netMET - Network's METrology
Une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus

Alexandre Simon

C.I.R.I.L : **C**entre **I**nteruniversitaire des **R**essources **I**nformatiques de **L**orraine
Rue du Doyen Roubault F - 54500 VANDOEUVRE

Tél : +33 (0)3.83.44.74.32
Fax :+33 (0)3.83.44.02.62
E-Mail : Alexandre.Simon@ciril.fr

Résumé

La métrologie ou plus précisément la mesure quantitative et qualitative des trafics présents sur les réseaux informatiques de l'Internet propose une connaissance exacte de l'utilisation et de l'évolution à venir de ces réseaux. Seulement, les réseaux informatiques ont évolué beaucoup plus vite que les solutions pour les mesurer : les technologies employées et les débits disponibles aujourd'hui posent de réels problèmes pour le développement de solutions de métrologie. Dans ce contexte, cet article présente une solution de métrologie générale appliquée aux réseaux régionaux, métropolitains et de campus s'appuyant sur la technologie propriétaire *NetFlow Cisco*. Cette solution, connue sous le nom de netMET – Network's METrology, est développée au CIRIL (Nancy) depuis novembre 1999. Elle est actuellement en production sur le réseau régional lorrain Lothaire mais également sur de nombreux autres réseaux de France. La solution peut être considérée aujourd'hui comme tout à fait homogène et opérationnelle, les résultats proposés donnent entière satisfaction et les évolutions et autres améliorations ne manquent pas. Tout au long de cet article nous tenterons d'expliquer les concepts et les mécanismes qui constituent la solution. Nous aborderons tous les points qui ont amené au développement de netMET en commençant par la problématique initiale, puis par une présentation de la technologie *NetFlow Cisco* et enfin par une description complète de l'architecture de la solution. Enfin nous terminerons par quelques informations spécifiques sur la disponibilité de netMET ainsi que par une présentation du groupe de travail qui utilise cette solution.

Sommaire

Introduction

L'évolution actuelle des réseaux de l'Internet tant au niveau des technologies que des débits s'accompagne de l'expression de nouveaux besoins et la métrologie, définie comme "l'art de mesurer", en fait partie intégrante. Le domaine de la métrologie et les solutions associées ne sont pas nouveaux contrairement au contexte dans lequel elles doivent s'appliquer. En effet, lévolution des réseaux et plus particulièrement ceux reliés àRenater rend difficile voir impossible l'utilisation des solutions proposées par le passé àbase d'écoute sur le réseau (machine ou sonde dédiées) ou de collecte sur matériels actifs (matériel réseau ou sonde). La solution netMET, qui sera étudiée dans cet article, est considérée comme une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus. Elle est une réponse aux problèmes posés par les solutions précédentes tout en proposant àla suite d'un déploiement simplifié un large spectre de fonctionnalités (métrologie, statistiques, consultation sur critères, sécurité, archivage) qui n'étaient pas aussi facilement disponible de par le passé.

Pour cet exposé nous commencerons par un petit retour en arrière pour bien comprendre d'où vient netMET : pourquoi et quels ont été les choix initiaux qui constituent aujourd'hui la solution de base. Puis, sans entrer dans les détails techniques et pour "séduire" le lecteur, nous ferons une description exhaustive des résultats proposés par netMET. La solution s'appuyant sur des informations de métrologie proposées par les routeurs Cisco, nous expliquerons d'une manière simplifiée la technologie *NetFlow* et le fonctionnement réel des routeurs de nouvelle génération. Ensuite nous aborderons la partie technique de netMET, àsavoir la description de l'architecture de la solution et son fonctionnement en décrivant les concepts généraux mais également certains mécanismes internes qui permettront de bien comprendre comment la solution s'articule. Et pour finir nous donnerons quelques informations complémentaires sur ce projet.

1. Un peu d'histoire : d'où vient netMET ?

Pour bien comprendre les choix et compromis qui ont été réalisés pour netMET, il nous paraît essentiel d'expliquer pourquoi et comment a émergé ce projet et quelles ont été ses grandes étapes.

Le réseau **Lothaire** (Le réseau **LO**rrain de **T**élécommunications à**H**aut débit pour les **A**pplications **I**nformatiques de la **R**echerche et de l'**E**nseignement supérieur) [lothaire] assure la connectivité *IP* pour les Universités de la Lorraine entre elles et vers l'Internet ; la connexion vers l'Internet se faisant via Renater (**Re**seau **Na**tional de télécommunications pour la **T**echnologie, l'**E**nseignement et la **R**echerche) [renater].

En tant qu'exploitant du réseau régional, le CIRIL [ciril] souhaite mesurer le trafic du lien entre Lothaire et Renater. Le souhait d'obtenir de telles informations n'est plus àjustifier, surtout pour un exploitant régional qui pourra y retrouver les tendances d'utilisation et d'évolution de son réseau et les éventuels problèmes de sécurité qui pourraient apparaître.

La Figure 1 illustre l'arrivée du service *IP* de Renater1 (Renater phase 1) jusqu'àa oût 1999 sur le réseau régional Lothaire.

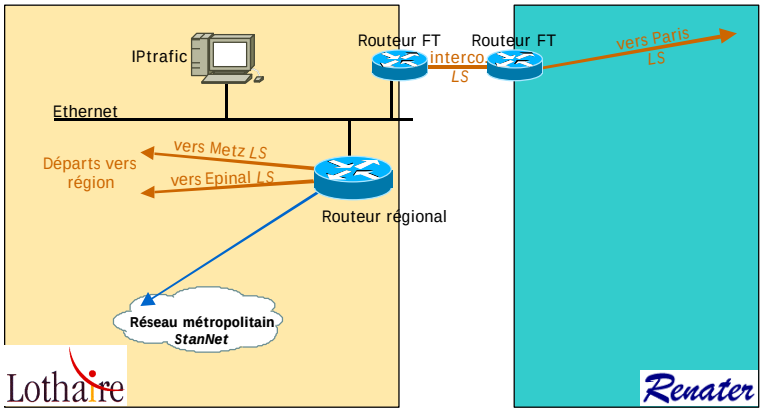


Figure 1 : Arrivée Renater1 sur Lothaire

Durant cette première phase, l'interconnexion entre Renater et les réseaux régionaux de France étaient généralement réalisée par des liens *Ethernet* ou un anneau *FDDI*. Le fonctionnement de ces technologies avec leur principe de diffusion permet à des solutions telle que IPtrafic [iptrafic] de se mettre en écoute sur le réseau (carte réseau en mode *promiscious)*, de reconstruire tous les paquets et enfin de réaliser la métrologie voulue sur les informations collectées. C'est ainsi qu'IPtrafic a été utilisé au CIRIL pour réaliser la métrologie du lien vers Renater durant cette période.

La migration vers Renater2 en août 1999, illustrée par la Figure 2, avec l'utilisation de la technologie *ATM* et l'augmentation des débits a rendu l'utilisation de solutions à base d'écoute impossible.

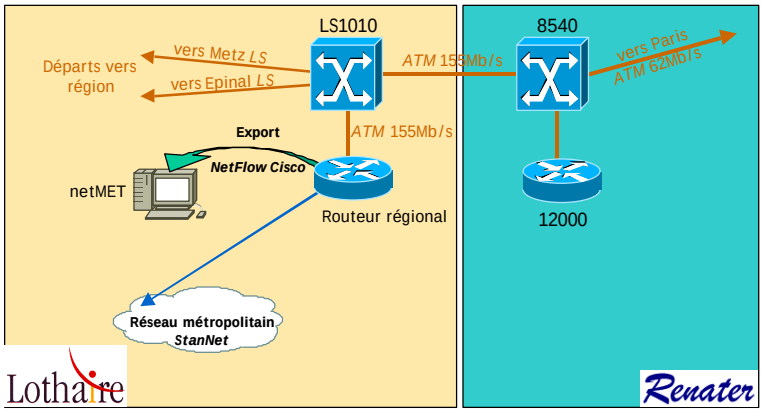


Figure 2 : Arrivée Renater2 sur Lothaire

En effet dans cette architecture, il n'existe plus de brin *Ethernet* unique sur lequel passe tout le trafic en source/destination de Renater. De plus, les débits d'interconnexion étant beaucoup plus élevés que par le passé, le trafic à collecter devient ingérable par une solution d'écoute logicielle simple. Avec ces remarques, on comprendra assez aisément qu'il devient très difficile de déployer une station d'écoute unique sur le réseau.

A partir de ce moment, le CIRIL n'avait plus aucune métrologie fine sur le trafic du lien Renater. Bien sûr, l'utilisation d'outils tel que *MRTG* [mrtg] fournit des informations sur l'occupation de la bande passante mais la pertinence de ces informations est loin d'être suffisante. En septembre 1999, il a donc été décidé au sein du CIRIL d'effectuer une expertise des solutions de métrologie disponibles sur le marché.

L'objet de cette étude était avant tout de trouver la solution logicielle ou matérielle qui permettrait **d'obtenir les informations de base** pour réaliser la métrologie voulue sur le plus grand nombre de topologies réseaux différentes. C'est en effet les informations de base qui sont difficiles à obtenir alors que la faisabilité de l'exploitation de ces informations pose moins de problème.

Dans l'architecture présentée Figure 2, les nœuds de concentration dans lesquels transite tout le trafic en source/destination de Renater sont le switch régional *ATM LS1010,* le routeur régional et la fibre entre les deux commutateurs *ATM*. Dans ce cas, si l'on souhaite mesurer le trafic du lien Renater il y a essentiellement deux solutions :

1. réaliser les mesures directement dans la fibre d'interconnexion entre le *LS1010* et le *8540* à l'aide d'une sonde par exemple
2. réaliser les mesures à partir des matériels de concentration

Dans ce contexte, nous avons expertisé et comparé pendant près de deux mois (de septembre à novembre 1999) cinq solutions différentes : IPtrafic, une équivalence d'IPtrafic en *ATM*, une solution à base de *MIB RMON2* embarquée, une sonde *ATM* [netscout] et *NetFlow Cisco* [netflow]. Les Figure 3 et Figure 4 font apparaître la synthèse et les conclusions des travaux réalisés durant cette expertise. Sur la Figure 3 nous réalisons un comparatif entre les différentes solutions sur un certain nombre de points qui nous paraissent essentiels. La Figure 4 quant à elle apporte quelques points complémentaires sur chaque solutions qui ne pouvaient pas être classifiés/comparés dans le document de synthèse.

				IPtrafic	Equiv. Iptrafic en *ATM*	*MIB RMON2* embarquée	Sonde *ATM*	NetFlow Cisco
Avantages / Inconvénients	Solution **L**ogicielle / **M**atérielle			L	L	M	M	M
	Indépendance collecte / matériel actif			oui	oui	non	non	non
	Maîtrise de la solution			oui	oui	partielle	partielle	partielle
	Simplicité de la solution			-	--	+	+	++
	Complétude des informations founies			+	+	--	++	++
	Facilité de mise en place			+	+	-	-	++
	Nécessité de puissance de calcul importante	Collecte		oui	oui	oui	non	non
		Exploitation		oui	oui	oui	oui	oui
	Développement à effectuer	Collecte		oui	oui	non	non	non
		Exploitation		oui	oui	oui	option	option
	Solution adaptée aux topologies récentes			--	-	+	+	++
Coût	Coûts incompressibles	Développement		oui	oui	oui	oui	oui
		Matériel(s) spécifique(s)		non	non	carte / logiciel	sonde	routeur
		Machine(s) dédiée(s)	Collecte	oui	oui	non	non	non
			Exploitation	oui	oui	oui	oui	oui
Etat	Adapté aux besoins CIRIL / Lothaire			--	+	-	+	++
	Choix àpriori envisageable			non	non	non	oui	oui

Légende :	
++	avantage
--	inconvénient

Figure 3 : Comparatif des solutions existantes

	Remarques particulières
IPtrafic	Pas de mesure d'*ATM* en natif Abandonné depuis migration vers Renater2 en juillet-août 1999 Non adapté aux topologies récentes Faisabilité sur les réseaux hauts débits actuels ?
Equiv. Iptrafic en *ATM*	Possibilité de mesure d'*ATM* en natif Compléxité du portage sur *ATM* Faisabilité sur les réseaux hauts débits actuels ?
***MIB RMON2* embarquée**	Utilisation des matériels actifs au coeur/périphérie du réseau Pas de mesure d'*ATM* en natif Charge de matériels actifs Manque d'informations de base Pas disponible sur tous les matériels actifs
Sonde *ATM*	Possibilité de mesure d'*ATM* en natif Exploitation logicielle peu adaptée au besoins CIRIL / Lothaire Matériel + logiciel = 200KF Peut être trop d'informations ? Pas toujours déployable sur les topologies complexes Solution propriétaire constructeur sonde Possibilité d'accès en *SNMP*
NetFlow Cisco	Utilisation des matériels actifs au coeur/périphérie du réseau Pratiquement déployable sur toutes les topologies Solution propriétaire constructeur Cisco Disponible sur la plupart des matériels (routeurs et switchs/routeurs) Activation très facile Pas de référence sur : charges matériels, quantités, ...

Figure 4 : Comparatif des solutions existantes - remarques particulières

A la suite de cette expertise, seulement deux solutions étaient àpriori envisageables : une solution à base de sonde *ATM* ou une solution àbase de *NetFlow Cisco*. C'est la technologie *NetFlow Cisco* qui a été retenu comme solution de base pour réaliser la métrologie sur Lothaire, essentiellement pour les points suivants :

1. *NetFlow Cisco* est plus facilement déployable sur un grand nombre de topologie réseau
2. les informations collectées sont plus facilement exploitables
3. le coût du déploiement est plus faible
4. il est possible d'utiliser les matériels actifs déjàprésents sur le réseau (routeurs)

Pour l'exploitation des informations envoyées par les routeurs implémentant *NetFlow*, Cisco propose un collecteur et un analyseur. Seulement, ces solutions ne sont disponibles que sur des plate-formes *Sun* spécifiques et aux vues des fonctionnalités proposées pour l'analyse, nous savions que ces outils ne rempliraient pas le cahier des charges établi en interne. C'est pour ces raisons qu'il a été décidé de

développer une solution propriétaire au CIRIL, nous permettant d'avoir une maîtrise complète sur le développement et sur les fonctionnalités à implémenter. A partir de novembre 1999, nous avons donc commencer à développer un embryon de collecteur *NetFlow* tout en validant étape par étape la faisabilité de la solution. Par la suite le projet suivit son cours et les grandes étapes sont récapitulées dans le tableau ci-dessus.

Juillet-Août 1999	Passage à Renater2 pour le réseau régional Lorrain Lothaire sur *ATM* et donc impossibilité de continuer à utiliser IPtrafic pour réali ser de la métrologie régionale. → Plus de métrologie sur Lothaire
Septembre 1999	Décision du CIRIL et de son équipe réseau de réaliser une expertise des solutions de métrologie disponibles sur le marché. → Expertise menée par Alexandre Simon
Novembre 1999	Choix de la technologie *NetFlow Cisco* comme information de base pour réaliser de la métrologie. Décision du CIRIL et de son équipe réseau de développer une solution de métrologie pour ses réseaux métropolitains et régional par rapport à un cahier d es charges initiale. → Tests de faisabilité et écriture du premier collecteur netMET
Janvier-Février 2000	Tests de faisabilité du collecteur ok... Exploitation en perl ok... → netMET 1.0 en production au CIRIL
31 janvier 2000	Présentation de la solution de métrologie netMET à la communauté Renater (groupe de travail métrologie : *wgqos*) au GIP Renater. → Décision de rendre disponible netMET pour les autres régions et réseaux de France.
26 avril 2000	Présentation au CIRIL - Nancy du fonctionnement, de l'installation et de la configuration de la solution netMET aux premiers utilisateurs. → Création du "*Groupe de travail netMET*" (WG-netMET) → Mise à disposition de la première version distribuable : netMET 2.0
Juin 2000	Stagiaire CIRIL : **Peyman Gohari**, pour travailler sur netMET et son approche sécurité. → Ecriture de l'outil de recherche multi-critères *netMET LookUp* → Premières bases pour *détection de scans*
Septembre-Octobre 2000	Nouvelles versions de *netMET* 2.1 puis très rapidement 2.2 : métrologie, statistiques et sécurité (collecte + *nmlookup*) → version non-officielle mais installée par téléphone dans plusieurs régions.
Novembre-Février 2001	Modification et amélioration de la version 2.2 vers la version 2.3 plus performante. → mise à jour des versions dans les régions
Février 2001	Ecriture d'un outil pour obtenir une évaluation du coût de la métrologie (nb de flows, quantité octets, charge routeur, ...) → *metaMET* : combien coûte le *NetFlow Cisco*
Février-Mai 2001	Rédaction des documentations : "Installation de la distribution netMET - Mise à jour système et installation" "Collecteur & fichier de configuration *netmet.conf*" Création du domaine : netmet-solutions.org Réécriture du web de netMET Etude et écriture de la Licence netMET et des conditions d'accès à netMET Préparation pour le basculement du web et *mailing-list* sur nouveau domaine. Modification et amélioration de la version 2.3 vers la version 2.4beta.
Juin 2001	Stagiaire CIRIL : **Cyril Proch**, pour travailler sur netMET et son approche sécurité. Suite du stage de Peyman Gohari avec les orientations *détection de scans*, création et détection de problèmes de *sécurité sur profils* et métrologie orientée *matrice de flux intra-réseaux*...
Septembre-Octobre 2001	Basculement du web et *mailing-list* sur nouveau domaine netmet-solutions.org Nouvelles versions collecteur (2.4) et exploitation (1.1) pour mise à disposition distribution 1.1_2.4
19-20 Novembre 2001	Formation mise en œuvre technique de netMET. Formation CIREN - Montpellier
13 décembre 2001	Présentation netMET au JRes2001, Lyon. " *netMET - Network's METrology* : Une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus." Alexandre Simon

Figure 5 : Les grandes dates du projet netMET

2. Les outils et informations proposées par netMET

Avant de rentrer dans toutes considérations techniques et pour bien cerner l'intégralité du projet netMET, il semble intéressant de faire une description exhaustive des outils et des informations proposées par netMET.

Le projet netMET est aujourd'hui mené autour de deux voies de développement :

1. le **collecteur netMET** de datagrammes *UDP NetFlow Cisco*
2. l'**exploitation netMET** des informations collectées

La **distribution netMET**, quant àelle, regroupe ces deux voies de développement, ainsi :

- le collecteur netMET reste utilisable sans l'exploitation (collecte simple dans des fichiers binaires)
- l'exploitation ne peut fonctionner qu'avec les données fournies par le collecteur netMET

La Figure 6 propose l'organisation du projet netMET, y apparaissent également les fonctionnalités et informations proposés par chaque éléments constituants la solution.

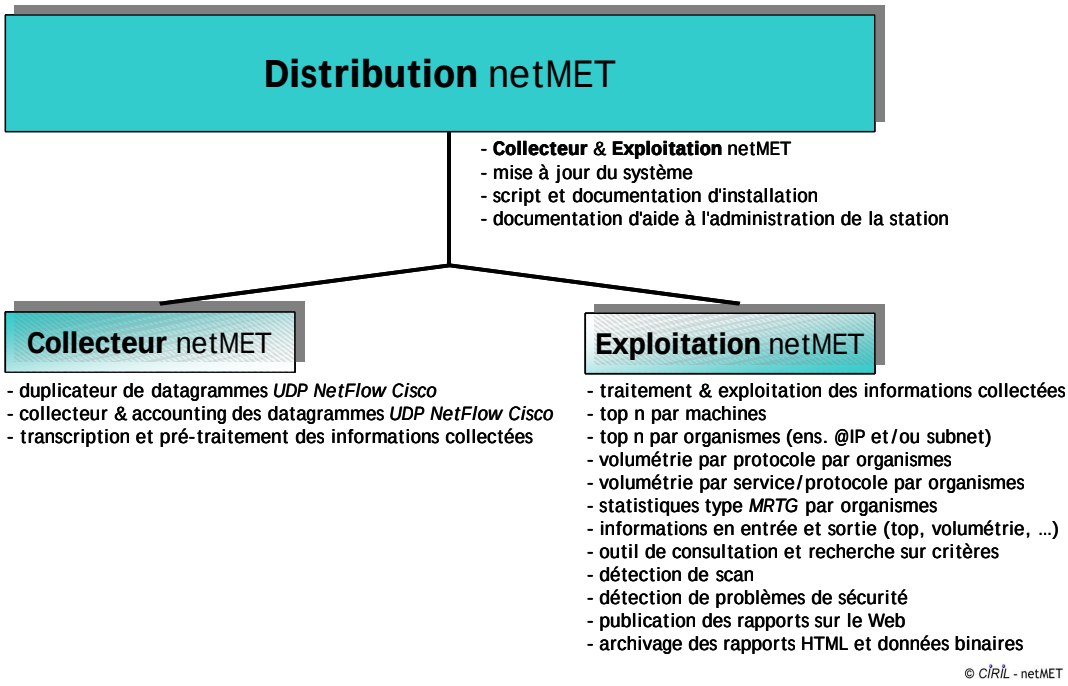


Figure 6 : Le projet netMET, fonctionnalités et informations proposées

Pour compléter la description précédente, quelques points particuliers peuvent être notés :

- le collecteur netMET est dit "générique" et reste utilisable pour d'autres problématiques que pour "l'exploitation netMET"
- l'exploitation netMET est orientée : mesure d'un réseau régional, métropolitain ou de campus vers un réseau fédérateur (Renater par exemple) connecté par un lien unique (cf. Figure 7), mais elle peut être facilement dérivée et adaptée pour d'autres problématiques.

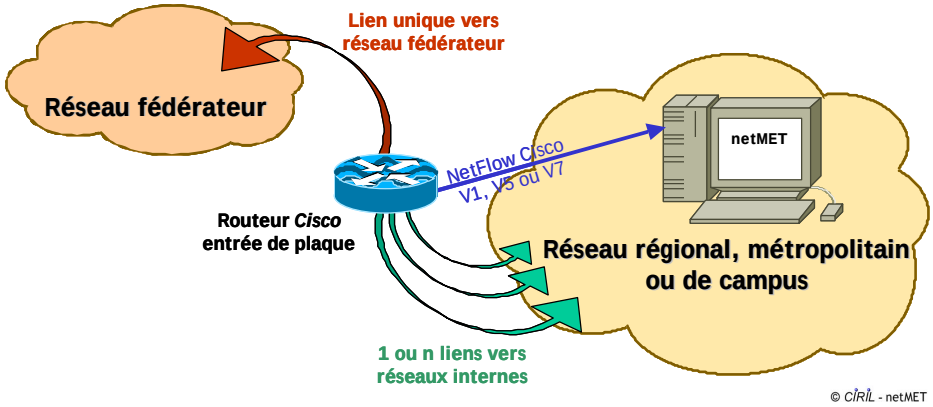
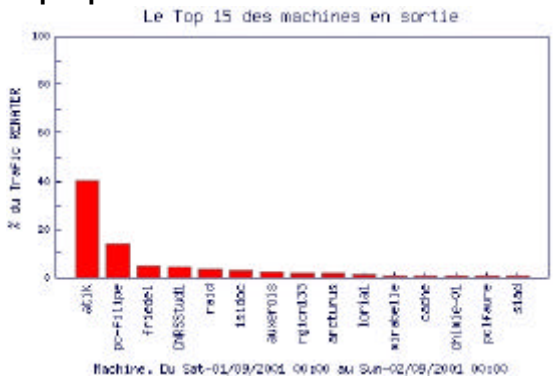


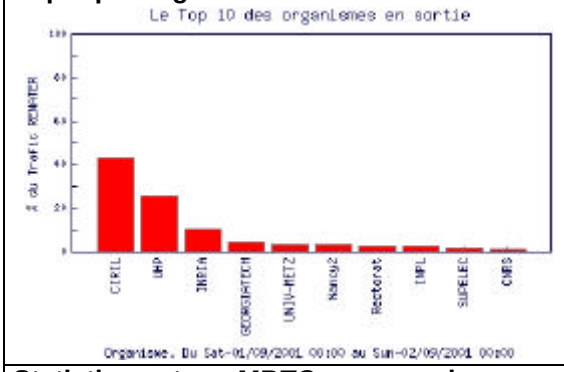
Figure 7 : Schéma typique d'utilisation de l'exploitation netMET

La Figure 8 fait apparaître quelques images et captures d'écrans des informations disponibles via le web d'un serveur faisant fonctionner netMET.

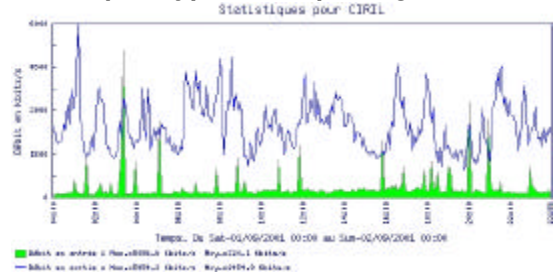
Top n par machines



Top n par organismes



Statistiques type *MRTG* par organismes



Volumétrie par protocole par organismes
Volumétrie par service/protocole par organismes

Métrologie détaillée pour CIRIL vers RENATER
Total de CIRIL vers RENATER : 26.6 Go

Métrologie par protocoles

Protocole	Cumul (octets)	Cumul (%)
tcp (6)	26.5 Go	99.71
udp (17)	66.5 Mo	0.25
icmp (1)	11.9 Mo	0.04

Métrologie par services/protocoles

Service/Protocole	Cumul (octets)	Cumul (%)
UNKNOWN/tcp (65535/6)	15.3 Go	57.48
ftp-data/tcp (20/6)	9.0 Go	33.82
ntp/tcp (119/6)	1.0 Go	3.82
radacct/tcp (1813/6)	521.8 Mo	1.96
www/tcp (80/6)	519.6 Mo	1.95
domain/udp (53/17)	65.2 Mo	0.25
ftp/tcp (21/6)	33.7 Mo	0.13
icp/tcp (3130/6)	28.0 Mo	0.11
pop3/tcp (110/6)	21.6 Mo	0.08

Détection de scan

Liste des scans en largeur:

	Machine source	Machine destination	Horaires	Nb services
1	toto.orgat.fr (192.168.200.254)	61.103.90.22	10:00	345
2	61.103.90.22	toto.orgat.fr (192.168.200.254)	10:00	347
3	tata.orga2.fr (192.168.144.16)	suspect1.mal intentionne.fr (122.203.45.21)	12:30	312
4	suspect2.mal.intentionne.fr (122.213.85.150)	www.machine1.fr (192.168.156.53)	13:40	441
5	www.machine1.fr (192.168.156.53)	suspect2.mal.intentionne.fr (122.213.85.150)	13:40	681
6	192.168.51.233	202.58.198.58	14:50	6521

Liste des scans en hauteur:

Machine source : 172.10.0.87

	Réseaux	Organismes	Horaires	Nb machines scannées	Services scannés	Nb réponses
1	192.168.208.0	"ORGA1"	12:40-12:50	216	[111/s]	0
2	192.168.209.0	"ORGA1"	12:40-12:50	216	[111/s]	1
3	192.168.210.0	"ORGA2"	12:40-12:50	211	[111/s]	0
4	192.168.224.0	"ORGA2"	12:40-12:50	190	[111/s]	0
5	192.169.35.0	"ORGA1 ORGA2"	12:50-13:00	192	[111/s]	0
6	192.169.137.0	"ORGA1"	12:50-13:00	224	[111/s]	1
7	192.170.115.0	"ORGA3"	12:50-13:00	197	[111/s]	1
8	192.170.118.0	"ORGA3"	12:50-13:00	226	[111/s]	1
9	192.170.254.0	"ORGA4"	13:00-13:10	240	[111/s]	12

Outil de consultation et recherche sur critères

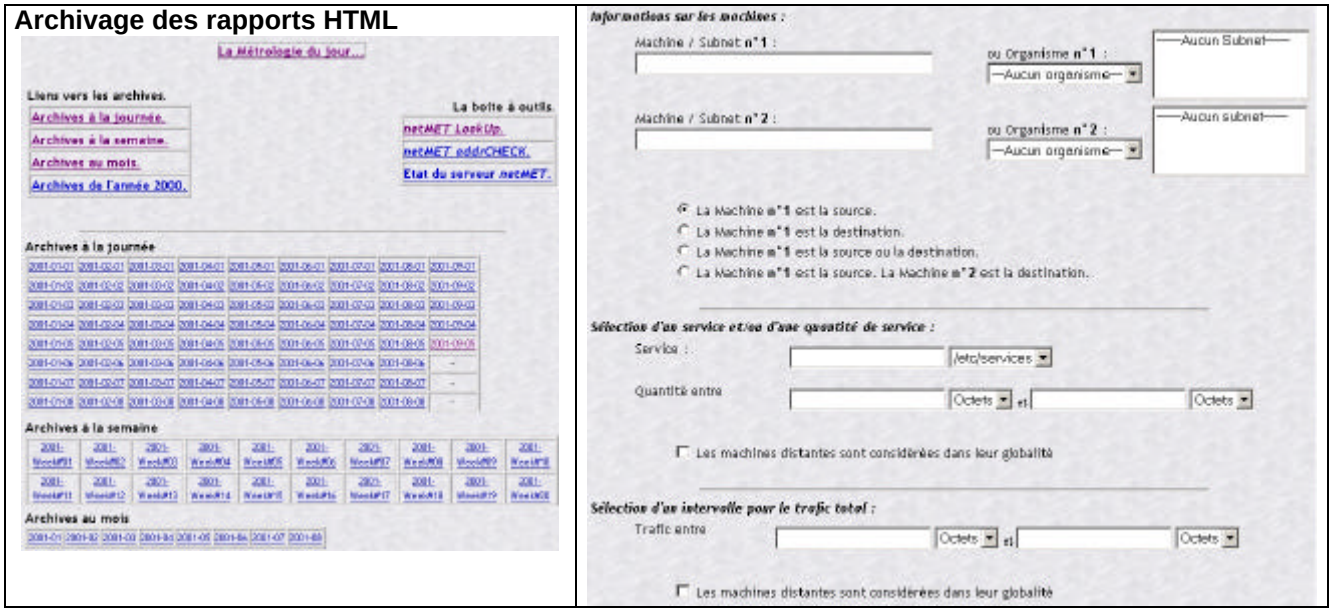


Figure 8 : Informations proposées par l'exploitation netMET

3. Routeurs et technologie *NetFlow Cisco*

Pour bien saisir toute la problématique de la solution de métrologie netMET, il faut impérativement comprendre la technologie et les mécanismes sur lesquels s'appuie cette solution. La technologie *NetFlow Cisco* [netflow] et les informations qu'elle propose sont la base de netMET. Il semble donc important de :

- comprendre le "pourquoi" de cette technologie
- comprendre son fonctionnement et ses mécanismes.

3.1. La technologie *NetFlow Cisco* - Pourquoi ?

Il apparaît clairement aujourd'hui que les goulets d'étranglement des liens de l'Internet se situent essentiellement au niveau des routeurs. Effectivement, les débits, les services et le nombre de machines présents sur l'Internet augmentent et complexifient les paquets à acheminer et de ce fait, ils augmentent et complexifient les opérations à réaliser par les routeurs.

Il n'est plus raisonnable de penser que les routeurs puissent fonctionner dans un mode de routage "classique" dans lequel chaque paquet à acheminer est analysé puis routé selon les informations contenues dans une table de routage. Le nombre de paquets et la taille des tables de routage étant assez considérables, les routeurs ne peuvent plus traiter tous les paquets dans un temps satisfaisant, ce qui peut impliquer des temps de réponses médiocres et parfois même des pertes de paquets.

Dans ce contexte on comprend bien que des efforts considérables ont été réalisés pour trouver des solutions permettant de "soulager" ces routeurs. Des solutions existent aujourd'hui et *NetFlow* en fait partie, mais tout n'est pas encore implémenté et d'autres travaux sont en cours.

3.2. Principe

Le *NetFlow* n'est qu'une **technologie** et pas un **mécanisme**, qui définit un **processus général** qui sera mis en oeuvre par différents mécanismes. *NetFlow* est embarqué dans les routeurs (ex. 7200, 3640, ...) et switch-routeurs (ex. 5500, 6000, ...). Il fait généralement partie intégrante du système d'exploitation du matériel (*IOS*) et fonctionne en **natif** (= ce n'est pas un *plug-in* ajouté !).

NetFlow peut être défini comme un **mécanisme d'accélération du routage** grâce au passage du routeur d'un mode "classique" de **forwarding** (routage) à un mode "accéléré" de **switching** (commutation). Cette technologie permet également, au travers des données de flux qu'elle manipule, de proposer des informations de métrologie assez détaillées sur les flux qui ont traversés le routeur. Ce sont sur ces informations que s'appuie netMET pour obtenir les données de métrologie.

3.3. La notion de flux (*flow*)

La notion de flux commence à être bien connue dans le domaine des réseaux, car c'est une entité qui est assez couramment manipulée dans différents domaines : ex. *QoS*, qualification de trafic, filtrage (*ACL*), ... Cette notion est étroitement liée au protocole *IP* et plus particulièrement dans notre cas à la version *v4* de *IP*.

Un flux est *unidirectionnel* et est définit par le *n-uplet* suivant :

- **@*IP* source** - **@*IP* destination**
- **protocole** (*ICMP, TCP, UDP, GRE, RSVP*, ...)
- **port source** - **port destination** (80/tcp, 20/tcp, 53/udp, ...)
- **interface entrée** - **interface sortie**
- **champ TOS**

3.4. Fonctionnement et mécanismes dans un routeur *NetFlow*

Pour bien expliquer *NetFlow*, nous allons prendre un cas d'école :

- une communication entre une machine A et C pour un même flux donné
- A et C étant sur deux réseaux différents, obligeant à passer au travers d'un routeur
- nous ne nous intéresserons qu'aux deux premiers paquets de ce flux :
  - le paquet initial
  - et le suivant.

Ce cas d'école est traité dans le cas du routage classique par la Figure 9 et dans le cas du routage accéléré par les Figure 10 et Figure 11.

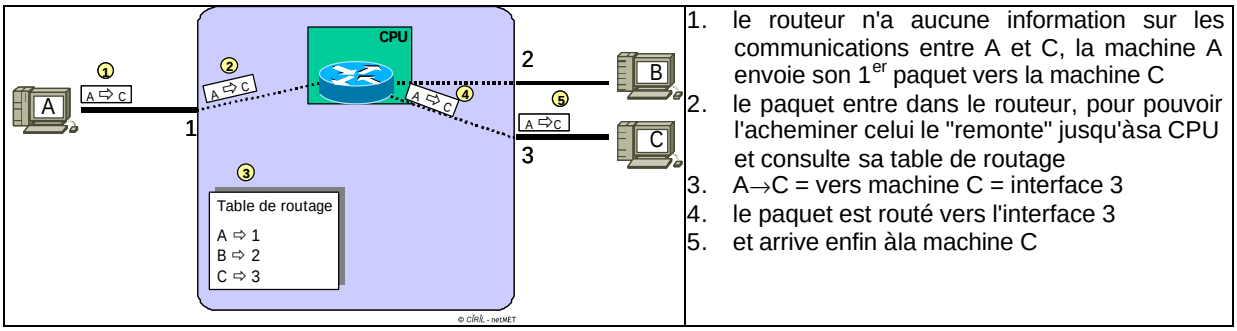
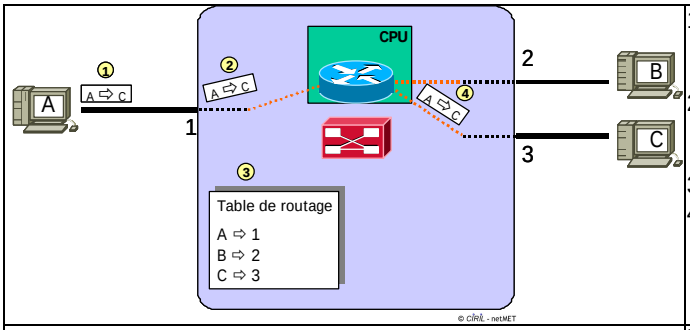


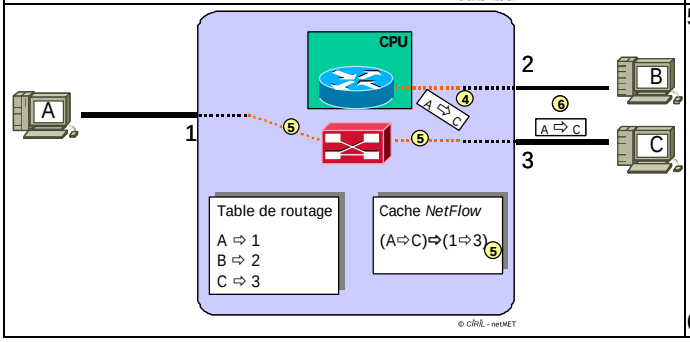
Figure 9 : Routage classique, 1er et 2ème paquets

Dans le cas du 2ème paquet le processus est exactement le même, c'est à dire qu'il y a "remontée" du paquet à la CPU et consultation de la table de routage pour l'acheminement vers l'interface 3.

Il n'est donc pas difficile de comprendre que c'est dans ce cas de figure que le routeur perd énormément de temps à décoder et à consulter sa table de routage pour chaque paquet. Intuitivement on pourrait se dire que pour le 2ème paquet et les suivants toutes ces consultations ne sont plus obligatoires car le routeur connaît (dès le 1er paquet) l'existence de ce flux entre A et C (= flux entre interfaces 1 et 3). Cette dernière observation donne les bases du fonctionnement du *NetFlow*...

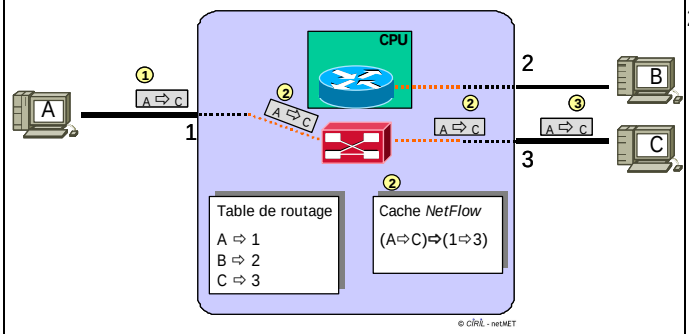


1. le routeur n'a aucune information sur les communications entre A et C, la machine A envoie son 1er paquet vers la machine C
2. le paquet entre dans le routeur, pour pouvoir l'acheminer celui le "remonte" jusqu'àsa CPU et consulte sa table de routage
3. A→C = vers machine C = interface 3
4. le paquet est routé vers l'interface 3



5. le routeur crée dans son **cache *NetFlow*** une nouvelle entrée pour le flux de A vers C qu'il vient de détecter. Cette entrée spécifie qu'il existe un flux entre la machine A et C et que tous paquets appartenant à ce flux doivent être acheminés de l'interface 1 àl'interface 3. De même, le routeur va programmer de façon ***hardware*** l'acheminement de ce flux entre ces 2 interfaces (basculement des liens rouges de la CPU vers un module de *switching*)
6. le paquet arrive enfin àla machine C

Figure 10 : Routage accéléré, 1er paquet



1. le routeur connaît l'existence du flux entre la machine A et C au travers de son **cache *NetFlow***, la machine A envoie son 2ème paquet vers la machine C
2. avant de consulter sa table de routage, pour acheminer les paquets, le routeur consulte son **cache *NetFlow*** pour savoir si le paquet n'appartient pas à un flux déjà existant. Ici c'est le cas, le paquet ne "remonte" pas jusqu'à la CPU mais prend le chemin *hardware* qui a été programmé précédemment et est donc acheminé directement vers l'interface 3. On ne peut pas dire que le paquet est été **routé** car il n'y a pas eu consultation de la table de routage, mais plutôt qu'il a été **commuté** par un mécanisme *hardware* plus rapide que le routage.
   C'est de la **commutation de niveau 3**.
3. le paquet arrive enfin àla machine C

Figure 11 : Routage accéléré, 2ème paquet

Le principe du *NetFlow* est assez simple et assez intuitif : pour gagner du temps globalement sur un flux de plusieurs paquets *IP* il faut :

- perdre un peu de temps sur le 1er paquet pour construire les structures de données et mettre en place tous les mécanismes nécessaire àl'accélération,
- puis s'appuyer sur ces mécanismes simplifiés et très performants (*hardware*) pour accélérer les paquets suivants.

Le nombre d'étapes dans chaque cas de figure est assez explicite : une fois le routage accéléré programmé, le transit dans le routeur coûte trois étapes, alors que le routage classique coûte toujours cinq étapes àchaque paquets.

Globalement, le *routage accéléré* permet bien de gagner du temps, même si localement son fonctionnement est plus compliqué (et plus long) que le *routage classique*.

3.5. Cache *NetFlow* et informations de métrologie

Le contenu et la granularité des informations gérées dans le cache *NetFlow* rendent possible la déduction d'informations de métrologie sur les flux qui ont traversé le routeur. Ces informations de métrologie sont très fines et qualifient entièrement tous les flux qui ont été détectés par le routeur. L'accès à ces informations, une fois les flux **relâchés** (communication terminée = fin de flux → flux relâché), se fait par exportations de datagrammes *UDP* par le routeur vers une machine qui collectera et exploitera ces données. L'invalidation (relâchement d'informations) du cache *NetFlow* et l'exportation sont illustrées par la Figure 12.

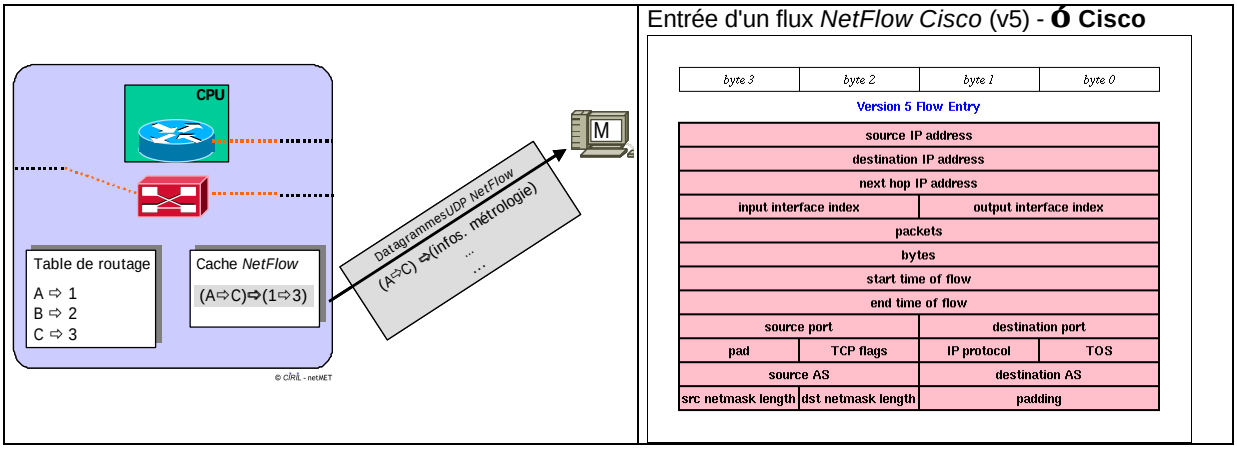


Figure 12: Invalidation du cache *NetFlow* et informations de métrologie (version 5)

4. Architecture et fonctionnement de la solution

Comme nous l'avons vu précédemment, la solution netMET est disponible sous forme d'une **distribution** qui regroupe le **collecteur** netMET et l'**exploitation** des informations collectées. Pour comprendre l'intégralité de la solution, nous allons détailler comment s'articulent ces éléments entre eux et quels sont leurs fonctionnements internes.

4.1. Architecture générale

Le fonctionnement de netMET est assez simple, pour l'expliquer nous allons suivre les flux *NetFlow* provenant des routeurs jusqu'àla publication des résultats sur le web. La Figure 13 donne le cheminement de ces flux au travers de la solution :

1. les flux *NetFlow* sont envoyés depuis 1 ou n routeur(s) et/ou 1 ou n duplicateur(s) (la notion de duplicateur de flux sera expliquée plus tard)
2. ces flux sont envoyés àdestination du collecteur netMET, qui se charge de les collecter et de les traiter pour en générer des fichiers binaires (image de la collecte)
3. àpartir de ces fichiers de collecte, la partie d'exploitation génère les résultats (pages *HTML* et images) pour les différentes informations proposées (TOP n, statistiques, métrologie détaillée, …) pour des périodes de 10 minutes, d'une journée, d'une semaine et d'un mois
4. et pour finir, tous ces résultats sont publiés sur le web.

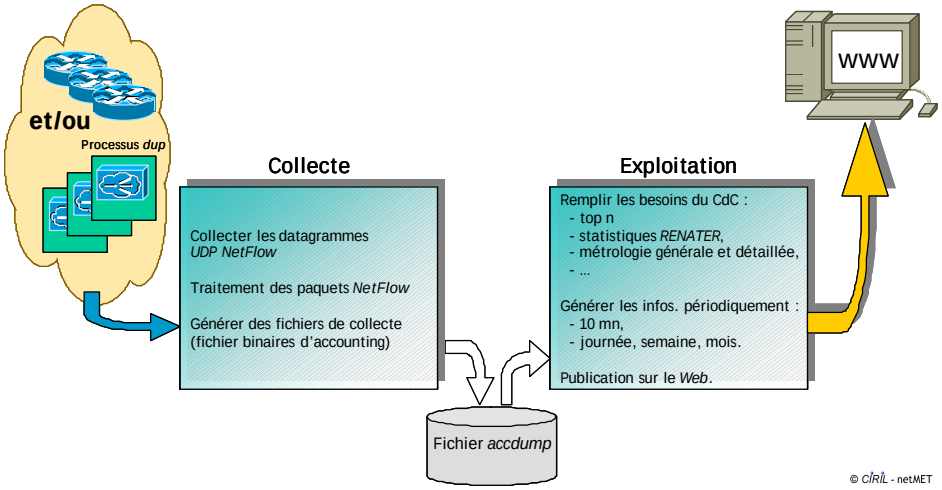


Figure 13 : Architecture générale

Au niveau de ces deux importantes parties, il est intéressant de noter que :

- la collecte
  - est la partie la plus critique
  - elle a été développée en langage *C*
  - elle fait l'objet d'optimisations fines
- l'exploitation
  - est la partie devant être la plus flexible possible
  - elle est développée en langage *Perl* pour les générations *HTML* et *images*
  - certaines parties nécessitant d'être rapides sont directement développées en langage *C*

4.2. Le duplicateur de flux : *netMETdup*

La programmation de l'exportation des flux *NetFlow* sur les routeurs Cisco ne peut se faire que vers une et une seule destination (= une seule machine de collecte). Cela pose un problème de fond, car dans ce contexte comment faire pour exporter vers plusieurs machines pour réaliser des tests ou pour faire des productions parallèles ? De plus netMET propose aujourd'hui plusieurs "point de vue" :

- collecte agrégée (absorption des @*IP* de l'Internet)
  - métrologie générale
  - statistiques Renater
- collecte non-agrégée (@*IP* de l'Internet visibles)
  - sécurité sur 10mn
  - sécurité sur 24h

avec des périodes d'échantillonnage différentes :

- 5mn : statistiques Renater
- 10mn : sécurité sur 10m
- 24h : métrologie générale, sécurité sur 24h

Ces "points de vue", avec l'agrégation ou la non-agrégation et les différentes périodes d'échantillonnage obligent à utiliser plusieurs collecteurs. En effet, à chaque "point de vue", appelé **service** dans la suite, sera associé un collecteur :

- métrologie générale : metro
- statistiques Renater : stats
- sécurité sur 10mn : secure10mn
- sécurité sur 24h : secure24h

Le problème posé par ces quatre collecteurs est que le routeur devrait être capable d'exporter vers quatre destinations différentes et même si à partir de la version 12.2(1)T de l' *IOS* Cisco, l'export vers deux machines devient possible, ce n'est pas encore assez. netMET apporte donc une solution logicielle (processus démon) qui permet de :

- programmer sur le(s) routeur(s) l'exportation des flux *NetFlow* uniquement vers le duplicateur
- le duplicateur reçoit ces datagrammes sur son port d'entrée
- puis, duplique vers autant de machines/ports que souhaité

La Figure 14 illustre l'utilisation du duplicateur de flux *netMETdup* qui alimente les 4 services de la solution netMET (metro, stats, secure10m, secure24h) àpartir des flux provenant de 1 ou n routeur(s).

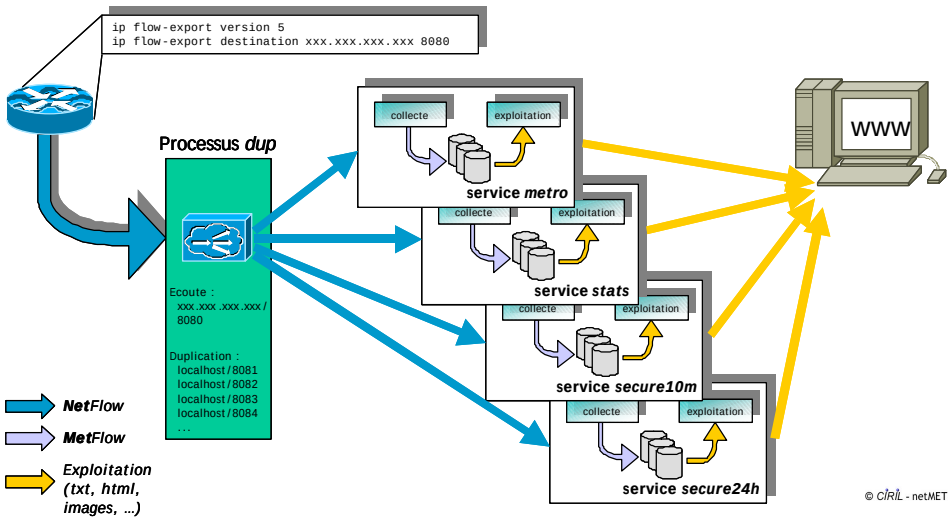


Figure 14 : Le duplicateur de flux *netMETdup*

4.3. La collecte et l'accounting : *netMETcll – netMETacc*

Le collecteur netMET est constitué de 2 processus :

- *netMETcll* : un processus de réception des paquets *UDP NetFlow* en provenance directe d'un routeur ou du duplicateur de flux de netMET (*netMETdup*).

netMETcll est capable :

- de décoder les paquets *NetFlow* selon les formats 1, 5 et 7
- de recevoir de paquets *NetFlow* en provenance de plusieurs routeurs ou duplicateurs différents
- d'exclure des flux reçus qui correspondent à une détection de flux "non souhaitée" pour la métrologie àappliquer (ce qui revient à pourvoir garder uniquement les flux qui intéressent)
- d'agréger "àla volée" tous les flux en provenance/destination d'une interface particulière du routeur avec une adresse *IP* symbolique ("virtuelle") : réalisation d'un "trou noir"

Une fois toutes ces opérations appliquées sur les flux *NetFlow* originels, *netMETcll* construit des **MetFlow** (qui sont en fait des *NetFlow* épurés avec application de règles précédentes) puis les passe au processus *netMETacc*.

- netMETacc : un processus d'accounting de **MetFlow** (MetFlow = flux de métrologie au sens netMET). *netMETacc* réalise l'accounting -c'est àdire la gestion de compteurs de métrologie dédiés- en temps réel en gérant en mémoire des structures de données plus ou moins complexes.

Le fonctionnement entre le processus *netMETcll* et *netMETacc* ainsi que la circulation des différentes informations mise en oeuvre sont illustrés par le schéma Figure 15.

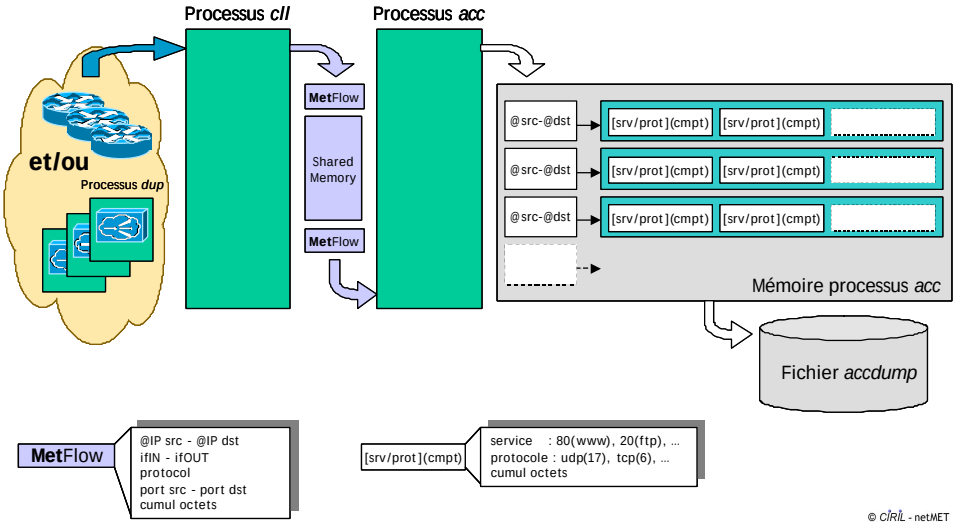


Figure 15 : Fonctionnement des processus *netMETcll - netMETacc*

4.4. Exploitation netMET et informations proposées

L'exploitation netMET est entièrement écrite en *Perl*, mais les fichiers de collecte étant sous forme binaire, nous utilisons l'outil de **transcription binaire/ascii** *netMETexp* pour pré-traiter les informations collectées et fournir à *Perl* une interface standard. Cet outil est la base de l'exploitation actuelle, mais son format de sortie standard autorise tous autres développements à partir des informations collectées par netMET. Le format de sortie standard et un exemple sont donnés Figure 16.

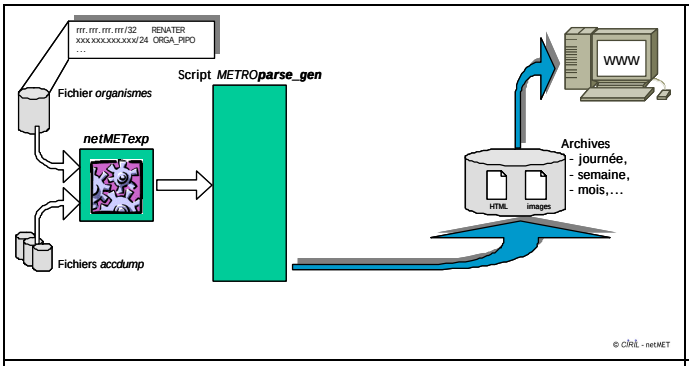
```
Format de sortie standard :
@IPsrc          @IPdst          [srv_1/prot_1](qo_1) [srv_2/prot_2](qo_2) … [srv_n/prot_n](qo_n)

où
   srv_i  = service (80=www, 20=ftp, …)
   prot_i = protocole (6=TCP, 17=UDP, …)
   qo_i   = quantité en octets


Exemple :
193.50.27.66    194.214.110.110 [53/17](7193) [65535/1](156) [137/17](1170)
193.50.27.68    195.220.197.100 [80/6](40)
194.214.110.110 194.214.217.34  [65535/1](280)
```

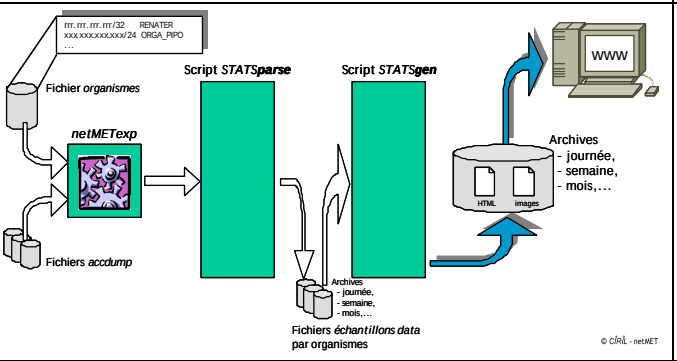

Figure 16 : Format de sortie de *netMETexp*

Les scripts *Perl* et le fonctionnement de l'exploitation pour les 4 services de netMET apparaissent Figure 17. L'utilisation d'un fichier de **déclaration d'organismes** autorise le regroupement d'ensembles d'adresses *IP* ou de *subnets* de classe sous un nom d'organisme et permet ainsi une métrologie par organismes (TOP n, statistiques, …).



Exploitation service metro

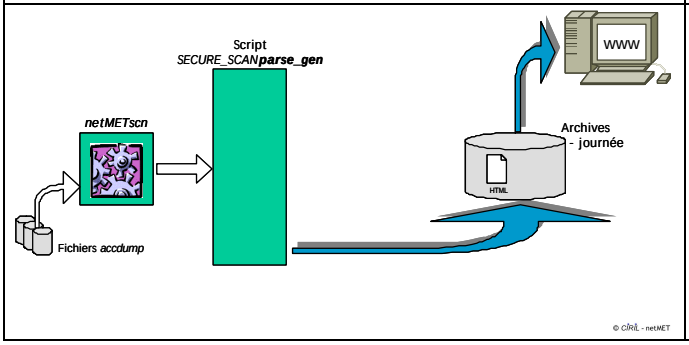
- TOP n par machines
- TOP n par organismes
- Métrologie détaillée par organismes (volumétrie par protocole et service/protocole)



Exploitation service stats

- Statistiques type *MRTG* par organismes

Remarque: passage par des fichiers d'échantillons intermédiaires de manière à accélérer le traitement pour les périodes semaines et mois.



Exploitation service secure10m et secure24h

- Détection de scans

Remarque: utilisation de l'outil *netMETscn* dédié au pré-traitement en langage *C* pour la détection de scans (perfomances). Format de sortie standard similaire à *netMETexp*.

Figure 17 : Scripts et exploitation netMET

netMET LookUp ne fait pas réellement partie de l'exploitation générale de netMET car cet outil ne publie aucune information de manière automatique, mais est utilisable de façon ponctuelle. netMET LookUp est définit comme un "outil de recherche multi-critères". L'idée de base est lancer des *grep* évolués dans les fichiers de collecte de manière à répondre rapidement à "y a t -il un réel problème ?". L'application est assez simple, au travers d'un formulaire web on va pouvoir :

- choisir un fichier de recherche (agrégé ou non, période)
- choisir une machine source, destination, source et ou destination
- choisir un service/protocole
- choisir une quantité
- …
- et lancer la requête sur le fichiers sélectionnés.

netMET LookUp ne peut pas résoudre tous les problèmes ou répondre à toutes les questions mais il permet plutôt d'exprimer des requêtes quotidiennes simples (et parfois même compliquées) pour une première approche sécurité.

5. Informations complémentaires

5.1. Linux et netMET

La distribution netMET n'est disponible aujourd'hui que pour **Linux** (compilation des binaires). netMET n'est théoriquement lié à aucune distribution Linux particulière mais les distributions Redhat et Mandrake ont largement été validées et sont de ce fait préconisées pour l'installation. La distribution Debian est en cours de validation.

La distribution netMET, une fois installée et configurée, demande peu de maintenance. netMET est d'ailleurs aujourd'hui reconnu pour être facilement installable et très cohérent en exploitation grâce à son déploiement (cohérence des noms de scripts, activation des *crons*, reprise sur fichier après arrêt, ressources et fichiers de configurations bien localisés) et à sa création d'arborescences hié rarchisées.

5.2. Groupe de travail netMET : *WG netMET*

netMET regroupe aujourd'hui une petite communauté d'utilisateurs qui participent à ce projet en utilisant netMET sur leur réseau et en communiquant sur la mailing-list dédiée à cette solution. netMET est à ce jour en production à :

- Nancy, CIRIL
- Paris, Campus Jussieu
- Rouen, CRIHAN, CORIA
- Angers, GEDOR
- Lyon, CISR
- Grenoble, CICG
- Montpellier, CINES, LIRMM
- Toulouse, CICT

D'autres sites sont actuellement en phase de test ou souhaitent déployer, à court ou moyen terme, netMET sur leur réseau.

A noter que d'autres personnes s'investissent dans des développements autour de netMET pour compléter ou améliorer les fonctionnalités proposées de base par la solution. Un bon exemple est l'approche netSEC [netsec] développé par Bernard MARTINET et son équipe – CICG, Grenoble. Le développement de netSEC est en fait en approche sécurité à base de base de données alimentées par les fichiers de collecte de netMET. Les premiers résultats de netSEC sont tout à fait prometteurs et confirment bien que l'on peut traiter des problèmes de sécurité en s'appuyant sur des données issues de la métrologie.

Je tiens tout particulièrement à remercier toutes les personnes qui participent à ce projet sans qui netMET ne serait pas la solution que l'on connaît aujourd'hui. La confiance et le soutient de chacun a toujours été très moteur et motivant pour faire avancer la solution dans le bon sens.

5.3. Contacts

Voici une liste des différents contacts pour la solution de métrologie netMET :

- web : http://www.netmet-solutions.org
- mail : netmet@netmet-solutions.org
- mailing-list : netmet-list@netmet-solutions.org (sous Sympa, pour l'inscription se reporter à http://www.netmet-solutions.org/support/abonnement.html)

Références

[lothaire] : http://www.lothaire.net
[renater] : http://www.renater.fr
[ciril] : http://www.ciril.fr
[iptrafic] : http://www.urec.cnrs.fr/iptrafic/
[mrtg] : http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
[netscout] : http://www.netscout.com/products/probes.htm
[netflow] : http://www.cisco.com/go/netflow
[netsec] : Bernard MARTINET, Jean-François SCARIOT – Métrologie comportementale pour la sécurisation. netSEC : une contribution à la sécurisation des campus – JRes2001, Lyon