netMET Network's METrology

Mise en œuvre pratique de la solution de métrologie netMET

24-28 mars 2003 - CINES, Montpellier

CiRen	*ciren@renater.fr*
netMET	*netmet@netmet-solutions.org*
Christine LIBOUBAN	*Christine.Libouban@cines.fr*
Sébastien MOROSI	*Sebastien.Morosi@ciril.fr*
Alexandre SIMON	*Alexandre.Simon@ciril.fr*

netMET
Network's METrology

netMET Network's METrology

Une solution de métrologie développée par le

CRIL

Centre
Interuniversitaire des
Ressources
Informatiques de
Lorraine

netMET Network's METrology

Plan

- Introduction

- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

netMET Network's METrology

Introduction

- Pourquoi cette formation ?
  - netMET a bientôt 3 ans !
  - de plus en plus de monde s'intéresse à netMET
    - plus de 22 sites français l'utilisent en production
    - de nouvelles inscriptions au projet tous les mois
  - les fonctionnalités et informations proposées par netMET semblent faire l'unanimité et satisfaire les besoins actuels en terme de métrologie
  - la nouvelle version de l'exploitation (2.0) est disponible!

netMET Network's METrology

Introduction

- Historique
  - novembre-février 1999-2000
    - tests de faisabilité et développement netMET-1.0
  - 31 janvier 2000 : GIP Renater
    - **Présentation** de la solution de métrologie netMET à la communauté Renater (*wgqos*)
  - 26 avril 2000 : CIRIL
    - **Présentation** netMET (fonctionnement, installation et configuration) et mise à disposition restreinte de netMET-2.0
    - création du « Groupe de travail netMET » : *wg-netMET*
  - juin-septembre 2000
    - stage Peyman GOHARI : *netMET Lookup* et orientation sécurité
  - septembre-octobre 2000
    - versions 2.1 puis 2.2 orientées sécurité : services secureXXX + *nmlookup*
  - novembre-février 2000-2001
    - version 2.3 plus performante : reprise de toutes les structures de données et algorithmes

netMET Network's METrology

Introduction

- Historique
  - juin-septembre 2001
    - stage Cyril PROCH : orientation sécurité, détection de scans et métrologie pour matrice de flux interne
  - 19-20 novembre 2001
    - Formation CiRen, Montpellier
  - décembre 2001
    - JRES2001 Lyon

netMET Network's METrology

Introduction

- Historique
  - août 2002
    - développement exploitation v2.0
    - nouvelle interface, nouvelles fonctionnalités (scans, détails, ..)
  - décembre 2002 : Formation Technologique Avancée
    - présentation devant industriels et partenaires Cisco
  - mars 2003
    - Formation CiRen, Montpellier

netMET Network's METrology

Plan

- Introduction
- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

netMET
Network's METrology

Les informations proposées

Métrologie "**en temps réel**", mise à jour toutes les 10mn

Synthèse des octets sortant/entrant du lien Fédérateur

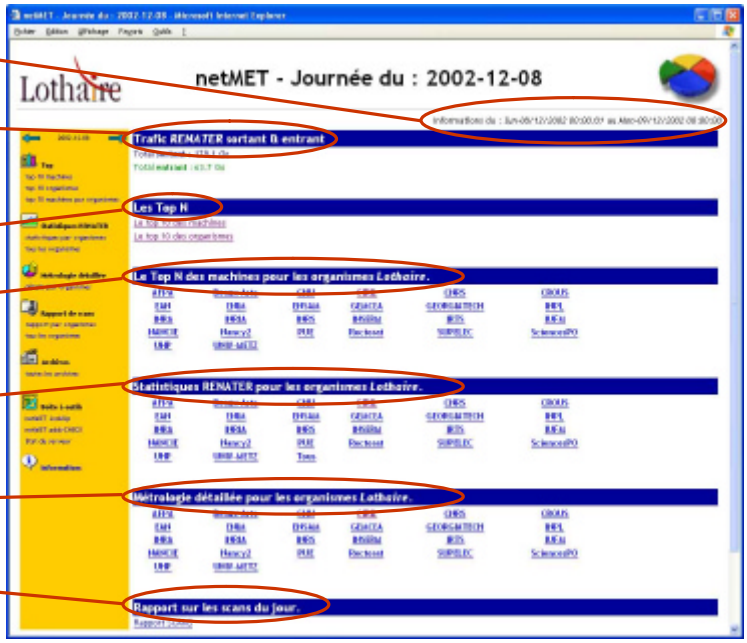
Les **TOP n généraux** des machines et organismes

Les **TOP n locaux** des machines internes aux organismes

Statistiques type *MRTG* pour chaque organismes

Répartitions par services/protocoles pour chaque organismes

Détection de scans en hauteur et largeur



netMET
Network's METrology

Les informations proposées

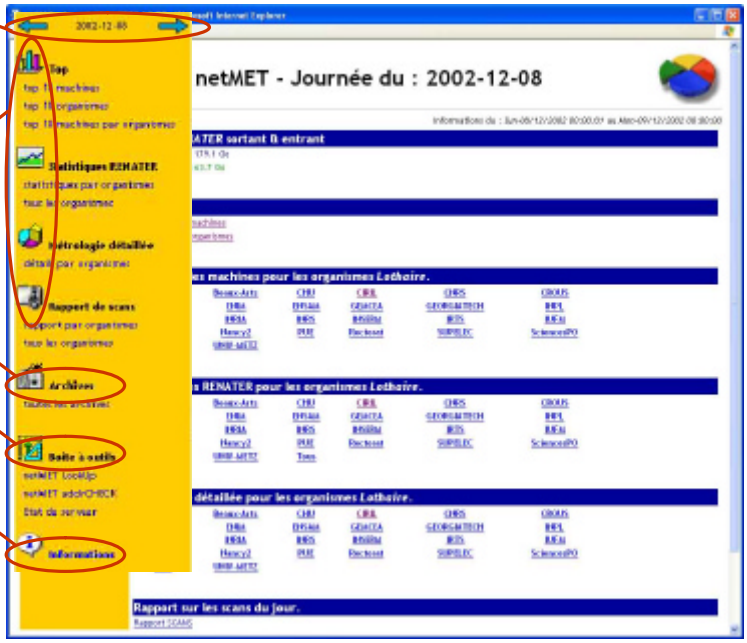
Navigation,
jour suivant – jour précédent

Accès aux informations "en 1 clic"

Archives Web

Boite à outils (scripts)

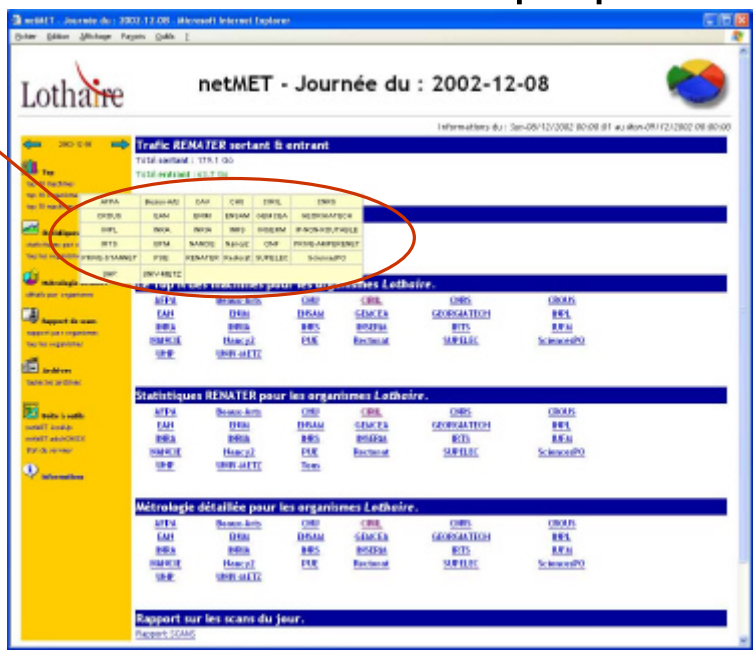
Page d'informations personnalisée



netMET Network's METrology

Les informations proposées

Menu popup,
pour accès "en 1 clic" aux informations déclinées par organismes

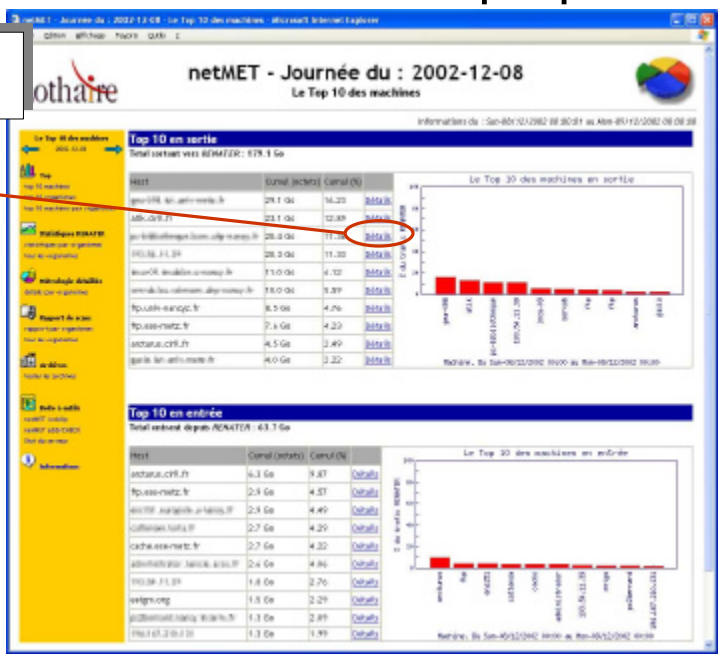


netMET
Network's METrology

Les informations proposées

Les TOPs 10 généraux des machines en entrée et en sortie

Accès aux détails de trafic
Quand ? Quoi ? Avec Qui ?



netMET
Network's METrology

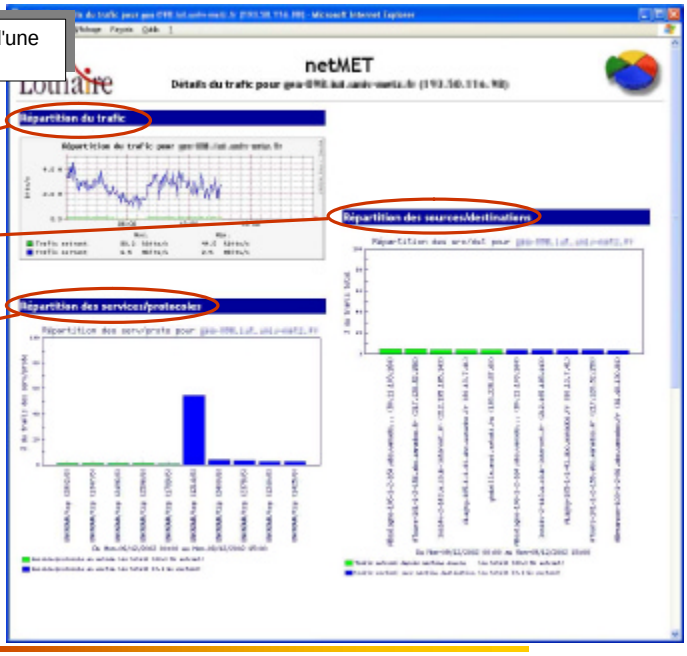
Les informations proposées

Tous les détails de trafic d'une machine particulière

Répartition du trafic dans le temps
Quand ?

Répartition du trafic par sources/destinations
Avec Qui ?

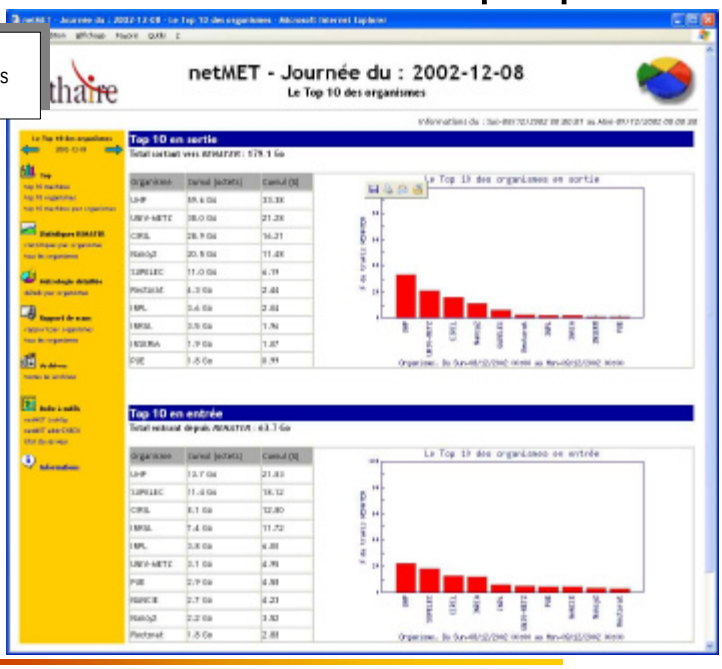
Répartition du trafic par services/protocoles
Quoi ?



netMET
Network's METrology

Les informations proposées

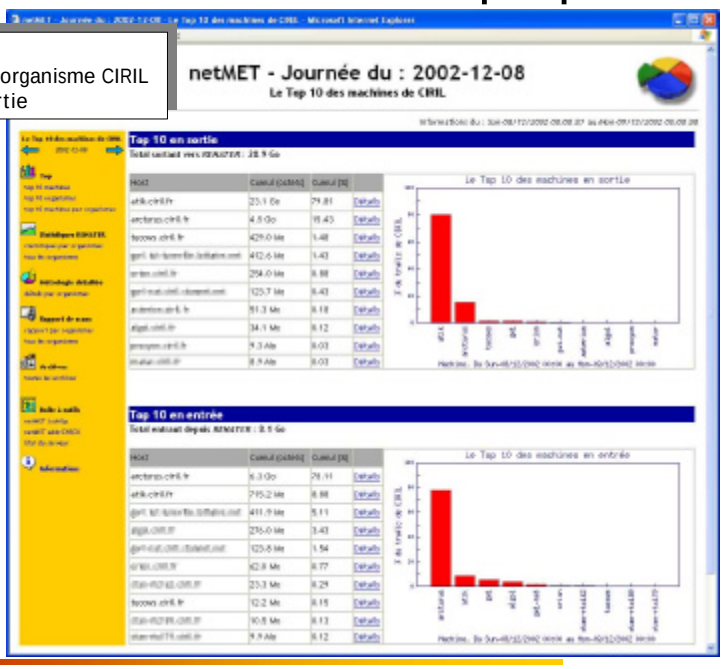
Les TOPs 10 généraux des organismes en entrée et en sortie



netMET
Network's METrology

Les informations proposées

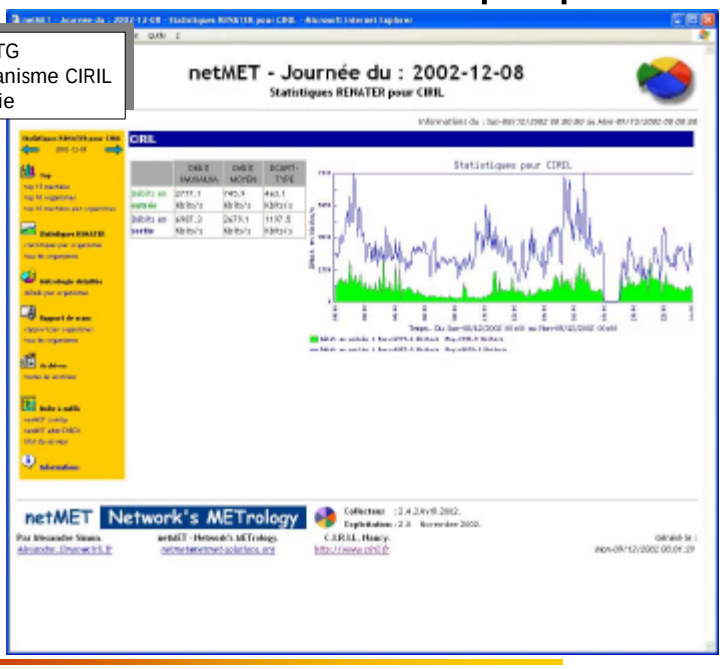
Les TOPs 10
locaux des machines interne à l'organisme CIRIL
en entrée et en sortie



netMET Network's METrology

Les informations proposées

Statistiques type MRTG
pour la consommation de l'organisme CIRIL
en entrée et en sortie



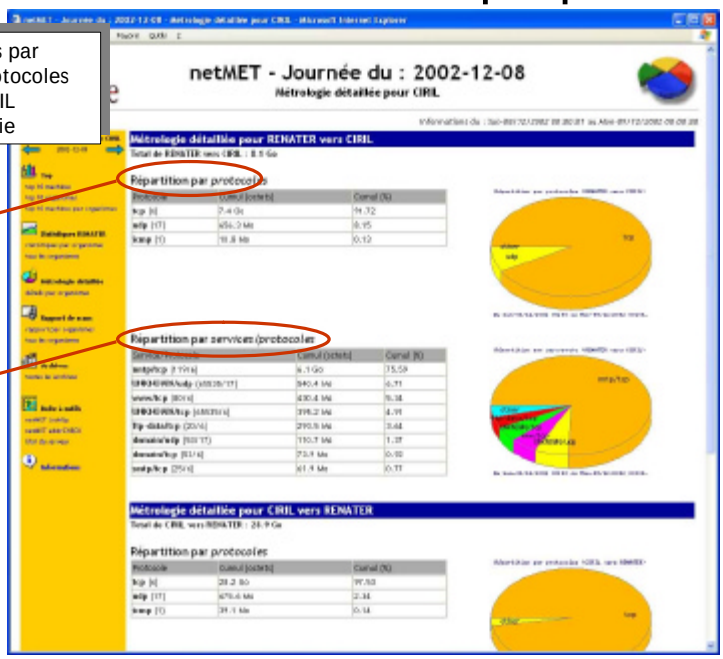
netMET
Network's METrology

Les informations proposées

Répartitions des trafics par protocoles et services/protocoles pour l'organisme CIRIL en entrée et en sortie

Répartition par protocoles

Répartition par services/protocoles



netMET
Network's METrology

Les informations proposées

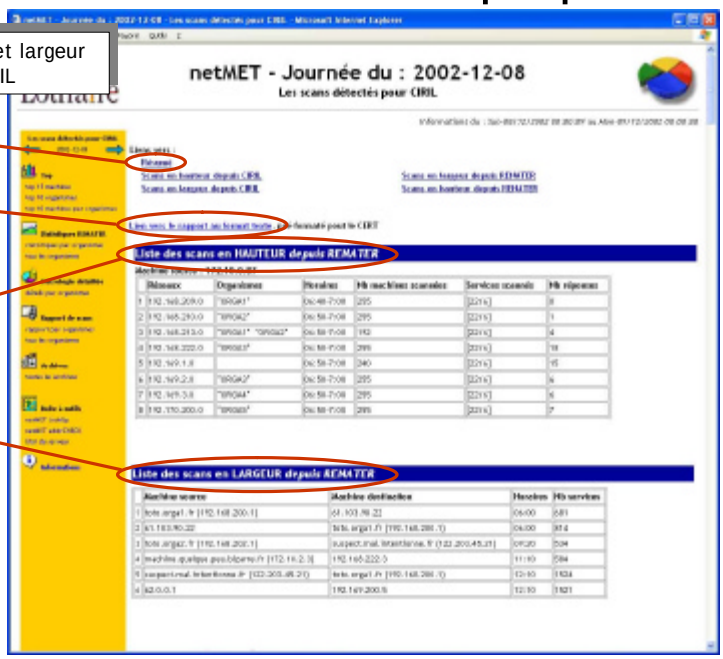
Liste des scans en hauteur et largeur pour l'organisme CIRIL

Résumé synthétique des scans

Rapport au format texte
conforme aux traitements automatiques du CERT

Scans en HAUTEUR
1 machine vers **n** machines sur **1** port

Scans en LARGEUR
1 machine vers **1** machine sur **n** ports

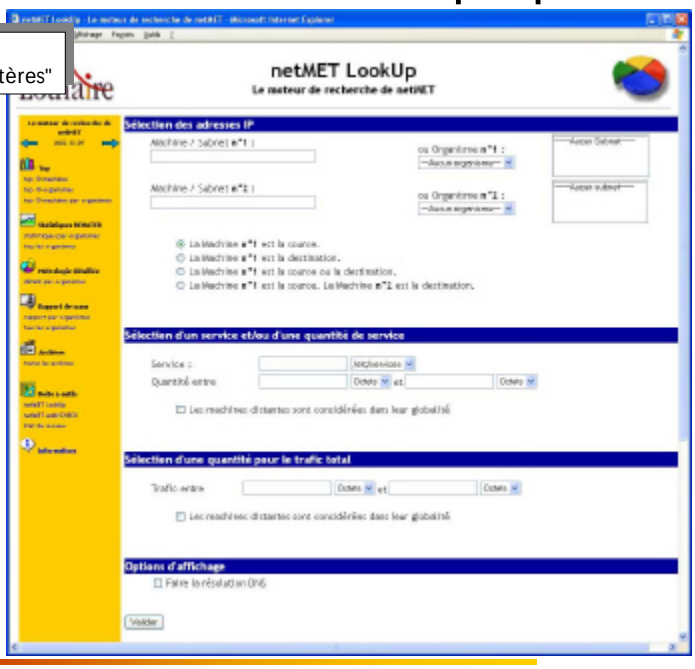


24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 18

netMET
Network's METrology

Les informations proposées

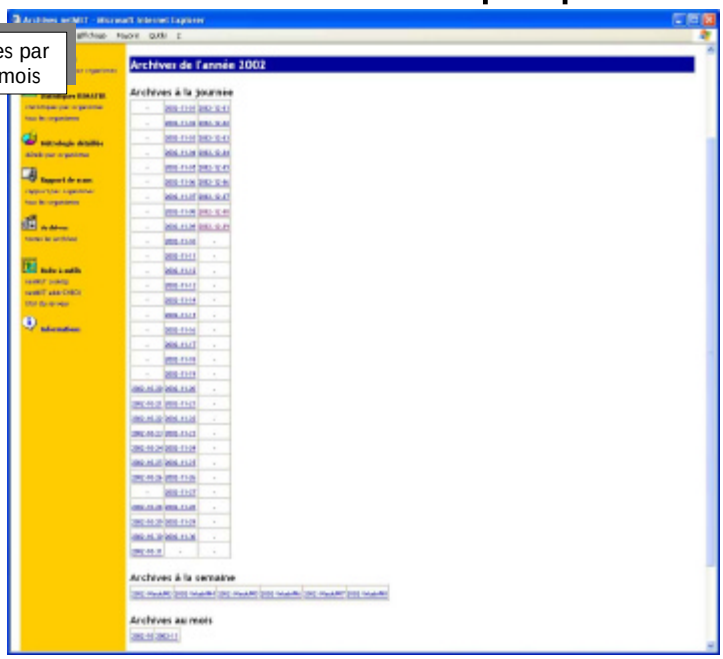
netMET LookUp
"Outil de recherches multi-critères"



netMET Network's METrology

Les informations proposées

Accès direct aux archives par journées, semaines et mois



netMET Network's METrology

Plan

- Introduction
- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

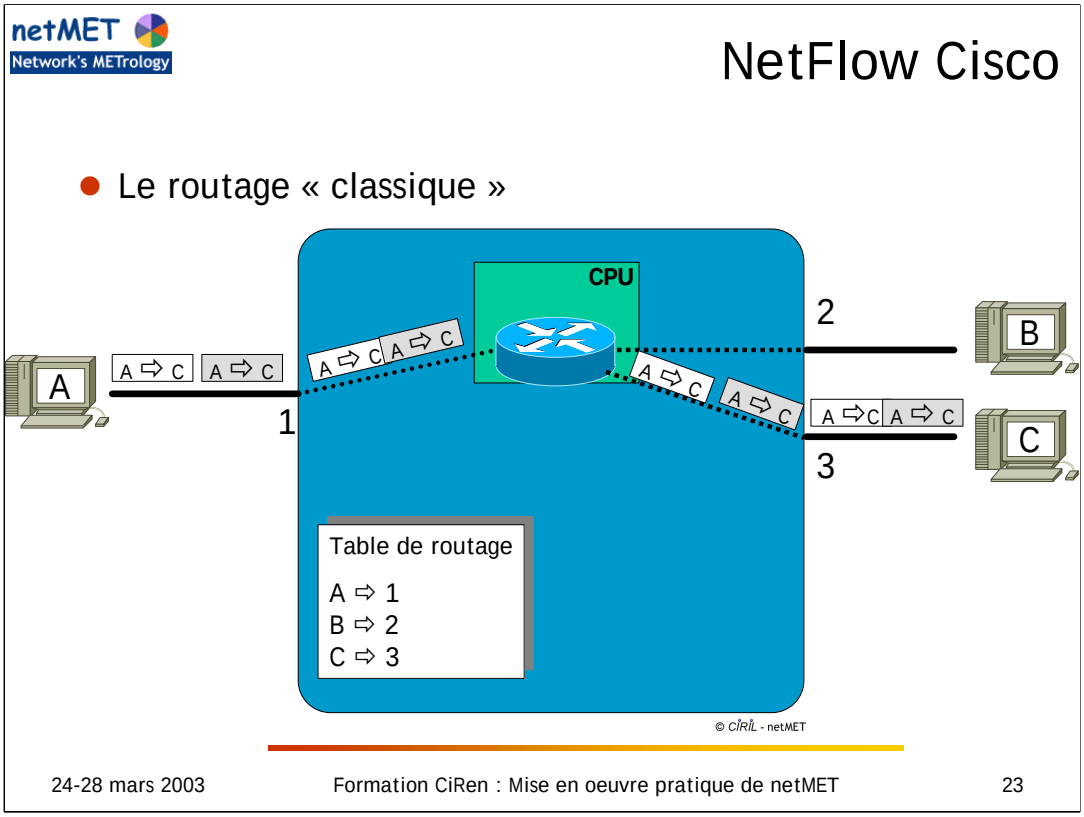
netMET Network's METrology

NetFlow Cisco

- Principes de la technologie *NetFlow- Cisco*
  - technologie embarquée dans les *routeurs* et *switch/routeurs*,
  - initialement conçue pour accélérer le passage des paquets dans un *routeur*
  - passage du mode *forwarding* au mode *switching* sur un flux identifié
- Identification d'un flux :
  - notion de flux *unidirectionnel*
  - *@IP* source - *@IP* destination
  - protocole
  - port source - port destination
  - interface entrée - interface sortie
  - champ TOS

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 22

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.



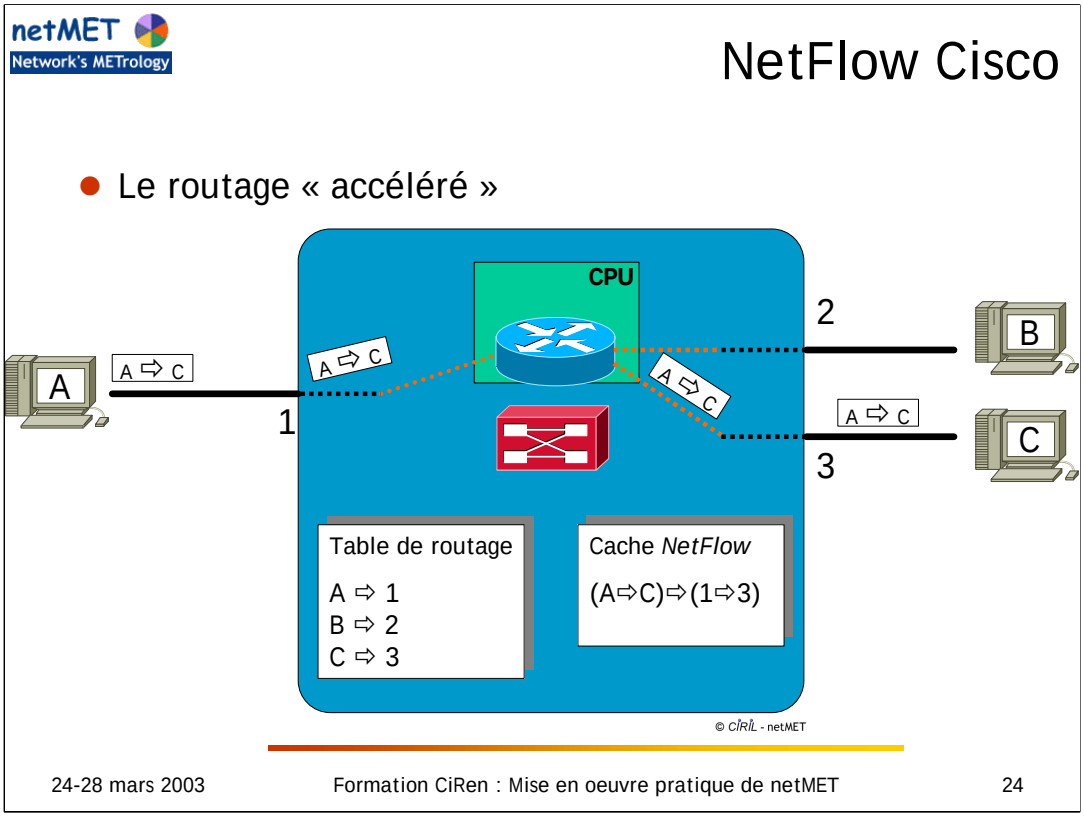
PROCESS :

*** 1er et 2ème paquet ***

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-ci le "remonte" jusqu'à sa 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. et arrive enfin à la machine C

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.

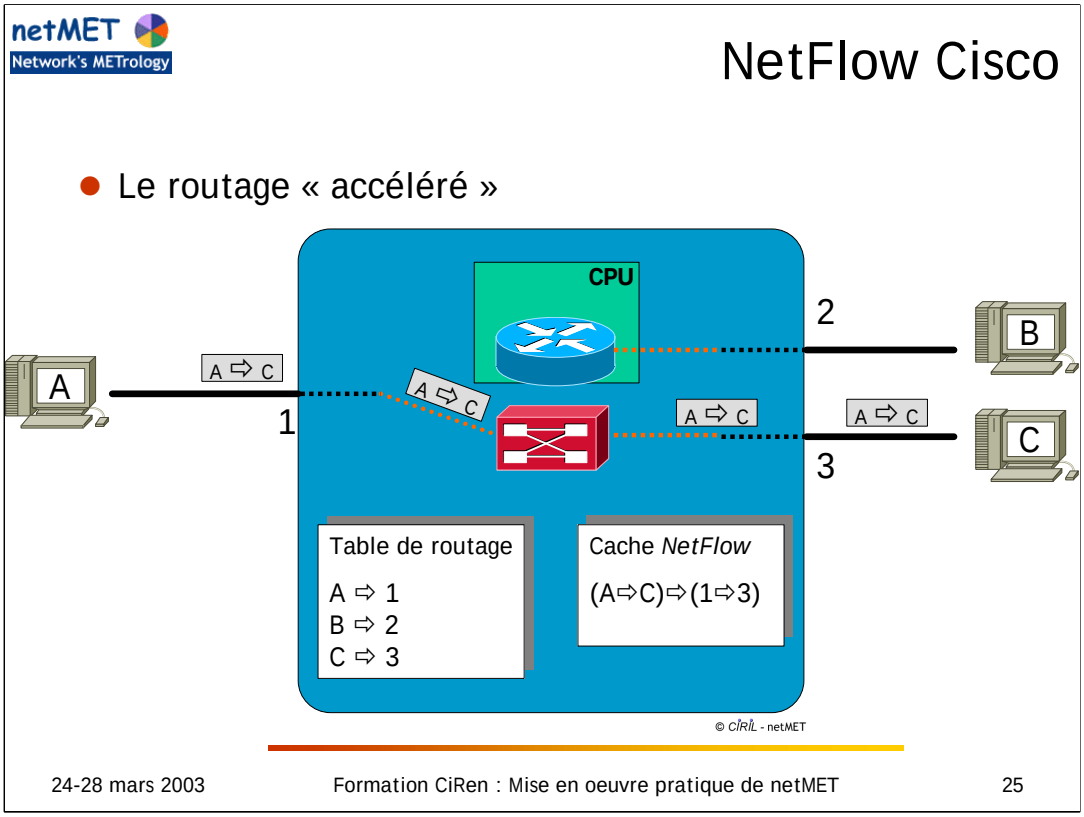
Il n'est donc pas difficile de comprendre que c'est dans ce cas de figure que le routeur perd énormément de temps à décoder et à consulter sa table de routage pour chaque paquet. Intuitivement on pourrait se dire que pour le 2ème paquet et les suivants toutes ces consultations ne sont plus obligatoires 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*...



PROCESS :

*** 1er paquet ***

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-ci le "remonte" jusqu'à sa 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 à l'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 à la machine C



PROCESS:

*** 2eme paquet ***

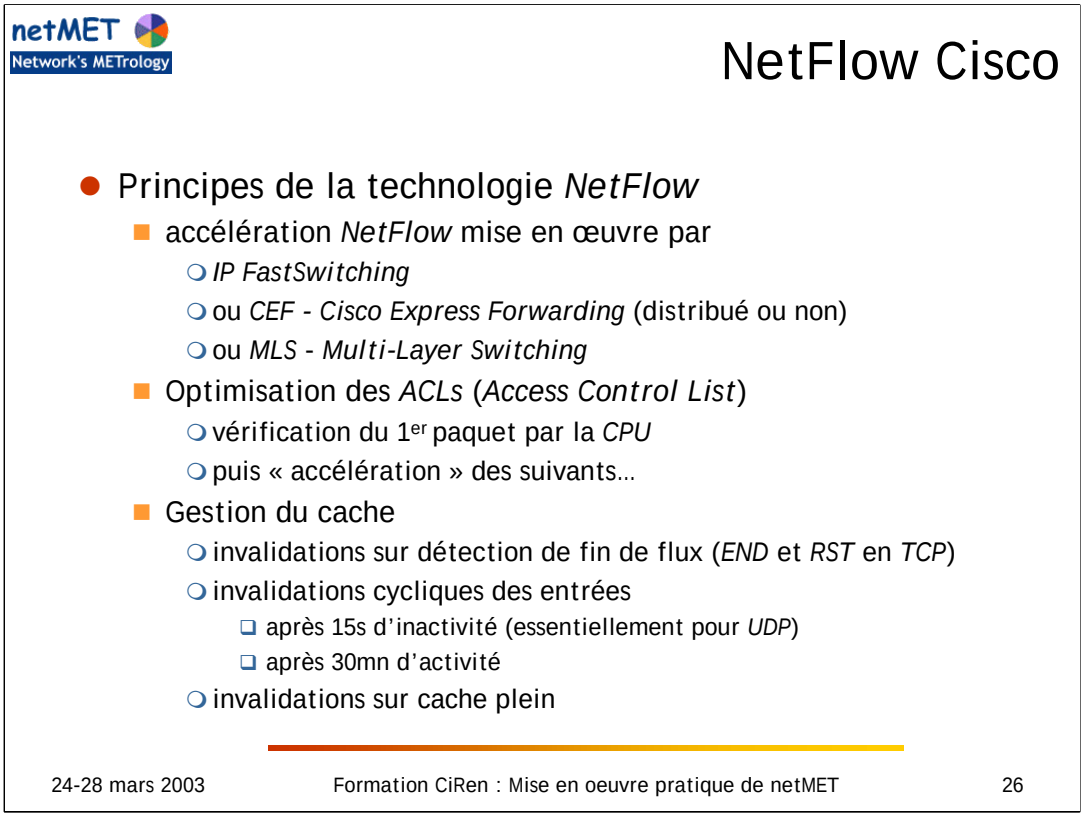
1. le routeur connaît l'existence du flux entre la machine A et C au travers de son cache *NetFlow*, la machine A envoie son 2ème paquet vers la machine C
2. avant de consulter sa table de routage, pour acheminer les paquets, le routeur consulte son cache *NetFlow* pour savoir si le paquet n'appartient 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 a 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 à la machine C

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 à l'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 à chaque 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.



NetFlow n'est qu'une technologie. L'accélération effective des paquets dans un routeur est mise en œuvre par des mécanismes (*IP FastSwitching*, *CEF* ou *MLS*) qui sont dépendant du type de matériel utilisé.

Pour moi : *NetFlow* est un processus à part qui utilise les structures de données manipulées par les mécanismes d'accélération pour construire le **cache *NetFlow*** est proposé des informations sur les flux en transit dans le routeur.

netMET Network's METrology

NetFlow Cisco

- Principes de la technologie *NetFlow*
  - Gestion du cache (suite)
    - configuration des invalidations cycliques des entrées
      - temps d'inactivité (*timeout inactive*) défaut 15s
      - temps d'activité (*timeout active*) défaut 30mn
    - configuration sur routeur avec commandes :
      `ip flow-cache timeout active nn`
      et `ip flow-cache timeout inactive nn`
  - !!! ATTENTION !!! pour netMET
    - les « statistiques Renater » sont calculées sur des échantillons de 5mn, il faut donc forcer le *timeout active* à 5mn !
    - *perl* fait `(octets sur 5mn)/5mn`
      si on laisse *timeout active* à défaut 30mn, *perl* fait `(octets sur 30mn)/5mn` : les stats. sont alors SURévaluées !

!!! ATTENTION !!! pour netMET

ne pas oublier la ligne de commande sur le routeur :

"**`ip flow-cache timeout active 5`**"

Question classique : "cela affecte-t-il les performances de mon routeur ???"

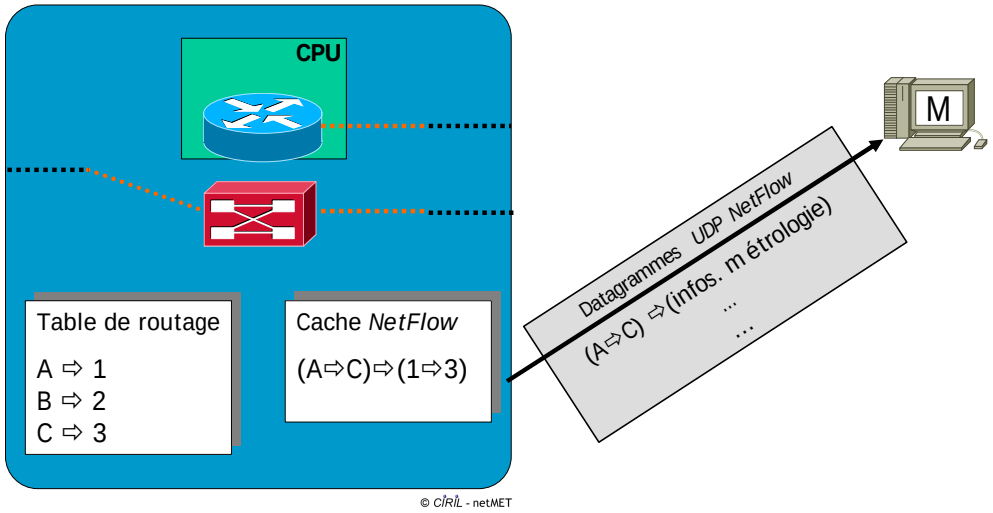
Réponse : "par expérience non", de plus il faut savoir que plus de 95% des flows détectés par un routeur durent moins de 1mn. (web, mail, …), donc les flows sont invalidés tout seul (la commande ip flow-cache tiimeout active 5, n'intervient donc pas).

Seuls les trafics longs (FTP, streaming, …) sont forcés à être invalidés… mais de toutes façons, pas de soucis, car au paquet suivant le routeur re-détecte le flux, et le flux est de nouveau accéléré…

netMET Network's METrology

NetFlow Cisco

- Envoi d'informations de métrologie sur invalidation



24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 28

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.

netMET Network's METrology

NetFlow Cisco

- Exportation de la métrologie :
  - *NetFlow* supporte 4 versions d'exportation de données
    - *V1, V5* sur la plupart des matériels
    - *V7* sur les switch/routeurs type *Catalyst* (*5000*, *6000*, …)
    - *V8* (agrégation de flux) sur la plupart des matériels
  - Pour moi :
    - *V1*, *5* et *7* : formats identiques (et compatibles) pour faire de la métrologie
    - *V8* : format pré-traité (programmation agrégation sur routeur) **inexploitable avec netMET**
  - Cisco recommande de ne plus utiliser la *V1*, **il faut donc** :
    - utiliser la *V5* sur les routeurs
    - utiliser la *V7* sur les switch/routeurs

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 29

Remarque :

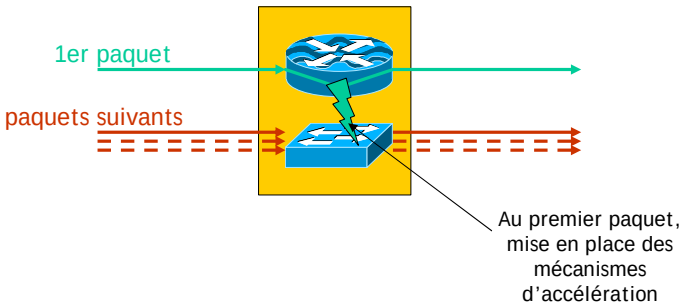
le collecteur netMET reconnaît les formats v1, v5 et v7, et ceci de manière complètement concurrente.

C'est à dire: on peut exporter vers un même collecteur des sources de routeurs différentes avec des version d'export *NetFlow* différentes.

netMET Network's METrology

NetFlow Cisco

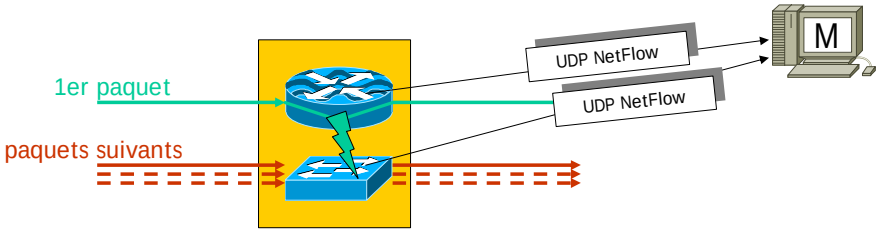
- Attention dans switch/routeur, il y a switch **et** routeur



netMET Network's METrology

NetFlow Cisco

- Attention dans switch/routeur, il y a switch **et** routeur
  - il faut donc activer le *NetFlow* sur les parties
    - routeur pour le 1er paquet
    - switch pour les paquets suivants
  - il faut exporter les information de flows depuis
    - le routeur pour la métro sur le 1er paquet
    - le switch pour la métro sur les paquets suivants



24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 31

MALHEUREUSEMENT…

Même si les informations exportées par la partie switch et routeur sont compatibles (v7 pour switch et v5 pour routeur), **les informations d'interfaces (ifIndex entre autres) ne sont pas compatibles**.

En effet, le routeur manipule des interfaces virtuelles (Vlan ou sous interface physique) alors que le switch manipule uniquement des interfaces physiques… un flow détecté entre le Vlan1 (ifIndex=3, par ex.) et le Vlan2 (ifIndex=8, par ex.), sera exporté :

- par la partie routeur avec ifIN = 3 et ifOUT = 8

- par la partie swicth avec ifIN = (port physique machine source) et ifOUT = (port physique machine destination)

Ce fonctionnement pose de réels problèmes pour le collecteur netMET (et à priori pour Cisco également…). Néanmoins cela peut être réglé de plusieurs manières :

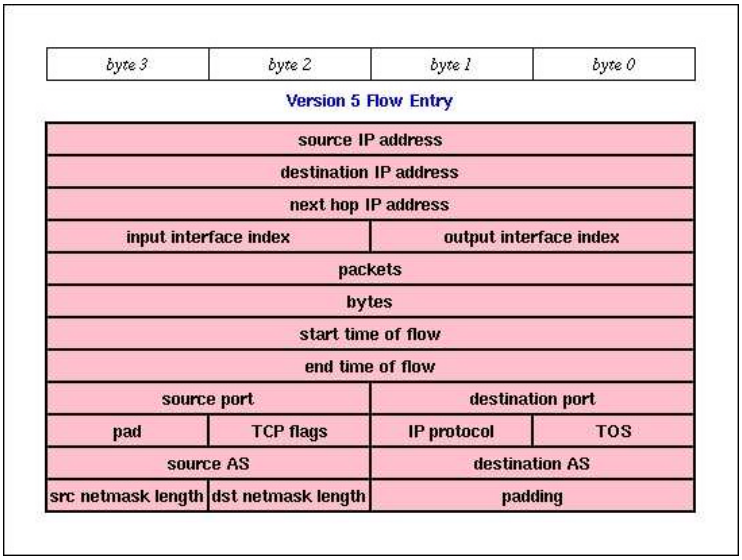
1. prise en compte de ce fonctionnement par le collecteur (OUI, c'est à venir dans la prochaine version)
2. désactivation de l'accélération ("no mls ip" sur un 6xxx par ex.) sur les Vlan à mesurer
3. fonctionnement du switch/routeur en "Full IOS". Par défaut les switch/routeur fonctionnent en "CatOS + IOS"

==> Solution la plus raisonnable à terme : " prise en compte par le collecteur netMET".

netMET Network's METrology

NetFlow Cisco

- Informations de métrologie (ex. *NetFlow V5*)



netMET Network's METrology

NetFlow Cisco

- Activation du *NetFlow* sur un routeur
  - activation par interface physique (impossibilité d'activer sur une sous-interface, sauf *Vlan* en *ISL*)
  - configuration de la machine distante pour les envois d'informations de métrologie
  - l'activation sur une interface donne lieu à l'envoi d'informations de métrologie ***uniquement*** pour les paquets qui ***entrent*** dans cette interface…
    Pour l'aller-retour il faut bien activer **2 interfaces** !
- ***Règle générale*** :
  - activation sur toutes les interfaces qui participent au réseau métropolitain ou régional

Cette histoire "d'aller-retour" est très importante, et c'est souvent la cause de problème lors de la mise en place de netMET sur un site…

Le bug classique est "division par 0" dans les messages du *cron* envoyés à l'administrateur netMET.

A VERIFIER :

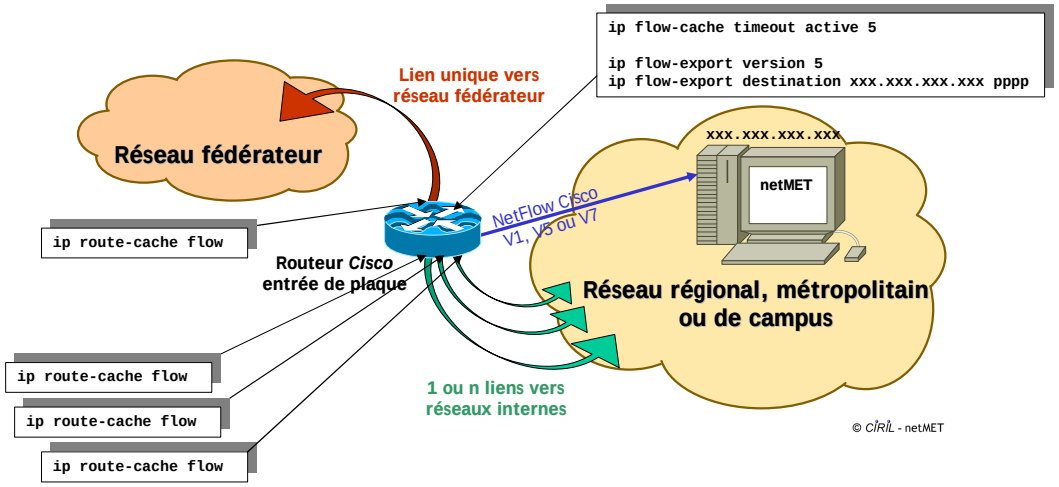
toutes les interfaces qui participent aux échanges internes/externes pour les trafics devant être mesurés
doivent être configurées pour faire du *NetFlow* :

"`ip route-cache flow`" sur ces interfaces.

netMET Network's METrology

NetFlow Cisco

- Activation du *NetFlow* sur un routeur



netMET Network's METrology

NetFlow Cisco

- Activation du *NetFlow* sur un routeur mise en garde !
  - *IP FastSwitching* activé de base
    - ligne : `ip route-cache` présente
      mais invisible car par défaut !
  - Utiliser `no ip route-cache` avec précaution… :-)
    - charge du routeur…
- ***Règle générale sur une interface*** :
  - ne rien avoir = `ip route-cache`
  - ou positionner = `ip route-cache flow`

Il est très fortement déconseillé de désactiver l'accélération sur un routeur, cela peut induire une charge CPU très importante qui peut causer des perturbations du service.

Comment vérifier cela ???

1. vérifier la charge sur routeur : "**`show processes cpu`**"

```
CPU utilization for five seconds: 36%/35%; one minute: 36%; five minutes: 37%
 PID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process
   1          84    91845      0   0.00%  0.00%  0.00%   0 Load Meter
   2          68      131    519   0.08%  0.03%  0.00%   2 Virtual Exec
  …
```

Une charge > à 50% commence à être suspecte (ce chiffre dépend bien sûre : du routeur, du site, du nombre de machines sur le réseau…)

2. vérifier qu'il n'existe pas de ligne "no ip route-cache" dans la configuration :
"**`show running-config | include no ip route-cache`**" sur routeur classique
"**`show running-config | include no mls ip`**" sur MFSC ou RSM (5xxx, 6xxx)

si oui, à voir avec son administrateur réseau préféré…

RQ: je ne traite aussi que le cas de routeurs "classiques", pour le switch/routeurs il y a également quelques blagues de la sorte !

netMET Network's METrology

Plan

- Introduction

- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

netMET Network's METrology

NetFlow Cisco, news

- Les interfaces supportées par *NetFlow*
  - presque tous types d'interfaces (Ethernet, FastEthernet, Serial, ATM, …)
  - à terme tous les types devraient être supportés
- Impossibilité d'activation par sous interface
  - sauf pour interfaces *Vlan* en *ISL*
  - seule possibilité :
    - activation sur interface physique (ATM2/0)
    - et récupération par sous-interface avec les ifIndex (ATM2/0.999-aal5 layer)
  - à terme l'activation par sous-interface devrait être supportée

netMET Network's METrology

NetFlow Cisco, news

- Persistance des numéros ifIndex SNMP des interfaces
  - normalement :
    - configuration d'une nouvelle sous-interface
      -> création nouveau ifIndex
    - réorganisation des ifIndex au reboot du routeur :-(
  - nouvelle fonctionnalité : persistance des numéros ifIndex
    - commande générale
      `snmp-server ifindex persist`
    - commande sur interface physique (PAS sur sous-interface)
      `snmp ifindex persist`
    - permet de conserver un numéro d'interface persistant toute la vie du routeur (plus de pb. de reboot)
    - disponible sur IOS 12.1(5)T

netMET Network's METrology

NetFlow Cisco, news

- Persistance des numéros ifIndex SNMP des interfaces
  - netMET « sensible » au reboot du routeur, il faudrait donc :
    - arrêter netMET
    - rebooter le routeur
    - redémarrer netMET
    - si arrêt non programmé : nettoyer les « data » concernées et redémarrer netMET
  - netMET manipule les ifIndex au travers des descriptions textuelles des interfaces
    - pas de manipulation directe des ifIndex : BIEN
    - ifIndex des descriptions sensibles au reboot : PAS BIEN
  - la persistance des numéros ifIndex SNMP est un plus significatif pour netMET (et autres)
    - configurations pérennes, plus de sensibilité au reboot

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 39

Au cas de reboot programmé du routeur il est important de respecter la manip. suivante :

1. arrêter netMET, tous les services (sauf éventuellement le duplicateur)
2. rebooter le routeur
3. redémarrer netMET, les services arrêtés avant le reboot

Si l'arrêt n'a pas été programmé (crash ou maintenance d'urgence), il se peut que de mauvaises données soient collectées : la métrologie est incohérente… il faut donc :

1. nettoyer les "data" et "html" pour la période concernée
2. éventuellement regénérer les informations (html+images) si la période concernée n'est pas dans la journée en cours

netMET Network's METrology

NetFlow Cisco, news

- Exportation UDP NetFlow vers plusieurs collecteurs
  - initialement
    - une seule destination
  - à partir de l'IOS 12.2(1)T
    - 2 destinations
    - disponible uniquement sur les routeurs (pas switch/routeurs)
  - pour moi :
    - c'est bien mais pas encore assez !
      Pourquoi seulement 2 destinations ?
  - le duplicateur netMET permet de contourner ce problème :
    - exportation depuis routeur vers duplicateur
    - n duplications vers
      - collecteurs netMET (prod. ou tests)
      - ou duplicateurs netMET

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 40

Le duplicateur netMET est présent depuis le début du projet et apporte des notions supplémentaires par rapport à l'exportation multiples à partir des routeurs :

1. netMETdup est capable d'exporter vers n destinations (avec n pouvant être > 2)
2. netMETdup autorise les chaînages de duplicateurs : passage des flows par plusieurs duplicateurs avant d'arriver à la machine de collecte.

Le point (2) n'est pas recommandé car multiplication des duplicateurs = multiplication des sources de pertes de paquets UDP. Néanmoins, pour des tests cette fonctionnalité est très intéressante.

Exemple :

- un serveur de production qui duplique vers lui-même (pour les 4 services) et qui duplique vers un serveur de backup
- le serveur de backup reçoit les flows comme si ils venaient du routeur originel.

netMET Network's METrology

NetFlow Cisco, news

Cisco IOS™ Software Release Version	Supported NetFlow Export Version(s)	Supported Cisco Hardware Platforms
11.1CA, 11.1CC	v1, v5	7200, 7500, RSP7000
11.2, 11.2P	v1	7200, 7500, RSP7000
11.2P	v1	Route Switch Module (RSM), 11.2(10)P and later
11.3, 11.3T	v1	7200, 7500, RSP7000
12.0	v1, v5	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM
12.0T 12.0S	v1, v5	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM, BPX 8600
12.0(3)T and later 12.0(3)S and later	v1, v5, v8	1400*, 1600*, 1720, 2500*,2600, 3600, 4500, 4700, AS5800, AS5300**, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM, BPX 8650
12.04XE	v1, v5, v8	7100
N/A	v7	Catalyst 5K NetFlow Feature Card (NFFC) Catalyst 6K with MSFC card
12.0(6)S	v8	12000

*Support for NetFlow Export v1, v5, and v8 on 1600 and 2500 platforms is targeted for Cisco IOS software release 12.0(5)T. NetFlow support for these platforms will not be available in the Cisco IOS 12.0 mainline release.

**Support for NetFlow Export v1, v5, and v8 on AS5300 platform is targeted for Cisco IOS software release 12.0(7)XR.

SOURCE : Slide par Cisco

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 41

Aujourd'hui tous les types de routeurs (routeurs classiques) supportent le NetFlow et peuvent alors être utilisés dans une architecture à base de netMET.

Nous savons que les matériels switch/routeur type 5xxx et 6xxx supportent également le NetFlow. Leur fonctionnement étant un peu particulier, ils ne sont pas entièrement supportés par netMET -MAIS CECI N'EST QU'UNE QUESTION DE TEMPS! –

==> **si les demandes sur ce point deviennent pressantes, ce point deviendra prioritaire pour la modification du collecteur…**

netMET Network's METrology

NetFlow Cisco, news

- Droit d'utilisation et Licence Cisco NetFlow
  - Plateformes Cisco 7200/7500/RSM
    - NetFlow dispo. dans toutes les images IOS
    - achat d'une licence par matériel pour droit à l'utilisation
  - Plateformes Cisco 1000/1600/2500/2600/3600/4000/AS5800 Series
    - NetFlow dispo. uniquement dans les images IOS IP Plus
    - achat de l'image IOS IP Plus pour droit à l'utilisation
    - pas de licence supplémentaire
  - Plateformes Catalyst 6xxx
    - NetFlow dispo. dans toutes les images IOS (carte routage)
    - achat d'une carte MSFC/MSFC2 (carte routage) pour droit à l'utilisation
    - pas de licence supplémentaire

Ces infos. sont des sources Cisco.

Souvent la commande (`ip route-cache flow`) est autorisée dans l'IOS, mais peut-être n'avez-vous pas le droit de (ie. peut-être n'avez-vous pas payé pour :-)) l'utiliser… dans le doute à voir avec l'intégrateur Cisco local.

Rq: c'est idem pour d'autres fonctionnalités Cisco : ex. BGP sur un 5xxx ou 6xxx.

netMET Network's METrology

Plan

- Introduction

- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

metaMET, le coût de la métrologie

- « Pour mieux compter, regarder ce qu'il faut mesurer »
- L'évaluation du coût de la métrologie a été et reste un point essentiel pour le développement du collecteur et de ces évolutions
- Connaître pour dimensionner et mettre en place
  - combien de flows je traite ?
  - quels sont les burst de flow ?
  - quel trafic cela génère sur mon réseau local ?
  - et maintenant, quelle machine ou quels services ?

metaMET, le coût de la métrologie

- metaMET est disponible pour ceux qui utilisent netMET
  - en production pour voir ce que netMET traite
  - en production pour connaître l'évolution de leur réseau
  - en test pour dimensionner et faire le choix d'une machine de production
- Exemple de metaMET :
  - mesure du lien Renater pour le réseau régional Lothaire
  - du 14 mai au 20 mai 2001

netMET Network's METrology

metaMET, le coût de la métrologie

metaMET du May 14 au May 20

	May 14	May 15	May 16	May 17	May 18	May 19	May 20
Nb UDP reçus	1 080 608	1 153 218	1 068 468	1 056 160	1 083 314	286 883	238 079
Nb flow reçus	**32 418 240**	**34 596 540**	**32 054 040**	**31 684 800**	**32 499 420**	**8 606 490**	**7 142 370**
Taille info. NetFlow reçus (octets)	1 586 332 544	1 692 924 024	1 568 511 024	1 550 442 880	1 590 304 952	421 144 244	349 499 972
Nb flow traités	31 710 154	33 845 014	31 314 449	30 977 450	31 766 039	8 179 117	6 703 599
Ratio flow reçus / flow traités	97.82%	97.83%	97.69%	97.77%	97.74%	95.03%	93.86%
flow/s sur 24h	375.2	400.4	371.0	366.7	376.2	99.6	82.7
UDP/s sur 24h	12.5	13.3	12.4	12.2	12.5	3.3	2.8
Taille info. NetFlow reçus bit/s sur 24h	146 882.6	156 752.2	145 232.5	143 559.5	147 250.5	38 994.8	32 361.1
Nb flow max. sur 5mn	**271 380**	**274 680**	**271 050**	**249 390**	**285 990**	**60 600**	**56 460**
flow/s max. sur 5mn	**904.6**	**915.6**	**903.5**	**831.3**	**953.3**	**202.0**	**188.2**
Nb UDP max. sur 5mn	9 046	9 156	9 035	8 313	9 533	2 020	1 882
UDP/s max. sur 5mn	30.2	30.5	30.1	27.7	31.8	6.7	6.3
Taille info. NetFlow reçus max. sur 5mn (octets)	**13 279 528**	**13 441 008**	**13 263 380**	**12 203 484**	**13 994 444**	**2 965 360**	**2 762 776**
Taille info. NetFlow reçus max. bit/s sur 5mn	**354 120.7**	**358 426.9**	**353 690.1**	**325 426.2**	**373 185.2**	**79 076.3**	**73 674.0**
Cumul Nb UDP reçus	1 080 608	2 233 826	3 302 294	4 358 454	5 441 768	5 728 651	5 966 730
Cumul Nb flow reçus	32 418 240	67 014 780	99 068 820	130 753 620	163 253 040	171 859 530	179 001 900
Cumul Taille info. NetFlow reçus (octets)	1 586 332 544	3 279 256 568	4 847 767 592	6 398 210 472	7 988 515 424	8 409 659 668	8 759 159 640
Nb UDP sur 1semaine	5 966 730						
UDP/s sur 1semaine	9.9						
Nb flow sur 1semaine	**179 001 900**						
flow/s sur 1semaine	**296.0**						
Taille info. NetFlow reçus sur 1semaine (octets)	**8 759 159 640**						
Taille info. NetFlow reçus bit/s sur 1semaine	**115 861.9**						

© CiRIL - netMET - AS

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 46

Dans ce tableau les chiffres les plus importants sont :

- d'un point de vue "évaluation de la taille du réseau" : **le nombre de flows sur 24h**
- d'un point de vue "charge que le collecteur doit supporter" : **le flow/s max. sur 5mn**

Ces évaluations ont été réalisées avant même d'avoir une seule ligne de code du collecteur netMET. En effet, ces résultats ont permis de prendre les "bonnes directions" par rapport aux structures de données et algorithmes utilisés dans le collecteur.

La puissance du collecteur ne s'évalue pas sur 24h ou sur 1 semaine mais plutôt sur les pics de trafic sur 5mn, là où le collecteur a le maximum de flows à traiter. Ici on sait que pour ne perdre aucun flow il faut être capable de traiter **953.3** flows à la seconde !

Toutes ces infos. sont disponibles dans les logs des collecteurs : "`/var/log/netmet`". A l'arrêt ou au redémarrage du collecteur, celui-ci donne des infos sur ce qu'il a traité :

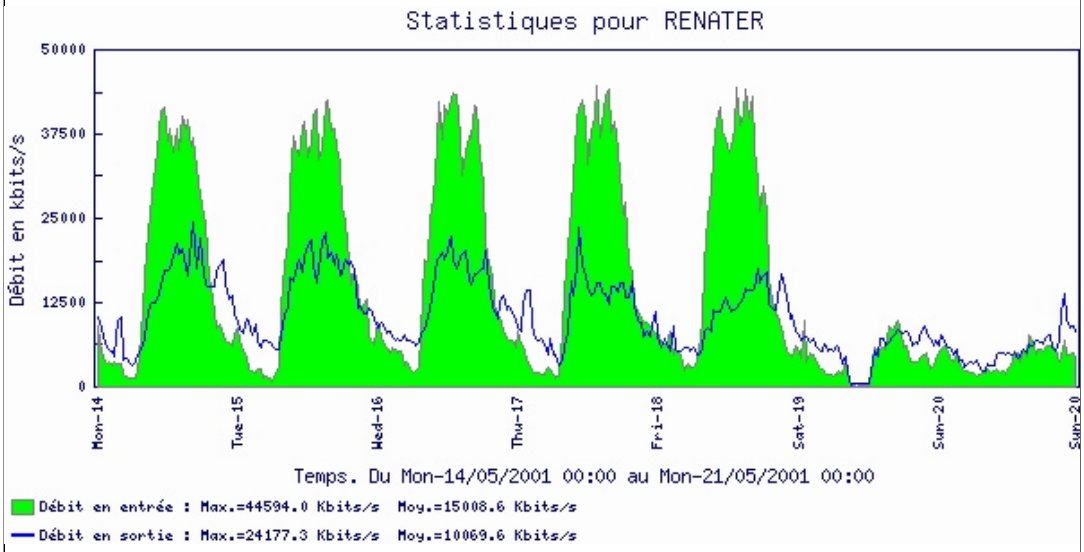
```
"Oct 31 15:00:01 ma_machine /home/netmet/netMet/le_service/netMETcll[821]: [I]
- Collector netMETcll restarted  -[UDP=12198, FLOW_r=365940, FLOW_f=358273,
FLOW_p=358273, 97.9% flows processed by netMETcll , 100.0% flows processed by
netMETacc]"
```

- UDP=12198 : nombre de paquets UDP traités
- FLOW_r=365940 : nombre de flows reçus dans ces 12198 paquets UDP
- FLOW_f=358273 : nombre de flows réellement traités par netMETcll (après application des règles (IF_PROCESSED et IF_AGGREGATION) et passés au processus d'accounting netMETacc
- FLOW_p=358273 : nombre de flows réellement traités par netMETacc

Ici le pourcentage 97.9% est normale puisque le collecteur épure quelques flows (flows non désirés). Si des flows étaient perdus entre les 2 processus netMETcll et netMETacc, le 2ème pourcentage ne serait pas à 100%… Si ce pourcentage n'est pas à 100%, cela signifie que la machine n'a pas pu tout traiter (manque de puissance CPU ou manque de mémoire ?!?). Ce cas de figure s'accompagne d'un WARNING dans les logs…

netMET Network's METrology

metaMET, le coût de la métrologie



netMET Network's METrology

Plan

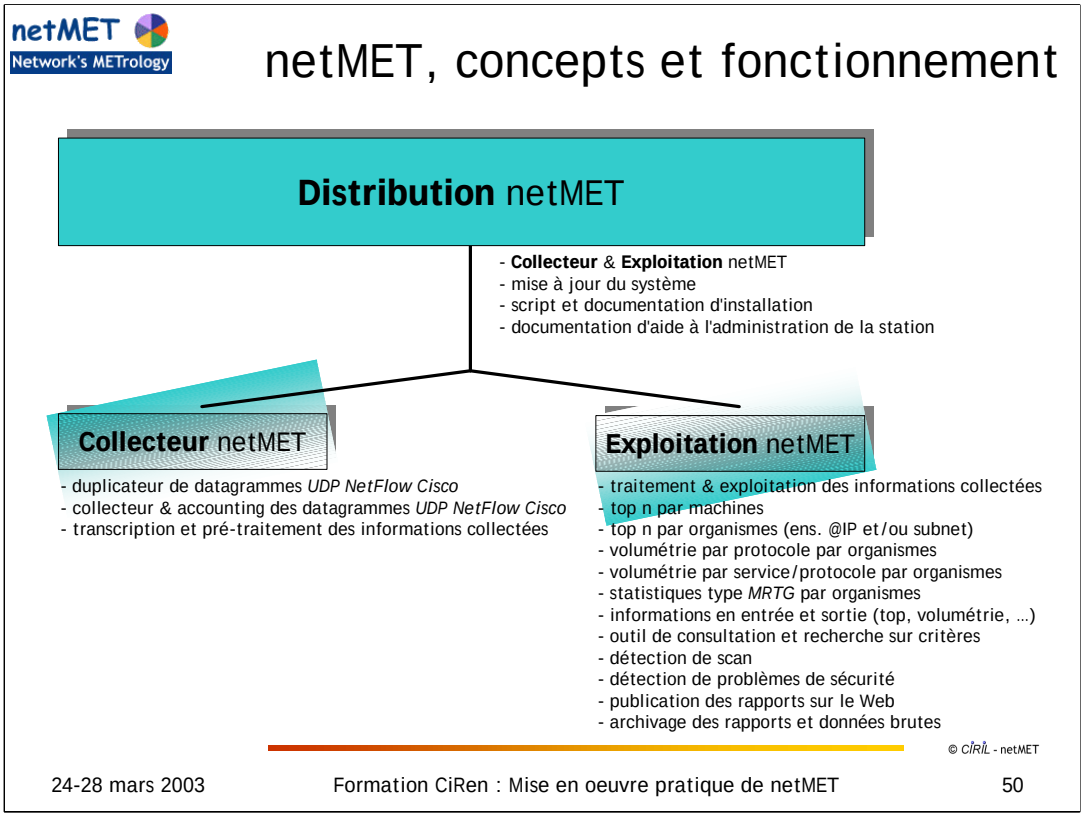
- Introduction

- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

netMET Network's METrology

netMET, concepts et fonctionnement

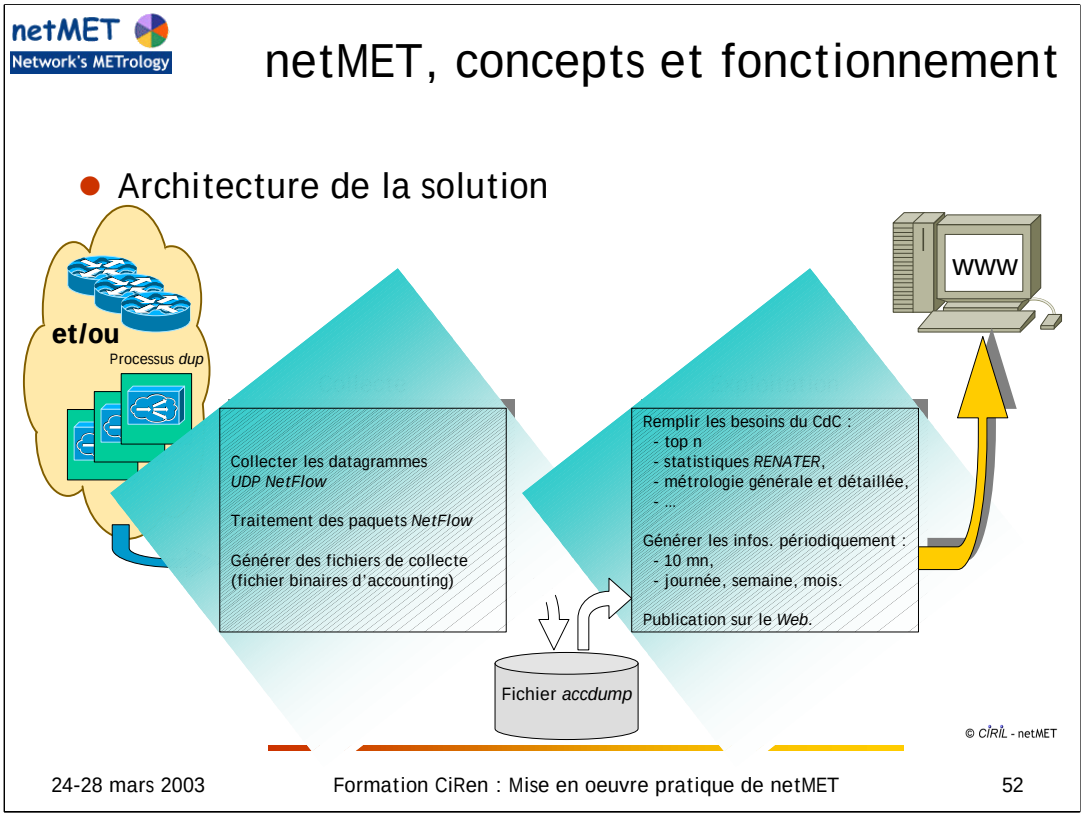
- Où en sommes nous aujourd'hui ?
- 2 voies de développement netMET :
  - le **collecteur** netMET de datagrammes *UDP NetFlow Cisco*
  - l'**exploitation** netMET des informations collectées
- La **distribution** netMET regroupe ces 2 voies de développement, ainsi :
  - le collecteur netMET reste utilisable sans l'exploitation (collecte simple dans des fichiers brutes)
  - l'exploitation ne peut fonctionner qu'avec les données fournies par le collecteur netMET


netMET
Network's METrology
netMET, concepts et fonctionnement
Distribution netMET
- Collecteur & Exploitation netMET
- mise à jour du système
- script et documentation d'installation
- documentation d'aide à l'administration de la station
Collecteur netMET
- duplicateur de datagrammes UDP NetFlow Cisco
- collecteur & accounting des datagrammes UDP NetFlow Cisco
- transcription et pré-traitement des informations collectées
Exploitation netMET
- traitement & exploitation des informations collectées
- top n par machines
- top n par organismes (ens. @IP et/ou subnet)
- volumétrie par protocole par organismes
- volumétrie par service/protocole par organismes
- statistiques type MRTG par organismes
- informations en entrée et sortie (top, volumétrie, ...)
- outil de consultation et recherche sur critères
- détection de scan
- détection de problèmes de sécurité
- publication des rapports sur le Web
- archivage des rapports et données brutes
© CIRIL - netMET
24-28 mars 2003
Formation CiRen : Mise en oeuvre pratique de netMET
50

netMET Network's METrology

netMET, concepts et fonctionnement

- Architecture de la solution
  - découpage de la solution en 2 thèmes principaux :
    - la collecte
      - partie la plus critique
      - langage *C*
      - optimisation fine
    - l'exploitation
      - partie devant être la plus flexible possible
      - langage *Perl* pour les générations *HTML* et *images*
      - langage *C* pour les parties nécessitant d'être rapides…



Avec cette architecture, on comprend mieux pourquoi j'ai séparé le développement de chaque partie. De cette façon je peux avancer en parallèle en minimisant les dépendances entre collecte et exploitation.

De plus cette architecture autorise le développement de sa propre exploitation à base d'informations proposées par le collecteur netMET.

netMET, concepts et fonctionnement

- Le duplicateur de flows : netMETdup
  - 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

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 53

Il faut que le terme "agrégation" soit bien compris pour la suite !

Le principe est assez simple : le collecteur netMET autorise d'agréger (translater, mapper, faire correspondre) toutes les adresses IP entrantes/sortantes d'une interface vers une adresse symbolique. Ainsi on ne voit plus les adresses IP sources/destinations entrantes/sortantes de cette interface mais uniquement l'adresse symbolique utilisée.

L'agrégation permet essentiellement de régler 2 problèmes :

- simplifier les adresses IP qui ne sont pas intéressantes et permettre une identification rapide des sens de communication,
- simplifier les traitements réaliser par le collecteur et réduire la taille des fichiers de collecte.

EX: agréger toutes les adresses IP de l'Internet vers une seule adresse symbolique…

Les 5mn des statistiques Renater sont historiques… en fait Renater souhaitait obtenir les statistiques de ses sites en région avec la même sémantique que MRTG, c'est à dire :

- granularité des informations = 5mn
- statistiques à la journée avec lissage sur 5mn
- statistiques à la semaine avec lissage sur 30mn
- statistiques au mois avec lissage sur 2h.

netMET et ses "Statistiques Renater" sont donc conformes aux pré-requis du GIP Renater pour la métrologie des sites Renater en région.

netMET Network's METrology

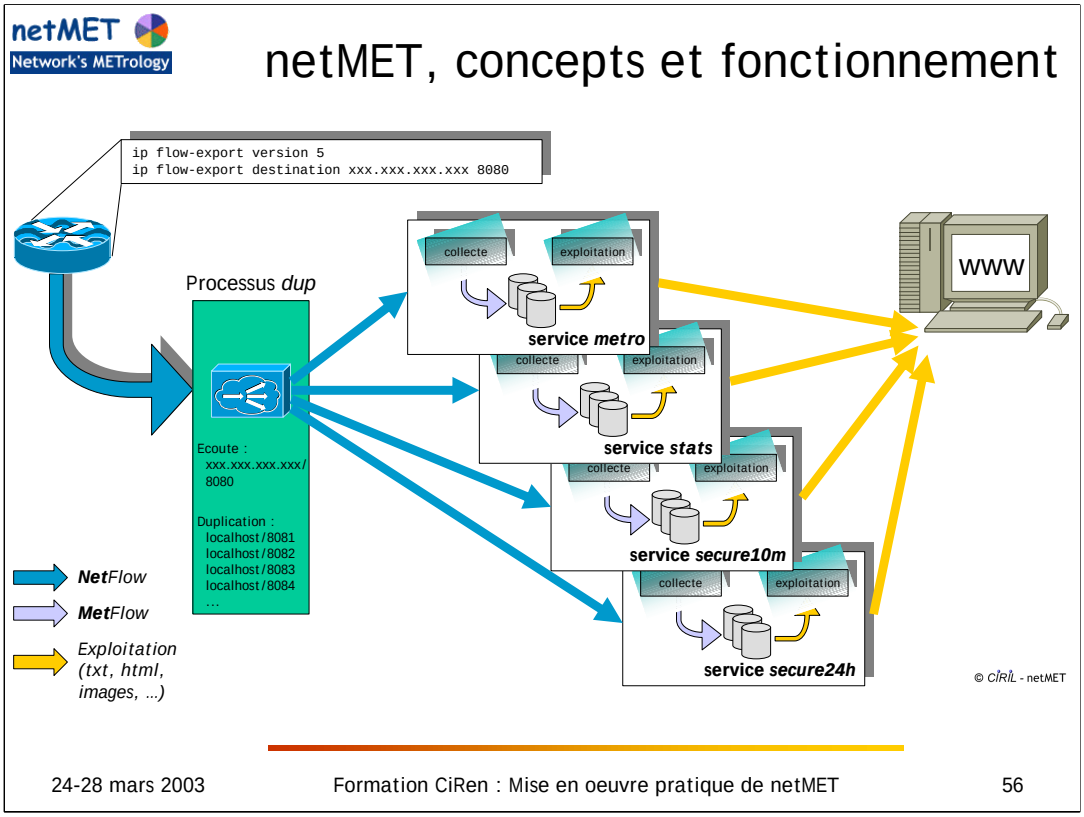
netMET, concepts et fonctionnement

- Le duplicateur de flows : netMETdup
  - l'agrégation et la non-agrégation obligent à utiliser des collecteurs différents
  - les périodes d'échantillonnage différentes obligent à utiliser des collecteurs différents
- Donc,
  - à chaque « point de vue » (service) sera associé un collecteur
    - métrologie générale : metro
    - statistiques Renater : stats
    - sécurité sur 10mn : secure10mn
    - sécurité sur 24h : secure24h

netMET Network's METrology

netMET, concepts et fonctionnement

- Le duplicateur de flows : netMETdup
  - Problème… 4 collecteurs = 4 ports d'écoute pour les datagrammes *UDP NetFlow*…
    - malheureusement, programmation d'exportation des datagrammes *NetFlow* sur le routeur, uniquement vers une seule (maintenant 2, IOS 12.2(1)T) machines et un seul port
      - **solution** : le « duplicateur de ports »
  - « Duplicateur de ports » (*netMETdup*) :
    - solution logicielle (processus démon)
    - programmation du routeur pour exporter le *NetFlow* vers le duplicateur
    - le duplicateur reçoit les datagrammes sur son port d'entrée
    - puis, duplication vers autant de machines/ports que souhaité


netMET
Network's METrology
netMET, concepts et fonctionnement
ip flow-export version 5
ip flow-export destination xxx.xxx.xxx.xxx 8080
Processus dup
Ecoute :
xxx.xxx.xxx.xxx/
8080
Duplication :
localhost/8081
localhost/8082
localhost/8083
localhost/8084
...
collecte
exploitation
service metro
service stats
service secure10m
service secure24h
WWW
NetFlow
MetFlow
Exploitation
(txt, html,
images, ...)
© CIRIL - netMET
24-28 mars 2003
Formation CiRen : Mise en oeuvre pratique de netMET
56

netMET, concepts et fonctionnement

- Le duplicateur de flows : netMETdup
  - règle générale : autant de collecteur que de service différents
  - pour la distribution netMET :
    - les 4 services (*metro, stats, secure10m et secure24h*) semblent satisfaire l'ensemble des besoins actuels et à venir

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 57

Le choix des 4 collecteurs c'est fait pour les raisons suivantes :

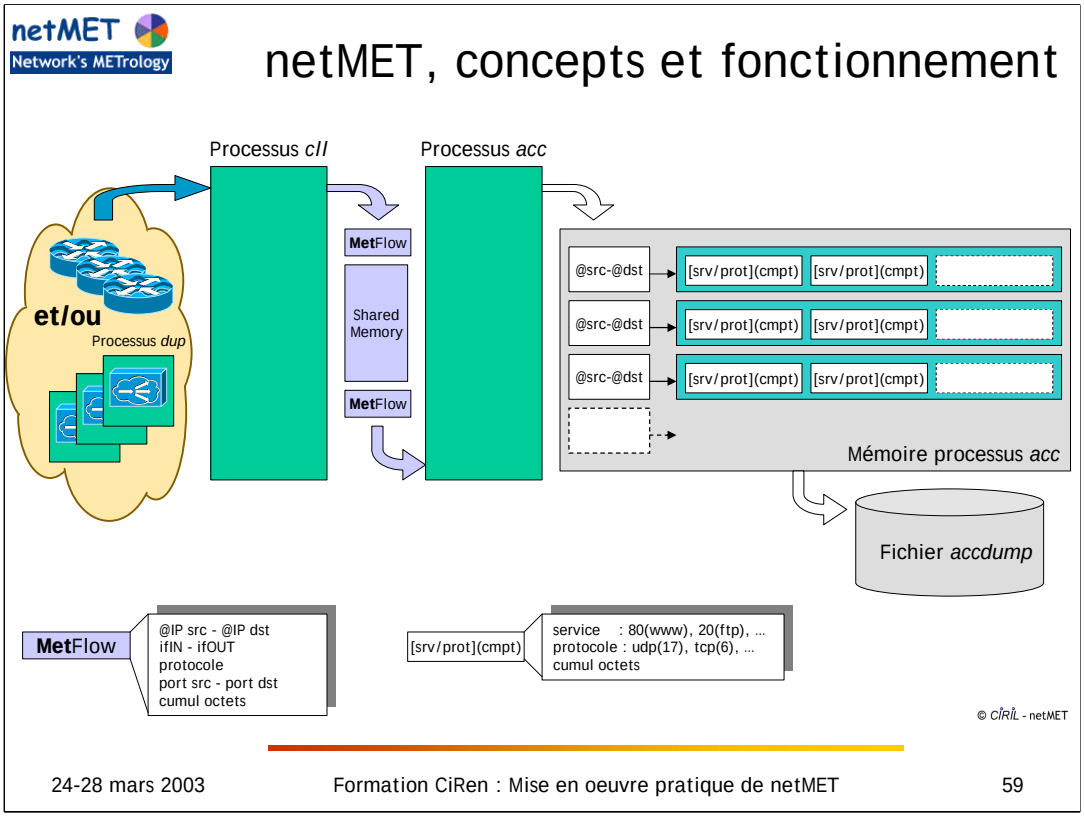
1. techniquement il n'était pas raisonnable de collecter les "différents points de vue" par un seul et même collecteur…
2. la séparation de chaque collecteur offre une grande souplesse :
   - possibilité d'activer ou non une collecte donnée (ex. "ne pas faire de sécurité")
   - possibilité de créer d'autres collecteur dédiés (test, backup, …)
   - possibilité de dispatcher les collecteurs sur différentes machines (une machine "métrologie générale" qui fait tourner "metro" et "stats", une machine "sécurité" qui fait tourner "secure10m" et "secure24h"), après l'exploitation peut se faire sur une seule et même machine.
3. les informations collectées (sémantiques et granularités) satisfont l'ensemble des besoins de métrologie : métrologie générale et sécurité avec une granularité minimum de 5mn.

Personnellement, je suis convaincu que ces 4 collecteurs suffisent… pour plus de valeurs ajoutées il faut regarder du côté de l'exploitation…

netMET Network's METrology

netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - le collecteur netMET se décompose en 2 processus
    - un processus de collecte des datagrammes *UDP NetFlow*
      - décode les paquets datagrammes aux formats 1, 5 et 7
      - applique des règles de traitement et agrégation sur les flows
      - formate des *MetFlow* (flow de métrologie) pour l'accounting
    - un processus d'accounting de *MetFlow*
      - construit et alimente ses structures de données en mémoire avec des *MetFlow*
      - génère des fichiers d'accounting binaires : image de la mémoire



MetFlow : un Flow de METrologie au sens netMET.

Un certain nombre de choix ont été fait quant aux informations que netMET devait manipuler. netMET est prévu pour faire de "la métrologie quantitative octets pour des trafics IP entre machines sources et destinations". Les informations disponibles dans les MetFlow sont donc **nécessaires et suffisantes** pour réaliser cette problématique.

Il ne faut pas demander à netMET de faire autre chose : métrologie sur champ TOS ou sur champ TCP_FLAGS, matrice de flux AS (bien que cela soit faisable si l'on connaît de façon exhaustive les machines appartenant à chaque AS… mais de manière directe cela n'est pas possible!)

Le fichier dump (nommé par défaut : `zzaccounting.dmp` dans les répertoires UNIX) est une image de la mémoire du processus d'accounting à un instant t. La génération de ce fichier se fait par la commande "`netMETacc --dump`" (ou arrêt du collecteur : "`netMETcll --kill`").

Un fichier dump contient des informations de métrologie pour une période donnée :

- entre le démarrage du collecteur et la demande de dump
- entre le redémarrage du collecteur et la demande de dump

Un fichier dump **n'est pas un fil de l'eau** !

Si une machine A a conversé plusieurs fois avec une machine B, le couple { A => B } n'apparaît qu'une seule fois dans le fichier, par contre les compteurs des services/protocoles utilisés auront été incrémentés de nombre octets correspondants à chaque communication.

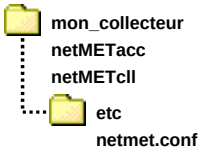
On perd donc la notion de flux entre 2 machines…

On pourra uniquement dire "**entre telle heure et telle heure, la machine A a fait … vers la machine B avec telle quantité**".

On parle ici **d'accounting** et pas de fil de l'eau.

netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - les règles de traitement et d'agrégation sur les flows par netMETcll sont exprimées dans un fichier de configuration
    - fichier `etc/netmet.conf` (1 par collecteur)



    - utilisation d'une grammaire puissante qui permet d'exprimer pratiquement tous les cas de figure : voir documentation « Collecteur & fichier de configuration *netmet.conf* »

Pour la configuration du collecteur et la syntaxe du fichier employée… je n'en dis pas plus dans cette présentation : se reporter à la documentation "Collecteur & fichier de configuration *netmet.conf*"

Il est important de bien lire cette documentation, car elle permet :

- d'apprendre à bien configurer le collecteur et ainsi avoir une bonne maîtrise des informations collectées
- mais surtout de bien comprendre le fonctionnement interne du collecteur et ainsi de connaître les possibilités du collecteur et les implications de l'utilisation des règles.

netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - La grammaire de `etc/netmet.conf`

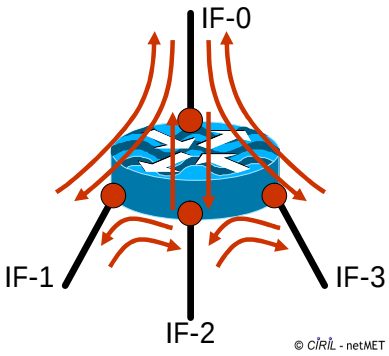
```
NETFLOW_LISTEN_ADDR_PORT { hhh.hhh.hhh.hhh/pppp }

ggg.ggg.ggg.ggg1 /* router_1 section */
{
  SNMP_READ_COMMUNITY { "community" }

  IF_PROCESSED
   {
     ALL |
     IF_1 <-> IF_2 [, IF_n <-> IF_m ... ]
     /* Where IF_i = "SNMP ifDescr"
           or IF_i =  OTHER */
   }

  [ IF_AGGREGATION
   {
     IF_1 (aaa.aaa.aaa.aaa) [ , IF_n (aaa.aaa.aaa.aaa) ... ]
     /* Where IF_i = "SNMP ifDescr" */
   } ]
}

[ ggg.ggg.ggg.gggi /* router_i section */
{
  ...
} ]
```

netMET Network's METrology

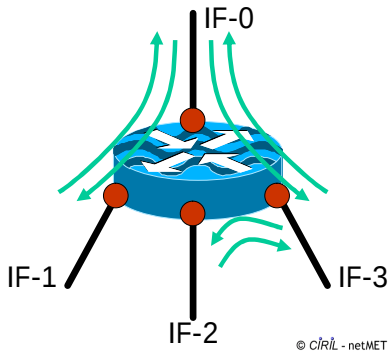
netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - Exemple de configuration

Activation du *NetFlow* sur un routeur à 4 interfaces donne des infos. sur les flux suivants



On ne veut conserver que les communications suivantes avec agrégation de l'interface IF-1 par 192.168.0.1 et IF-2 par 192.168.0.2



24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 62

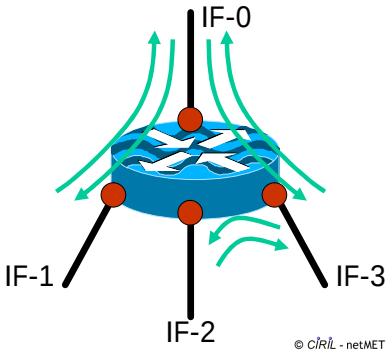
L'activation du NetFlow sur toutes les interfaces implique des sens de communications non souhaités. Le routeur ne permet pas d'éliminer avant exportation certains sens de communication. Pour résoudre ce problème le collecteur netMET utilise un fichier de configuration qui permet essentiellement deux choses :

- de ne conserver que certains sens de communication
- d'agréger (par une adresse symbolique) à la volée les @IP entrantes/sortantes d'une interface donnée.

netMET Network's METrology

netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - Exemple de configuration




```
/* 192.168.200.1 : machine netMET qui écoute sur le port 8080 */

NETFLOW_LISTEN_ADDR_PORT { 192.168.200.1/8080 }

192.168.200.254 /* mon routeur NetFlow */
{
  SNMP_READ_COMMUNITY {  "la_communauté_read_SNMP" }

  IF_PROCESSED
   {
            "IF-0" <-> "IF-1" ,
            "IF-0" <-> "IF-3" ,
            "IF-2" <-> "IF-3"

   }

  IF_AGGREGATION
   {
            "IF-1" (192.168.0.1) ,
            "IF-2" (192.168.0.2)
   }
}
```

© CIRIL - netMET

netMET Network's METrology

netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - *cll* reconnaît les versions 1, 5 & 7 de *NetFlow*
  - *acc* reconnaît les protocoles et services à partir de `/etc/protocols` et `/etc/services`
  - taille de la table [@src-@dst] dépend
    - de l'utilisation de l'agrégation ou non-agrégation
    - du nombre de machine sur le réseau
    - des attaques
  - Contraction du volume d'info.
    - *NetFlow* sur une journée (≈1,6Go) ⇨ fichier *accdump* (≈8Mo)

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 64

Le processus d'accounting construit pour un couple {addrSRC - addrDST} une liste de services/protocoles avec les quantités octets échangées. Pour la reconnaissance des protocoles et services connus, le processus s'appuie sur les fichiers de configuration du système :

- `/etc/protocols`

```
ip      0       IP              # internet protocol, pseudo protocol number
icmp    1       ICMP            # internet control message protocol
ipencap 4       IP-ENCAP        # IP encapsulated in IP (officially ``IP'')
tcp     6       TCP             # transmission control protocol
udp     17      UDP             # user datagram protocol
…
```

- `/etc/services`

```
tcpmux          1/tcp                           # TCP port service
multiplexer
echo            7/tcp
echo            7/udp
ftp             21/tcp
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
finger          79/tcp
www             80/tcp          http            # WorldWideWeb HTTP
…
```

Au démarrage, netMETacc "charge" ces fichiers et vérifie leur cohérence : un protocole utilisé dans `/etc/services` DOIT EXISTER dans `/etc/protocols`… si il existe une incohérence entre ces fichiers on obtient l'erreur :

```
[E] - initKNOWNprot_serv/getprotobyname() - src/accMETdata.c/271 :: No such
file or directory
```

netMET Network's METrology

netMET, concepts et fonctionnement

- La collecte et l'accounting : netMETcll - netMETacc
  - *acc* n'accepte que les protocoles connus (cf. `/etc/protocols`)
    - sinon *warning* dans `/var/log/netmet`
      `[W] - accMetFlow - protocol UNKNOWN : 6`
  - *acc* accepte des services inconnus (cf. `/etc/services`) algorithme d'identification du service :

```
identify__serv_proto( proto , port_destination , port_source )
{
  if( proto != connu )
    print «  [W] - accMetFlow - protocol UNKNOWN : proto »;
    exit;

  if     ( port_destination == connu )
    return service = port_destination;
  elseif (port_source == connu )
    return service = port_source;
  else
    return service = port_destination;
}
```

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 65

Les performances du collecteur sont directement dépendantes du nombre de flows que le collecteur reçoit et de taille de la table [@src - @dst] qu'il doit géré.

La taille de la table [@src - @dst] dépend :

- de l'utilisation de l'agrégation ou non-agrégation :
  dans le cas de l'agrégation des adresses IP de l'Internet ("le trou noir Renater") le process associé est
  peu chargé (metro et stats)
  dans le cas de non-agrégation (pour la sécurité) le process associé peut être très chargé (secure10m et secure24h)
- du nombre de machine sur le réseau :
  plus il y a de machine sur le réseau à mesurer, plus les combinaisons @src-@dst sont grandes
  donc plus la table [@src - @dst] est grande
- du nombre d'attaques :
  netMET se positionne généralement sur le routeur fédérateur, il voit donc tous les trafics passer même
  si ceux-ci sont supprimés par des ACL en aval. Selon ce principe toutes les attaques à base de "scans"
  sont donc détectées par netMET et ceci donne lieu à la création de nouvelles entrées dans la table [@src - @dst]. Une machine pirate de l'Internet qui scanne une réseau de classe C va créer au moins
  255 entrée dans cette table…

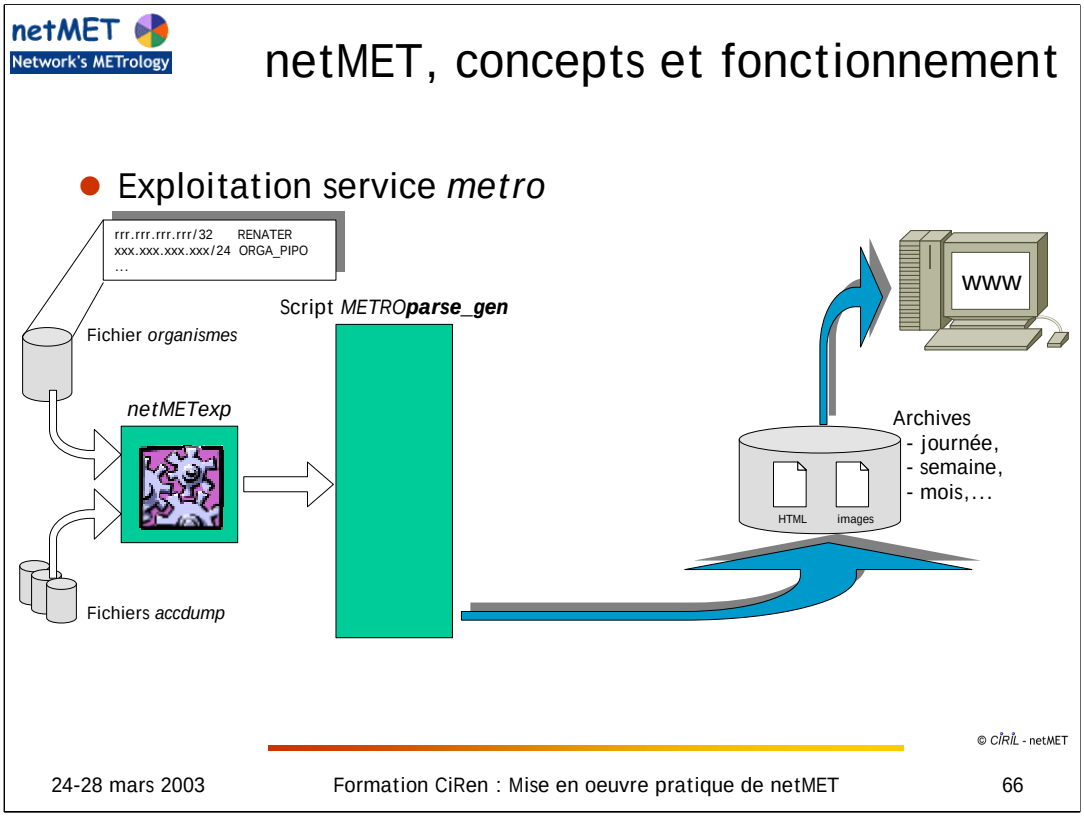
==> si la machine n'est pas correctement dimensionnée (mémoire+CPU), les attaques peuvent saturer le système et rendre indisponible la machine de production (plus de mémoire / plus de CPU ==> swap ==> recouvrement process ==> plantage général !!!)

La liste des protocoles connus doit être exhaustive dans `/etc/protocols` :

- si netMETacc reçoit un flow avec un protocole non déclaré dans `/etc/protocols`, il le signale par un
  WARNING

Par contre la reconnaissance des services est à la charge de l'administrateur : à lui de compléter/modifier le fichier `/etc/services` pour reconnaître ou non certain services.

A VOIR, L'ALGORITHME DE RECONNAISSANCE DES SERVICES !!!



Le service *metro* est utilisé pour la génération :

- TOP n général des machines

- TOP n général des organismes

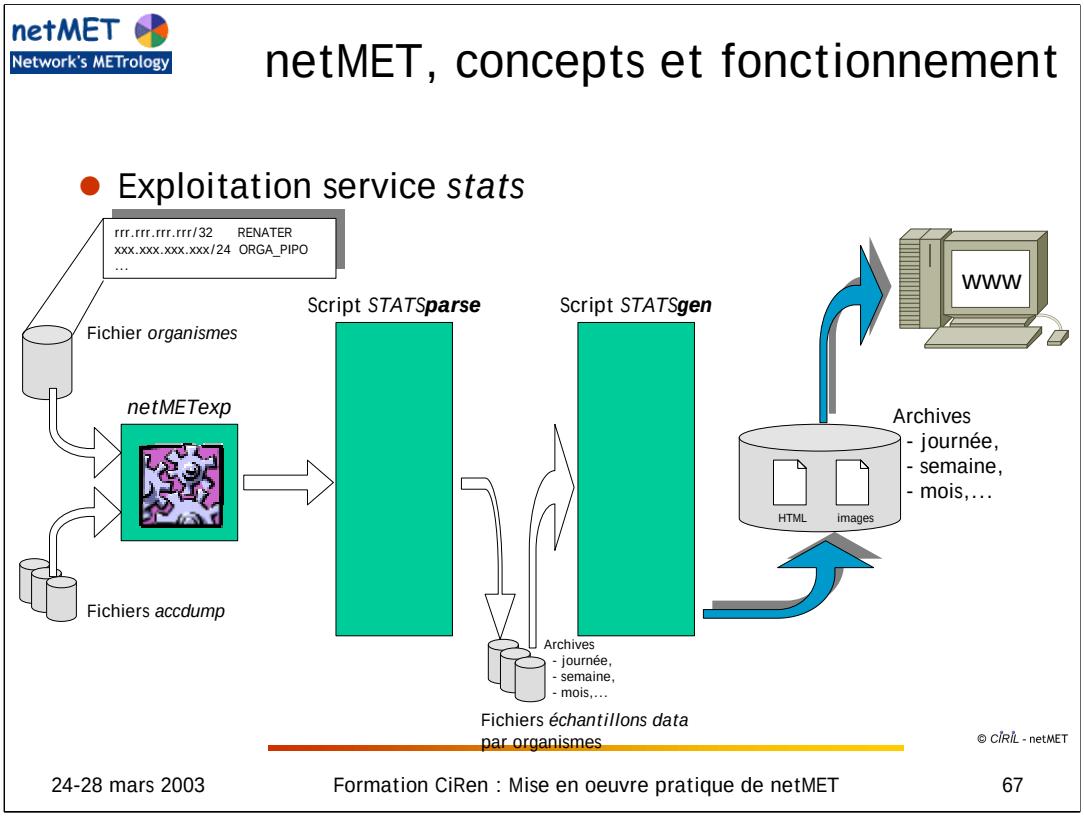
- TOP n locaux dans les organismes

- Métrologie détaillée par organisme

Certaines informations de métrologie font apparaître directement des IP de machines mais il est possible de manipuler des "organismes" qui sont des regroupements d'adresses IP et subnets de classes réseau (classes A, B et C).

Un fichier définition des organismes (`organism.def`) est utilisé par les différents scripts d'exploitation pour proposer de la métrologie par organisme :

- TOP n général des organismes
- TOP n local dans les organismes
- les statistiques Renater par organisme
- la métrologie détaillée (protocoles et services/protocoles) par organismes



Le service *stats* est utilisé pour la génération :

- Statistiques Renater de type *MRTG* par organisme

netMET, concepts et fonctionnement

- Exploitation services *secure10m* et *secure24h*
  - depuis 09/2001, suite aux stages
    - **Peyman GOHARI** 2000 et **Cyril PROCH 2001**
    - détection de scans (scan en hauteur et scan en largeur)
  - depuis 08/2002, reprise complète
    - **Sébastien MOROSI**
    - performances accrues
    - rapports de scans par organismes + rapports texte pour CERT
  - les données collectées sont également utilisables pour
    - *netMET LookUp*
    - à terme : détection de problèmes de *sécurité sur profils*

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 68

Les services *secure10m* et *secure24h* n'étaient pas présents dans les premières versions de netMET. L'approche "sécurité à base de métrologie" n'avait pas été envisagée mais :

- la connaissance des informations de base (TOP et statistiques) nous poussaient à en savoir plus
- les demandes de traitement de problèmes de sécurité sont apparus
- la faisabilité existait (d'après les infos. collectées nous savions que nous pouvions en faire qq chose)…

donc pourquoi pas ?!?

Les services de collecte *secure10m* et *secure24h* existent depuis plus d'1 an (septembre 2000) et n'étaient utilisés que par *netMET LookUp*. Aujourd'hui ils sont utilisés pour les détections de scans.

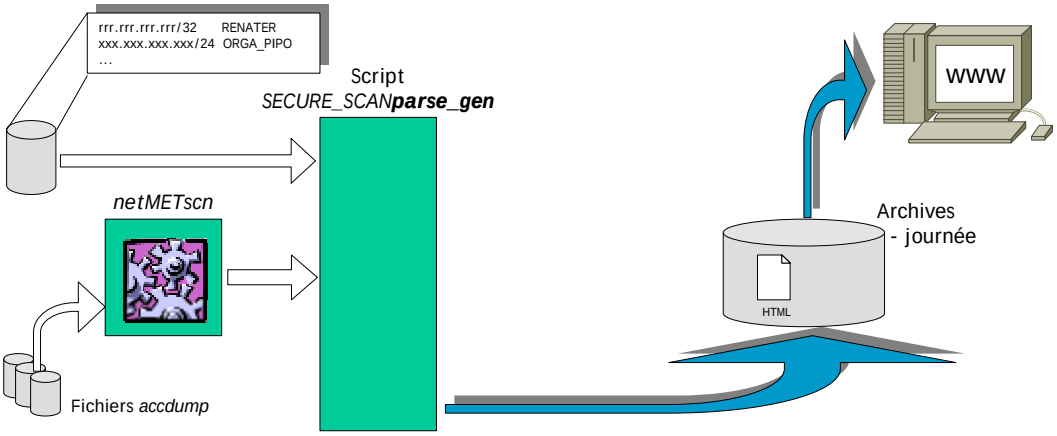
L'exploitation autour des services de sécurité n'est pas terminée… il reste beaucoup de chose à faire :

- présenter différemment les résultats de détection de scans
- faire de la détection de problèmes de *sécurité sur profils*

netMET
Network's METrology

netMET, concepts et fonctionnement

- Exploitation service *secure10m* et *secure24h*



Les services *secure10m* et *secure24h* sont utilisés pour la génération de :

- Détection de scans en "hauteur" et "largeur"

netMET Network's METrology

netMET, concepts et fonctionnement

- Les scans en "largeur" et scans en "hauteur"

Liste des scans en HAUTEUR *depuis RENATER*

Machine source : 172.10.0.87

	Réseaux	Organismes	Horaires	Nb machines scannées	Services scannés	Nb réponses
1	192.168.209.0	"ORGA1"	06:40-7:00	255	[22/t]	0
2	192.168.210.0	"ORGA2"	06:50-7:00	255	[22/t]	1
3	192.168.213.0	"ORGA1" "ORGA2"	06:50-7:00	192	[22/t]	4
4	192.168.222.0	"ORGA3"	06:50-7:00	255	[22/t]	18
5	192.169.1.0		06:50-7:00	240	[22/t]	15
6	192.169.2.0	"ORGA2"	06:50-7:00	255	[22/t]	6
7	192.169.3.0	"ORGA4"	06:50-7:00	255	[22/t]	6
8	192.170.200.0	"ORGA5"	06:50-7:00	255	[22/t]	7

Liste des scans en LARGEUR *depuis RENATER*

	Machine source	Machine destination	Horaires	Nb services
1	tots.orga1.fr (192.168.200.1)	61.103.90.22	06:00	681
2	61.103.90.22	toto.orga1.fr (192.168.200.1)	06:00	814
3	tots.orga2.fr (192.168.202.1)	suspect.mal.intentionne.fr (122.203.45.21)	09:20	524
4	machine.quelque.peu.bizarre.fr (172.10.2.3)	192.168.222.3	11:10	584
5	suspect.mal.intentionne.fr (122.203.45.21)	toto.orga1.fr (192.168.200.1)	12:10	1524
6	62.0.0.1	192.169.200.5	12:10	1521

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 70

netMET définit 2 types de scans :

- scan en "hauteur" : il y a scan en "hauteur" lorsqu'une machine communique avec plus de n machines d'un même réseau. Ce phénomène se traduit au niveau des structures de données manipulées par un grand nombre d'entrées @src-@dst différentes.
- scan en "largeur" : il y a scan en "largeur" lorsqu'une machine communique avec une seule machine destination mais sur un grand nombre de service. Ainsi, pour une entrée @src-@dst on trouvera une longue liste de services d'où le terme de scan en "largeur".

netMET Network's METrology

netMET, concepts et fonctionnement

- *netMET LookUp* : outil de recherche multi- critères
  - idées :
    - lancer des *grep* évolués dans les fichiers de collecte
    - répondre rapidement à « y a t-il un réel problème? »
  - applications :
    - choix d'un fichier de recherche (agrégé ou non, période)
    - choix machine source, destination, source et ou destination
    - choix service/protocole
    - choix quantité
    - ...
  - permet d'exprimer des requêtes quotidiennes simples (et parfois même compliquées) pour une première approche sécurité

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 71

Les 4 services *metro*, *stats*, *secure10m* et *secure24h* sont utilisés par *netMET LookUp*.

Idée de base :

- en consultant les informations de base (TOP et statistiques) j'étais intrigué par le comportement de certaines machines
- pour regarder ça de plus près, je me connectais en *telnet* sur la machine de production et à grands coups de "`netMETexp`" et "`grep`" je recherchais exactement ce qu'avait fait cette machine
- voyant que les "`grep`" étaient toujours les mêmes… l'idée du netMET LookUp avec son interface sur le web commençait à se préciser.

Aujourd'hui, netMET LookUp permet de répondre très facilement et assez rapidement aux questions classiques que l'on peut se poser en cas de problèmes avec une machine.

A lire :"netMET LookUp : Outil de recherche multicritères".

A voir : quelques requêtes réelles pour se rendre compte des possibilités de l'outil…

netMET Network's METrology

netMET, concepts et fonctionnement

- Les binaires netMETxxx
  - *netMET**dup***
    - duplicateur de datagrammes *UDP NetFlow*
  - *netMET**cll*** & *netMET**acc***
    - processus de collecte et d'accounting
    - arrêt, démarrage et redémarrage à partir de *netMETcll*
    - *dump* de l'accounting dans le fichier binaire
  - *netMET**exp***
    - pré-exploitation rapide des fichiers d'accounting *accdump*
    - rend lisible et facilement exploitable l'accounting
  - *netMET**scn***
    - pré-exploitation rapide des fichiers d'accounting *accdump* pour l'approche détection de scans
    - publication brute des scans en "hauteur" et des scans "largeur"

netMET, concepts et fonctionnement

- Les binaires netMETxxx
  - arguments des exécutables au format *GNU* :
    - -o [...]
    - --option [...]
    - aide en ligne pour tous les exécutables : *netMETxxx --help*

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 73

Tous les binaires sont utilisables en ligne de commande.
Pour connaître les paramètres et options : lancer `netMETxxx -- help`
Les paramètres et options peuvent être au format court (`-H`) ou au format long (`--HOSTaccprint`).

Quelques commandes rapides :
- `netMETcll --start` : démarrage du collecteur
- `netMETcll --kill` : arrêt du collecteur avec génération automatique du fichier dump
- `netMETacc --dump` : demande de génération manuelle du fichier dump
- `netMETexp --accinfo` : informations sur le fichier de collecte (heures, tailles, ...)
- `netMETexp --HOSTaccprint zzaccounting.dmp` :
  impression des infos. de collecte au format machine (impression avec @IP)
- `netMETexp --ORGAaccprint zzaccounting.dmp --ORGAfile etc/organism.def` :
  impression des infos. de collecte au format organisme (impression avec noms d'organismes définis dans `organism.def`)
- ...

netMET, concepts et fonctionnement

- Les binaires netMETxxx
  - quelques remarques sur *netMET**exp*** :
    - interfaçage entre fichiers *dump* bruts et exploitation
    - transcription binaire-ascii
    - pré-traitement de l'information
      - impression par machine ou organisme (avec différentes options)
      - recherche des machines inconnues / fichier d'organisme
      - manipulation et test manuel du fichier d'organisme
      - informations sur les fichiers *dump* (périodes, tailles, …)
    - utilisation sympathique en ligne avec « | grep »
    - format de sortie standard
      - @IPsrc @IPdst [service/protocole](quantité en octets) …

```
193.55.2.1      194.214.110.110 [53/17](7193) [65535/1](156) [137/17](1170)
193.54.11.1     194.214.110.110 [80/6](40)
194.214.110.110 152.81.17.1     [65535/1](280)
```

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 74

Le format de sortie de `netMETexp` est standard. Il n'est pas prévu d'en changer et toute l'exploitation repose sur ce format :

```
@IPsrc  @IPdst [service/protocole](quantité en octets) …
```

Je vous encourage vivement en cas de problème à utiliser `netMETexp` et à regarder de plus près les fichiers de collecte…

Il est également possible de programmer soi-même quelques scripts (*shell* ou *perl*) pour des recherches ponctuelles à lancer automatiquement dans un *cron*…

netMET, concepts et fonctionnement

- Les scripts *perl* netMET
  - noms des scripts…
    - « SSSScccc1_cccc2-tttt1_tttt2.pl »
    - SSSS
      - METRO : métrologie générale
      - STATS : statistiques *Renater*
      - SECURE10m : sécurité sur 10mn
      - SECURE24h : sécurité sur 24h
    - cccc
      - cron : scripts lancé par *cron*
      - parse : analyse des fichiers de données
      - gen : génération des fichiers *HTML* et images
    - tttt
      - fréquence d'activation du script (10 = 10 ' , daily, …)

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 75

Le nommage des répertoires et scripts de netMET est à priori très cohérent/explicite : à tous moments on peut savoir "où l'on est", "d'où viennent les données manipulées" et "ce qu'est susceptible de faire un script/exécutable"…

Dans ce contexte les scripts d'exploitation respectent les conventions décrites dans la diapositive, et avec ces noms on sait exactement **ce que** doit faire un script et **quand** il le fait.

Il existe aujourd'hui une petite exception pour les scripts de sécurité, car cette approche n'étant pas tout à fait finalisée, nous conservons la liberté de compléter les scripts SECURE_*

Les scripts d'exploitation :

```
INDEXgen-daily.pl
METROcron-10.pl
METROcron-daily_weekly_monthly.pl
METROparse_gen-daily_weekly_monthly.pl
SECURE10mcron-10.pl
SECURE24hcron-10.pl
SECURE_SCANScron-daily.pl
SECURE_SCANSparse_gen-daily.pl
STATScron-5.pl
STATScron-daily.pl
STATScron-weekly_monthly.pl
STATSgen-daily_weekly_monthly.pl
STATSparse_gen-daily.pl
STATSparse_gen-weekly_monthly.pl
netMETtk.pm
```

netMET Network's METrology

netMET, concepts et fonctionnement

- Les scripts *perl* netMET
  - appels des scripts…
    - « nom_du_script fichier_de_configuration [période] »
    - fichier_de_configuration :
      - path vers les différents exécutables, variables globales…
    - période :
      - période sur laquelle le script s'exécute : journée, semaine ou mois
      - journée : ***aaaa-mm/aaaa-mm-jj***
      - semaine : ***aaaa-Week#nn***
      - mois : ***aaaa-mm/Month***

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 76

Tous les scripts d'exploitation (sauf les scripts de *cron*) peuvent être lancés manuellement à posteriori, avec la condition suivante : que les données collectées pour la période à regénérer existent toujours (répertoires `~/data/`… et `~/secure/`…)

Ainsi tous les scripts :

```
INDEXgen-daily.pl
METROparse_gen-daily_weekly_monthly.pl
SECURE_SCANSparse_gen-daily.pl
STATSgen-daily_weekly_monthly.pl
STATSparse_gen-daily.pl
STATSparse_gen-weekly_monthly.pl
```

peuvent être lancés "à la main", selon le format : "nom_du_script fichier_de_configuration période".

netMET Network's METrology

netMET, concepts et fonctionnement

- Démarrage et arrêt de la machine…
  - utilisation du processus *init SysV*,
  - démarrage et arrêt automatique de tous les services
    - démarrage/arrêt du processus
    - activation/désactivation *cron*
  - Démarrage… reprise sur fichier ?
    - metro : reprise à partir du dernier fichier *dump*
    - stats : non reprise, mais fichiers échantillons valides
    - secure10m - secure24h : non reprise
- Machine autonome avec peu de maintenance journalière, métrologie cohérente

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 77

Le démarrage et arrêt des services netMET respectent le processus *init SysV* :
- arrêt/démarrage de services particuliers selon le *run-level* (boot et arrêt de la machine)
- possibilités de lancer, relancer ou arrêter des services

Comment travailler sur netMET :
- tout peut (et DOIT) se faire en user `netmet` : tous les droits sont validés pour le user `netmet`. De plus
  IL NE FAUT PAS travailler en `root`, sinon si on repasse en user `netmet`, les fichiers générés en `root`
  vont poser problème.
- pour le démarrage/arrêt des services il faut être en root et utiliser :
  * `/etc/rc.d/init.d/netmetDUP [start/stop/restart]`
  * `/etc/rc.d/init.d/netmet [start/stop/restart]`
  * `/etc/rc.d/init.d/netmetSECURE [start/stop/restart]`

- `netmetDUP` : lance le duplicateur de flows
- `netmet` : lance les services les collecteurs "metro" et "stats" et charge les *crontab* associées
- `netmetSECURE` : lance les services les collecteurs "secure10m" et "secure24h" et charge les *crontab* associées

Où sont les logs ???
- netmet : `/var/log/netmet`
- apache : `/var/log/httpd/*`

netMET Network's METrology

Plan

- Introduction

- Les informations proposées
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Dimensionnement d'un serveur netMET

Dimensionnement d'un serveur netMET

- 3 points essentiels
  - la CPU
  - la mémoire centrale
  - l'espace disque
- Points à dimensionner selon :
  - la taille du(es) lien(s) mesuré(s)
  - le nombre de machines sur le réseau mesuré
    - machines effectives (réelles)
    - machines potentielles (somme classes A, B, C)
  - le nombre de flows à traiter
  - les services souhaités
    - métrologie + statistiques simples
    - sécurité

Dimensionnement d'un serveur netMET

- Alors… que choisir ?
  - il n'y a pas de recette miracle
  - il n'y a que des expériences acquises et des points de repères
- Machine pour métrologie et statistiques simples
  - dépend peu de la « taille » du réseau car flows agrégés
  - machine moyenne :
    - PII monopro 200MHz à PIII monopro 500MHz
    - 128 à 512 Mo de RAM
    - 8Go à 18Go de disque

Dimensionnement d'un serveur netMET

- Machine pour metro, stats + sécurité
  - dépend de la « taille » du réseau car flows non-agrégés
  - machine performante :
    - PIII monopro 700MHz à PIII bi-pro 1GHz
    - 512Mo à 1Go de RAM
    - 10Go à +++Go de disque
- Recommandations :
  - le bi-processeur est vraiment adapté à netMET
  - la mémoire centrale est importante car collecte en mémoire
  - plus de disque = plus d'archives
  - !!! recompilation du noyau Linux !!! (pas de multimédia pour netMET)

netMET Network's METrology

Dimensionnement d'un serveur netMET

- Qq chiffres :
  - html (.html et images) = 1-1.5Mo par période
  - metro
    - journée ≈ 6.5Mo
    - semaine ≈ 45Mo
    - mois ≈ 200Mo
  - stats
    - journée ≈ 31Mo
    - semaine ≈ 220Mo
    - mois ≈ 950Mo
  - secure24h
    - journée ≈ 50-60Mo
  - secure10m
    - journée ≈ 100-120Mo

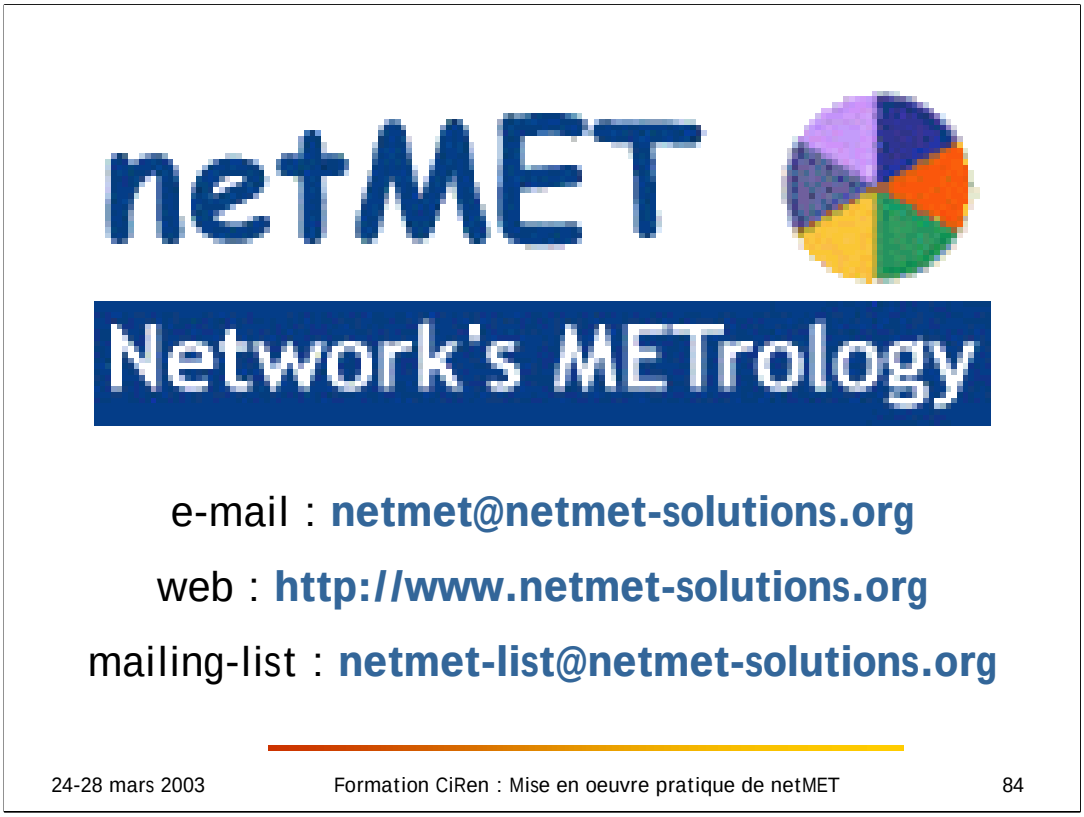
Dimensionnement d'un serveur netMET

- Conclusion :
  - 18Go pour metro et stats
    - archives sur plus d'1 an
  - 2.5Go pour secure24h et secure10m
    - archives sur 15 jours
- Exemple pour Lothaire :
  PIII bi-pro 700MHz, 512 Mo, 18+8 Go SCSI
  - lien Renater2 = 62Mb/s
  - 15 000 et 20 000 machines effectives (125 000 potentielles)
  - 30-35 millions de flows par jour
  - metro, stats, secure10m et secure24h

24-28 mars 2003 Formation CiRen : Mise en oeuvre pratique de netMET 83

Aujourd'hui comme il n'existe pas de "recette miracle" pour dimensionner un serveur de production et que les conseils se font plus par expérience, j'ai dans l'idée de :

- faire une enquête auprès des utilisateurs actuels pour connaître leurs configurations (réseau : routeur,
  nb de flow, … machine Linux : version, CPU, mémoire, services activés, …),
- de publier ces infos. sur le web de netMET,
- et permettre ainsi à chacun de voir selon son contexte si sa machine de production est bien dimensionnée.


netMET
Network's METrology
e-mail : netmet@netmet-solutions.org
web : http://www.netmet-solutions.org
mailing-list : netmet-list@netmet-solutions.org
24-28 mars 2003
Formation CiRen : Mise en oeuvre pratique de netMET
84