/ protocole	flux sortant	% du total sortant	flux entrant	% du total entrant	total	% du total
tina/tcp	1.3 Go	91.91%	1.3 Go	92.00%	2,6 Go	91.96%
www-http/tcp	10.71 Mo	0.76%	9,82 Mo	0.69%	20,53 Mo	0.73%
smtp/tcp	2.1 Mo	0.15%	1.7 Mo	0.12%	3.8 Mo	0.13%
ssh/tcp	40.88 Mo	2.89%	40.77 Mo	2.89%	81.65 Mo	2.89%
domain/udp	0.75 Mo	0.05%	0.72 Mo	0.05%	1.47 Mo	0.05%
nfs/tcp	60 Mo	4.24%	60 Mo	4.25%	120 Mo	4.24%%
Total	1.41 Go	100.00%	1.41 Go	100.00%	2.83 Go	100.00%

Figure 5 - *L'ensemble des échanges de da1*

Des tableaux analogues doivent être construits pour les départements *da2* et *db1*. Il faut noter qu'un même tableau peut être destiné à plusieurs interlocuteurs. Ainsi le tableau décrivant le trafic interne à *da1* intéresse les responsables de ce département mais aussi les responsables de *iutA* et de l'université de rattachement de cette entité tandis que le tableau décrivant les échanges entre *da1* et *db1* concerne les responsables de ces deux entités et de leurs organismes de rattachement (IUTs et Universités dans cet exemple).

3.3 Les informations disponibles aux nœuds de l'arborescence

Aux autres nœuds de l'arborescence, la situation est un peu plus complexe. Il reste pertinent de présenter des tableaux comparables à ceux construits pour le niveau le plus bas de l'arborescence. Dans l'exemple considéré, si on se place au noeud correspondant à *iutA*, un tableau donnera la ventilation en services/protocoles des flux entre *iutA* et *iutB* (Figure 6), et un autre analogue à celui de la Figure 4 précisera la ventilation en services/protocoles des flux internes à *iutA*.

[4]Nous appelons pair d'une entité une entité de même niveau dans l'arborescence. Dans l'exemple *iutB* est un pair de *iutA*, *da2* et *db1* sont des pairs de *da1*.

Échanges entre iutA et iutB

service/ protocole	iutA->iutB	% du total iutA->iutB	iutB->iutA	% du total iutB->iutA	iutB<->iutA	% du total
www-http/tcp	xxx	xxx%	xxx	xxx%	xxx	xxx%
https/tcp	xxx	xxx%	xxx	xxx%	xxx	xxx%
...	...	...	...	...	...	...
Total	xxx	100.00%	xxx	100.00%	xxx	100.00%

Figure 6 - *Les échanges de iutA avec ses pairs*

Ces tableaux ne donnent aucun renseignement sur la part de chaque composante dans le trafic. Il est pourtant souhaitable d'avoir à ce niveau une première vue sur les volumes provenant ou à destination de chaque département.

Part de chaque département dans le trafic de iutA

département	octets sortants	% du total sortant	octets entrants	% du total entrant
da1	1414,71 Mo	99,06%	1413,28 Mo	98,64%
da2	13,49 Mo	0,94%	19,43 Mo	1,36%
Total	1428,20 Mo	100.00%	1432,71 Mo	100.00%

Figure 7 - *La part de chaque composante dans le trafic total de iutA*

Pour satisfaire ce besoin un premier tableau visualise la part de trafic de chaque composante de l'entité considérée, ici *da1* et *da2* (Figure 7).

Ce tableau ne permet pas de savoir « qui dialogue avec qui ». Il faut lui adjoindre deux matrices montrant les échanges qui impliquent les composantes de *iutA*. La première présente le trafic entre les composantes *da1* et *da2* (Figure 8).

Qui communique avec qui au sein de iutA

	da1	da2	Total
da1	1400,26 Mo	14,43 Mo	1414,69 Mo
da2	12,99 Mo	0,40 Mo	13,39 Mo
Total	1413,25 Mo	14,83 Mo	1428,08 Mo

Figure 8 - *Les échanges au sein de iutA*

La seconde matrice montre le trafic entre *da1* et *da2* et les pairs de *iutA*, ici *iutB* (Figure 9). Le trafic entrant et le trafic sortant ne sont pas distingués mais totalisés.

Qui, au sein de iutA, communique avec l'extérieur

	da1	da2	Total
iutB	40,20 Ko	---	---
Total	40,20 Ko	---	---

Figure 9 - *Le trafic des composantes avec l'extérieur*

Ces informations concernant *iutA* s'adressent aux responsables de cette entité mais doivent être aussi visibles par les responsables de son organisme de rattachement (une université dans ce cas). En revanche les responsables des départements *da1* et *da2* n'y ont pas accès.

A chaque racine de l'arborescence, les universités de rattachement de *iutA* et *iutB* dans l'exemple, la situation est analogue au cas qui vient d'être exposé. Les mêmes tableaux et matrices présentent :

- la répartition en services/protocoles des échanges de l'université avec chacun de ses pairs ;
- la répartition en services/protocoles des échanges internes de l'université considérée ;
- la part de chaque composante dans le trafic entrant et sortant de l'université ;
- les volumes échangés entre composantes de l'université ;
- les volumes échangés entre les composantes de l'université et les autres universités.

L'arborescence Lothaire ne comporte que trois niveaux, mais quel que soit le nombre de niveaux de l'arborescence ce même schéma s'applique à tous les nœuds[5].

3.4 L'organisation des pages

Les différents tableaux et matrices décrits dans le paragraphe précédent sont placés dans des pages XML. Les mesures de trafic sont relatives à une période donnée et nous avons choisi la journée comme période de référence, ces pages sont donc générées quotidiennement. De plus les informations quotidiennes sont utilisées pour construire des bilans mensuels. Ces bilans mensuels sont présentés selon les mêmes schémas que les informations quotidiennes et placés dans des pages mensuelles.

A chaque noeud et à chaque feuille de l'arborescence des organismes correspond une page XML contenant les informations associées. Les différentes personnes habilitées à consulter ces pages ont une visibilité correspondant à leur domaine de responsabilité. Ainsi le responsable d'un département d'IUT n'a accès qu'à la page qui le concerne tandis celui d'une université peut accéder à tout le sous-arbre. Ces contrôles d'accès sont, comme dans netMET, assurés par le serveur HTTP et basés sur les noms des pages.

Bien entendu des liens permettent la navigation dans ces pages. Depuis la page d'une composante donnée, des liens placés dans les différents tableaux permettent de « zoomer » sur la sous-composante concernée. Il est aussi possible de naviguer dans le temps et d'accéder aux pages des autres jours et aux récapitulatifs mensuels.

Comme il n'est pas possible de prévoir tous les besoins de présentation des informations contenues dans ces pages ni les éventuels traitements complémentaires qui peuvent s'avérer utiles à leurs lecteurs (tris, filtrages sur critères), les contenus des différents tableaux sont accessibles sous forme de fichiers importables dans un tableur[6]. Chacun peut ainsi personnaliser l'exploitation des différents résultats.

[5] sauf aux feuilles (cf. paragraphe précédent).

[6] au format .csv

Une page d'accueil destinée aux ingénieurs du CIRIL en charge de Lothaire coiffe l'arborescence. Elle contient la matrice des volumes échangés entre les organismes partenaires (universités, centres de recherche...) ainsi qu'un tableau décrivant la répartition en services/protocoles de la totalité du trafic interne à Lothaire. Plusieurs graphiques synthétisent l'activité sur Lothaire, comme le « top N » des trafics par organisme (Figure 10) ou l'évolution du débit (Figure 11).

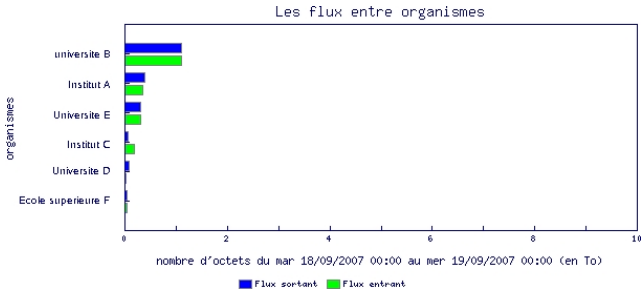

Figure 10 - *Le top N des organismes*

Avec l'expérience, les ingénieurs y détectent rapidement des anomalies comme un trafic anormal d'un organisme ou un pic d'activité à un moment inhabituel.

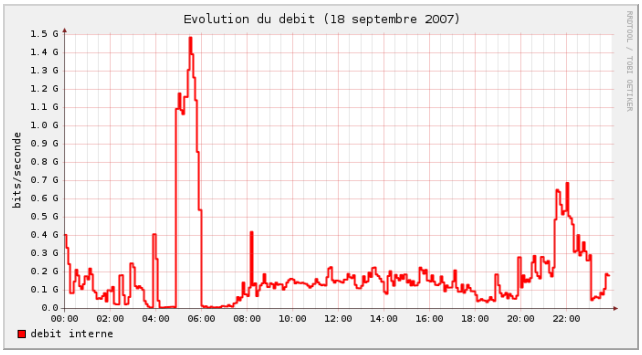

Figure 11 - *L'évolution du débit*

4 Exportation et filtrage des informations de flux

Analyser l'information et la mettre en forme suppose bien entendu que celle-ci soit correctement exportée par le réseau. Il est indispensable de configurer les équipements réseau afin de recevoir les NetFlows concernant tous les flux routés.

Nous devons de plus nous assurer qu'un même flux n'est pas pris en compte plusieurs fois par netMAT, et nous verrons que plusieurs mécanismes doivent être couplés pour arriver au résultat souhaité.

4.1 L'export des NetFlows

Sur Lothaire, l'ensemble des équipements actifs sont des équipements Cisco. Cette homogénéité facilite l'exportation des informations souhaitées, puisque l'ensemble du parc supporte cette fonctionnalité.

L'infrastructure de routage est composée pour partie de routeurs (série 28xx et des 7206) et de *Catalysts* (commutateurs/routeurs) de la série 6500. Concernant les routeurs, l'exportation des NetFlows est relativement aisée et peut se faire par interface. En revanche la configuration des *Catalysts* est plus délicate. Les NetFlows doivent être activés pour la partie routage et pour la partie commutation. Pour la partie routage, il est possible de choisir les interfaces pour lesquelles les informations sont exportées, par contre pour la partie commutation l'exportation est globale[7].

Nous verrons par la suite que cela est problématique et impose un filtrage au niveau du collecteur.

4.2 Le filtrage des NetFlows

Il est impératif de ne comptabiliser qu'une seule fois chaque paquet circulant sur le réseau.

Considérons l'exemple illustré par la Figure 12. Les paquets circulant du réseau A vers le réseau B traversent deux routeurs. Si chaque routeur exporte les informations de routage pour toutes ses interfaces vers la plate-forme de métrologie, les paquets allant de A à B seront comptés deux fois.

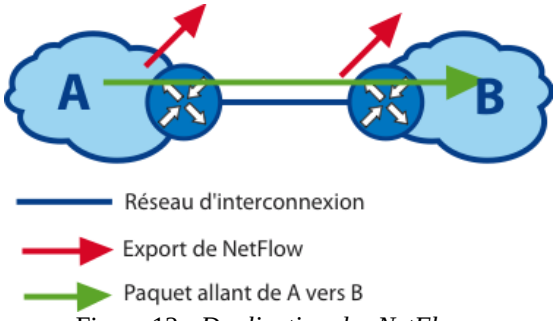

Figure 12 - *Duplication des NetFlows*

Une solution simple pour prévenir ce problème est de ne pas activer l'exportation de NetFlows pour l'une des deux interfaces. Nous avons alors opté pour la règle suivante : *ne jamais activer l'exportation des NetFlows sur les interfaces d'interconnexion*. En respectant cette règle, nous évitons toute duplication des informations collectées. L'exportation doit être activée sur toutes les interfaces de routage directement connectées aux réseaux d'utilisateurs.

Un problème subsiste néanmoins. Comme expliqué précédemment, il est parfois impossible de restreindre l'exportation à certaines interfaces. De plus, certains routeurs sont déjà configurés pour exporter les NetFlows vers netMET et ils ne peuvent trier ces NetFlows selon leur destination. Autrement dit, les deux plates-formes netMET et netMAT reçoivent forcément les mêmes informations de ce(s) routeur(s). Dès lors, il est nécessaire de pouvoir filtrer les NetFlows reçus.

---

[7]Les dernières versions d'IOS pour *Catalyst 6500* proposent maintenant l'exportation de niveau 2 par interface.

Compte tenu de la complexité de la configuration de certains routeurs ou encore du nombre d'interfaces gérées, la grammaire de filtrage du collecteur de netMET n'était plus adaptée. Nous avons dû l'étendre afin d'introduire la distinction entre interface d'entrée et interface de sortie d'un routeur et les notions de complémentaire d'un ensemble d'interfaces ou de flux.

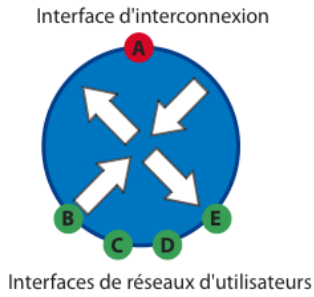

Figure 13 - *Filtrage des NetFlows*

Dans le cas de la Figure 13, si les NetFlows sont exportés pour l'ensemble du routeur, il faudra conserver tous les flux entrant dans les interfaces B,C,D et E, mais éliminer tous les NetFlows concernant les paquets entrant dans l'interface A. La syntaxe de netMET oblige à énumérer les couples valides (B et C, B et D, B et E, C et D, C et E, D et E). Une syntaxe permettant de désigner les interfaces ou les flux à ignorer, les flux de A vers n'importe quelle interface, simplifie notablement l'expression du filtrage.

5 Le collecteur

Dans un premier temps, le collecteur de netMET a été utilisé en l'état pour développer un prototype de l'application et obtenir un ordre de grandeur des flux internes, des quantités de données collectées, des durées de traitement et des tailles des pages de résultats tout en permettant de valider la mise en page retenue.

5.1 Configuration du collecteur netMET

Une fois ces premiers objectifs atteints une nouvelle version du collecteur a été développée pour étendre les possibilités de filtrage. Rappelons que le collecteur de netMET utilise un fichier de configuration spécifiant le port d'écoute des NetFlows et leur filtrage. Ce fichier contient donc l'adresse IP de l'interface locale de la machine et le numéro du port vers lequel sont envoyés les datagrammes NetFlows ainsi qu'une suite de règles de filtrage des NetFlows reçus. Chaque élément de cette liste décrit un des routeurs à prendre en compte dans la collecte et contient :

- l'adresse IP du routeur ;
- le mot de passe de la communauté « READ SNMP » du routeur considéré ;
- l'ensemble des couples de noms d'interfaces A <-> B indiquant les interfaces d'entrée et de sortie[8] des NetFlows à comptabiliser pour ce routeur, sans distinction de sens.

Facultativement, le fichier de configuration peut contenir un ensemble de couples constitués d'un nom d'interface et d'une adresse IP (dite d'agrégation), utilisés pour regrouper et comptabiliser tous les flux entrant ou sortant de ces interfaces.

5.2 Configuration du collecteur netMAT

Comme nous l'avons vu dans les paragraphes précédents il est impératif de pouvoir distinguer les interfaces d'entrée des interfaces de sortie des routeurs. La syntaxe des paragraphes décrivant le filtrage des flux, reprise de netMET, a donc été étendue avec des symboles précisant le sens de transit à travers les interfaces des routeurs.

```
IF_PROCESSED {
   if_B -> if_A
   if_A <- if_C
   if_B <-> if_C
}
```

Figure 14 - *Exemple de filtre*

Il est maintenant possible de comptabiliser les flux entrant par l'interface *if_B* et sortant par l'interface *if_A*, sortant par l'interface *if_A* et entrés par l'interface *if_C* (Figure 14). Il reste bien sûr possible d'utiliser la notation bilatère.

Le nombre d'interfaces pouvant être important sur un routeur (plusieurs centaines), l'énumération de ces couples peut devenir fastidieuse. Des notations complémentaires permettent de simplifier l'expression des règles de filtrage. Ainsi il est possible d'utiliser dans la spécification d'un couple d'interfaces les mots-clés *ALL* et *OTHER*[9].

Le premier représente n'importe quelle interface du routeur, le second n'importe quelle interface sauf l'autre terme du couple. La règle *ALL -> ALL* est équivalente à *ALL <- ALL* et à *ALL <-> ALL*. Bien entendu, dès qu'une telle règle figure dans une clause *IF_PROCESSED* elle rend caduque toute autre règle : tous les flux transitant par ce routeur sont conservés. La clause s'écrit alors plus simplement *IF_PROCESSED { ALL }*[10]. Comme *ALL* le mot-clé *OTHER* permet de simplifier l'écriture en factorisant l'interface d'entrée ou de sortie d'une liste de règles. Bien entendu il est interdit d'écrire *ALL -> OTHER* ou *OTHER -> OTHER*.

Pour désigner un ensemble d'interfaces il est maintenant possible d'utiliser la notation *ALL_EXCEPT* désignant une interface quelconque à l'exclusion de celles énumérées

[8]Les noms d'interfaces utilisés sont ceux figurant dans les descriptions associées aux numéros d'interfaces conservées dans la MIB SNMP.

[9]OTHER était déjà utilisable avec le collecteur netMET.

[10]Cette formulation est aussi héritée de netMET.

derrière le mot-clé. Ainsi l'exemple de la Figure 13 peut s'écrire :
IF_PROCESSED { ALL_EXCEPT { A } -> ALL }.

Il est enfin possible de décrire l'ensemble des flux retenus en explicitant les flux à exclure. L'exemple de la Figure 14 s'écrit :
ALL_IF_PROCESSED_EXCEPT { if_A -> ALL }
(en supposant que le routeur concerné ne comporte que trois interfaces A, B et C).

5.3 Nouveau format des NetFlows

Le collecteur de netMET a été développé avant l'introduction du format NetFlow v9 par Cisco. Seuls les formats v1, v5, v7 ont donc été pris en compte lors de son écriture. L'évolution inéluctable du parc nous a amenés à modifier le collecteur pour qu'il traite le format v9 des NetFlows. Ce format a pour intérêt de ne pas figer le format d'exportation des NetFlows grâce à l'utilisation de modèles d'exportation (*templates*). Cette souplesse dans la définition des informations exportées, ainsi que les possibilités d'échantillonnage des flux (*sampling*) permettent de diminuer le volume des NetFlows émis par les routeurs et donc d'alléger leur traitement. De plus la proximité du format v9 avec la norme IPFIX[11] rend possible l'utilisation d'une plus grande variété de routeurs.

Cette tâche de réécriture n'est qu'en partie terminée, le collecteur n'étant actuellement pas capable de traiter les adresses IPv6. Il reste en effet à définir un nouveau format des fichiers de collecte et à modifier en conséquence les codes de l'exploitation.

6 Etat du projet et perspectives

Une version de netMAT à usage interne au CIRIL est opérationnelle depuis plusieurs mois. Elle utilise un collecteur netMET partiellement réécrit afin d'intégrer les extensions de syntaxe présentées précédemment. Elle a permis de valider la présentation retenue pour les résultats et informe les personnes en charge de Lothaire sur l'utilisation du réseau. Il a ainsi été mis en évidence l'importance des échanges sur ce réseau, en moyenne 2 Tera octets par jour avec des pointes à près de 4 Tera octets dont près de la moitié correspondent à des services de sauvegarde.

Il faut noter que netMAT est « gourmand » en ressources. Les fichiers résultats de la collecte utilisent jusqu'à 1.5 Giga octets par jour lorsqu'on conserve les mesures servant aux calculs de débits (collecte par tranches de 5 minutes) et jusqu'à 400 Méga octets si on se contente de conserver les données pour la journée entière. Les pages générées quotidiennement occupent jusqu'à 150 Méga octets par jour, et les récapitulatifs mensuels environ 350 Méga octets chaque mois. La génération de ces pages nécessite entre un quart d'heure et une heure chaque jour.

[11] http://www.ietf.org/rfc/rfc3917.txt

Une nouvelle version du collecteur capable d'analyser les NetFlows au format v9 est en cours de développement. L'architecture de cette version est sensiblement différente de la précédente, elle repose sur l'utilisation de « threads » en lieu et place de processus. Nous espérons ainsi augmenter les performances du collecteur et en permettre le contrôle au fur et à mesure de son exécution, afin d'éviter par exemple d'avoir à l'arrêter pour prendre en compte une nouvelle configuration (nouveau routeur, nouvelle interface).

L'étape suivante consistera à intégrer le traitement des adresses IPv6, à documenter et à conditionner le produit de façon à permettre sa diffusion.

Bibliographie

[1] Alexandre SIMON, Network's METrology Une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus Dans *Actes du congrès JRES2001*, pages 37-49, Lyon, Décembre 2001.

[2] Sébastien MOROSI et Alexandre SIMON, netMET - Network's METrology De nouveaux besoins, de nouvelles fonctionnalités. Dans *Actes du congrès JRES2003*, pages 625-638, Lille, Novembre 2003.