netMET – Network's METrology

Un an après…
Fonctionnement, projet et conditions d'accès,
évolutions à venir

Groupe de travail netMET
21 juin 2001 - Campus Jussieu, PARIS

netMET *netmet@netmet-solutions.org*
Alexandre SIMON *Alexandre.Simon@ciril.fr*

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- Dimensionnement d'un serveur netMET

netMET Network's METrology

Introduction

- Pourquoi cette réunion ?
  - netMET a officiellement 1 an depuis le 26 avril 2001
  - les fonctionnements de base sont quasiment stables
  - de nouvelles orientations ont été explorées
  - pour faire le point sur :
    - le fonctionnement (NetFlow, netMET, ...)
    - le projet et les conditions d'accès
    - les évolutions à venir
  - pour permettre aux utilisateurs (anciens et nouveaux) :
    - de (re)découvrir netMET
    - de se rencontrer et d'échanger leurs points de vue
    - d'exprimer les attentes et besoins
    - de s'impliquer dans le projet

netMET Network's METrology

Introduction

- Historique depuis 1 an
  - 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

netMET Network's METrology

Introduction

- Historique depuis 1 an (suite)
  - 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
  - février-mai 2001
    - rédaction de documentations
      - fonctionnalités
      - installation
      - configuration
    - réécriture complète du web netMET
    - création domaine *netmet-solutions.org*

netMET Network's METrology

Introduction

- Historique depuis 1 an (suite)
  - février-mai 2001 (suite)
    - étude LICENCE et conditions d'accès
    - ajouts/modifications pour netMET-2.4beta
  - 21 juin 2001 : Campus Jussieu
    - **Présentation** netMET un an plus tard
  - juin-septembre 2001
    - stage Cyril PROCH : orientation sécurité, détection de scans et métrologie pour matrice de flux interne, + ???
  - décembre 2001 : JRES2001 Lyon
    - **Présentation** netMET, ok depuis le 13/06/2001.

netMET Network's METrology

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- Dimensionnement d'un serveur netMET

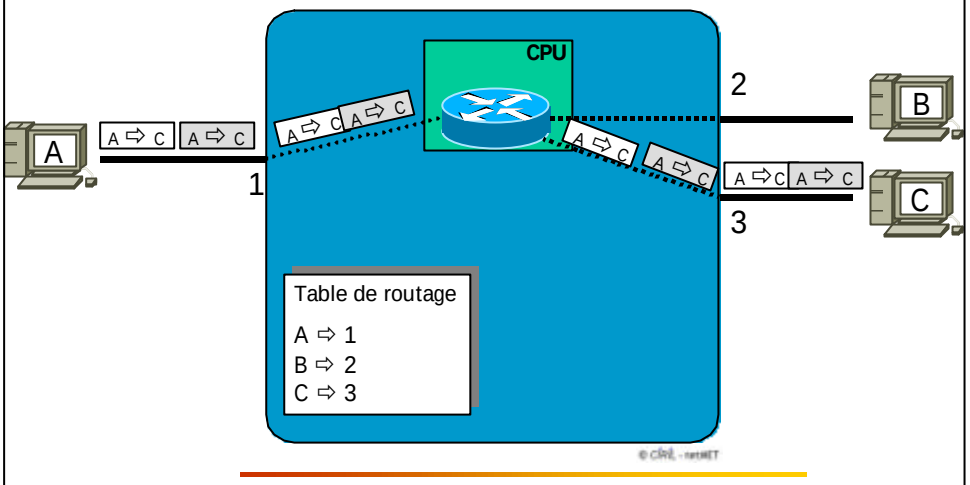
netMET Network's METrology

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

NetFlow Cisco

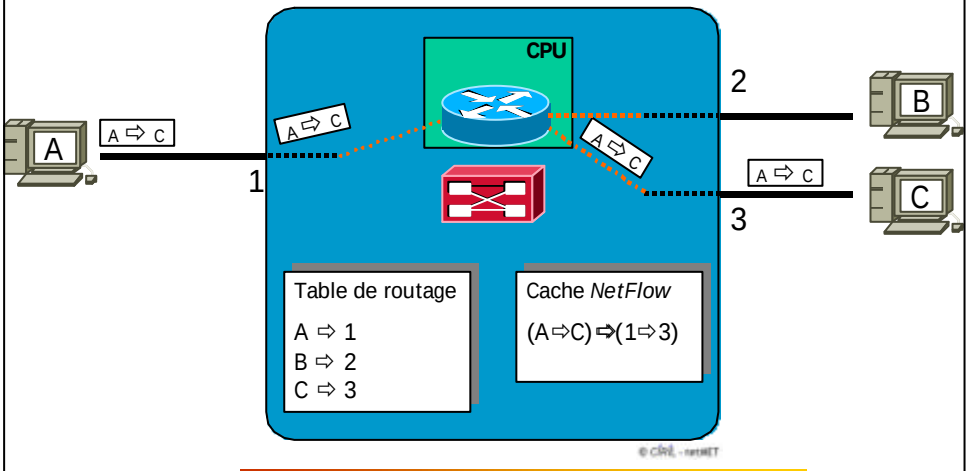
- Le routage « classique »



21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 9

NetFlow Cisco

- Le routage « accéléré »

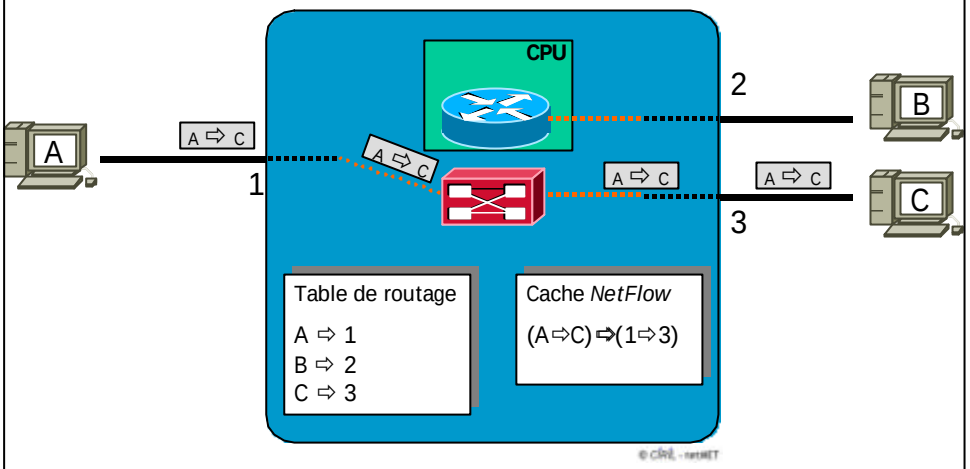


21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 10

netMET Network's METrology

NetFlow Cisco

- Le routage « accéléré »



netMET Network's METrology

NetFlow Cisco

- Principes de la technologie *NetFlow*
  - accélération *NetFlow* mise en œuvre par
    - *IP FastSwitching*
    - ou *CEF - Cisco Express Forwarding* (distribué ou non)
    - ou *MLS - Multi-Layer Switching*
  - Optimisation des *ACLs* (*Access Control List*)
    - vérification du 1er paquet par la *CPU*
    - puis « accélération » des suivants...
  - Gestion du cache
    - invalidations sur détection de fin de flux (*END* et *RST* en *TCP*)
    - invalidations cycliques des entrées
      - après 15s d'inactivité (essentiellement pour *UDP*)
      - après 30mn d'activité
    - invalidation sur cache plein

netMET Network's METrology

NetFlow Cisco

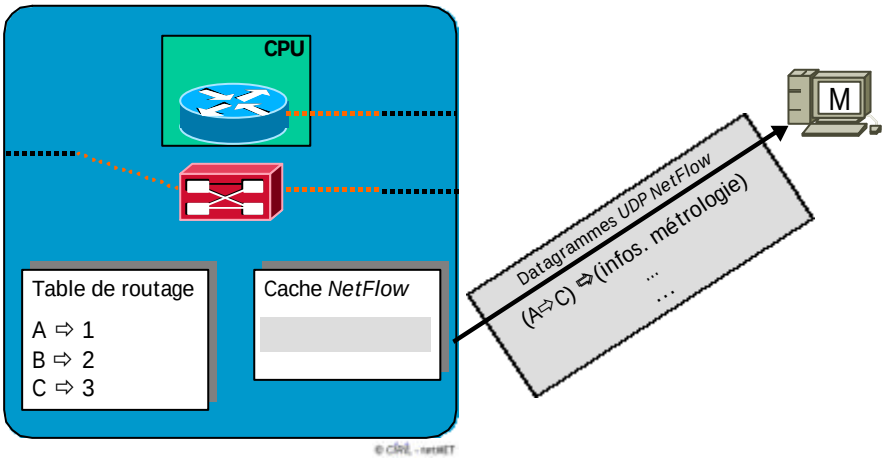
- Principes de la technologie *NetFlow*
  - Gestion du cache (suite)
    - configuration des invalidations cycliques des entrées
      - temps d'inactivité (*timeout inactive*) défaut 15s
      - temps d'activité (*timeout active*) défaut 30mn
    - configuration sur routeur avec commandes :
      `ip 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 !
    - le 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 !

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 13

netMET Network's METrology

NetFlow Cisco

- Envoi d'informations de métrologie sur invalidation



21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 14

netMET Network's METrology

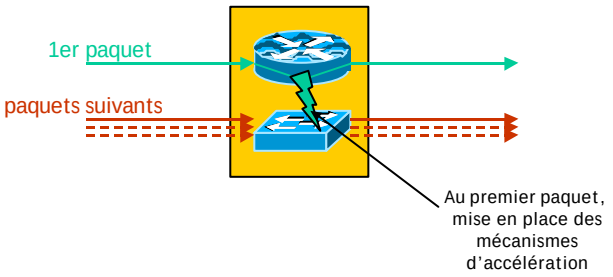
NetFlow Cisco

- 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 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

netMET Network's METrology

NetFlow Cisco

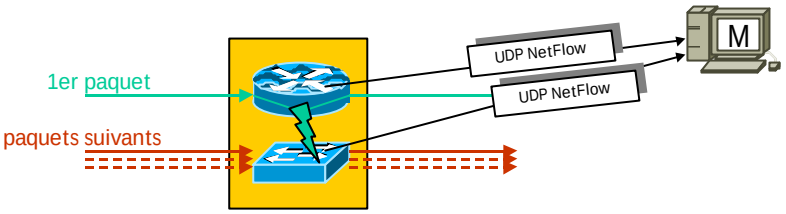
- Attention dans switch/routeur, il y a switch et routeur



netMET Network's METrology

NetFlow Cisco

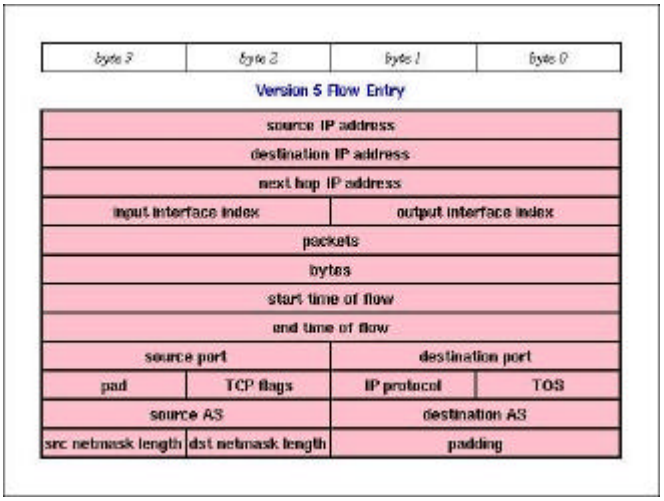
- Attention dans switch/routeur, il y a switch et routeur
  - il faut donc activer le NetFlow sur les parties
    - routeur pour le 1er paquet
    - switch pour les paquets suivants
  - il faut exporter les information de flows depuis
    - le routeur pour la métro sur le 1er paquet
    - le switch pour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



netMET Network's METrology

NetFlow Cisco

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



netMET Network's METrology

NetFlow Cisco

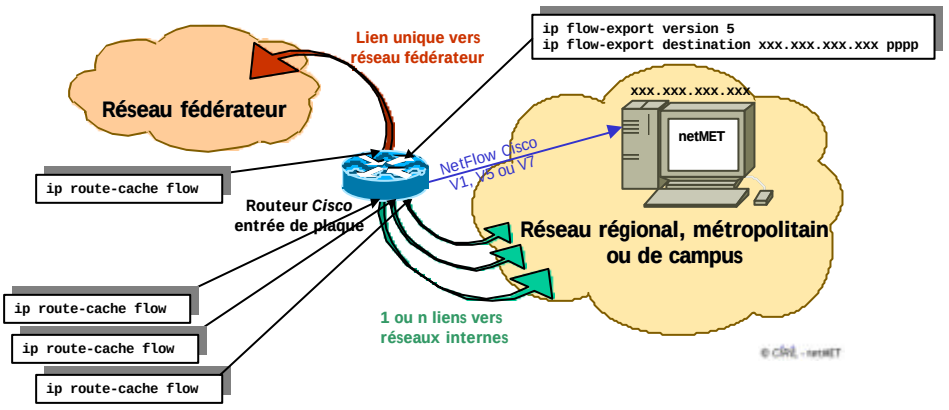
- Activation du *NetFlow* sur un routeur
  - activation par interface physique (impossibilité d'activer sur une sous-interface, sauf ISL)
  - configuration de la machine distante pour les envois d'informations de métrologie
  - l'activation sur une interface donne lieu à l'envoi d'informations de métrologie ***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

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 19

netMET Network's METrology

NetFlow Cisco

- Activation du *NetFlow* sur un routeur



21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 20

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`

netMET Network's METrology

Plan

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

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

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

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 25

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 que 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

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 26

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

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

netMET Network's METrology

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- Dimensionnement d'un serveur netMET

netMET Network's METrology

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 ?

netMET Network's METrology

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 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

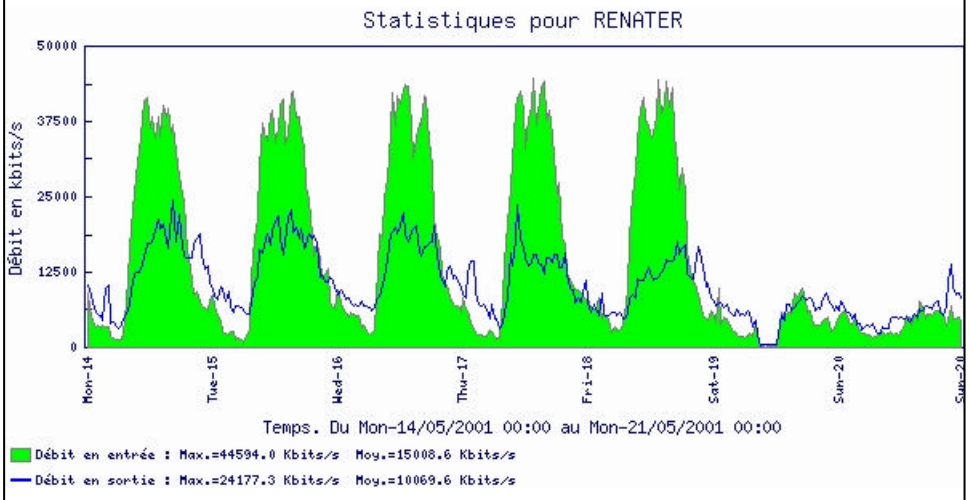
netMET Network's METrology

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**						

netMET Network's METrology

metaMET, le coût de la métrologie



netMET Network's METrology

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- Dimensionnement d'un serveur netMET

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

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 35

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

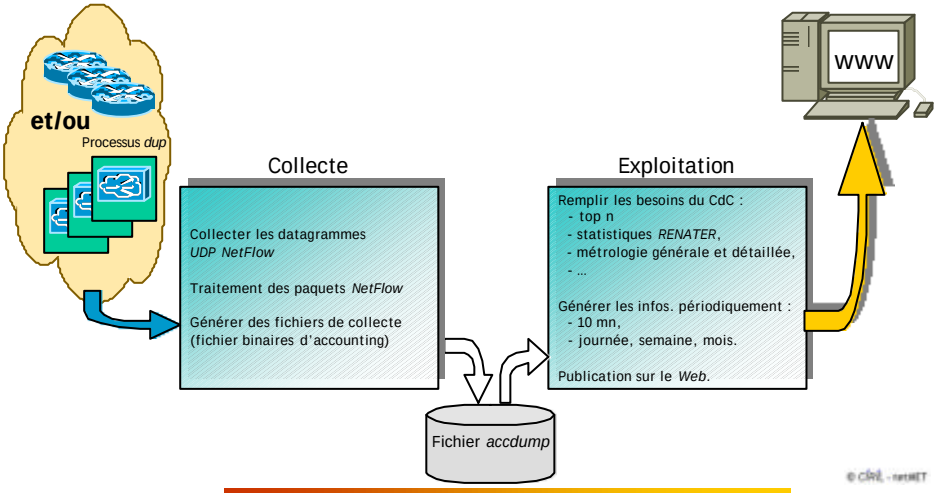
21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 36

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...

netMET, concepts et fonctionnement

- Architecture de la solution



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

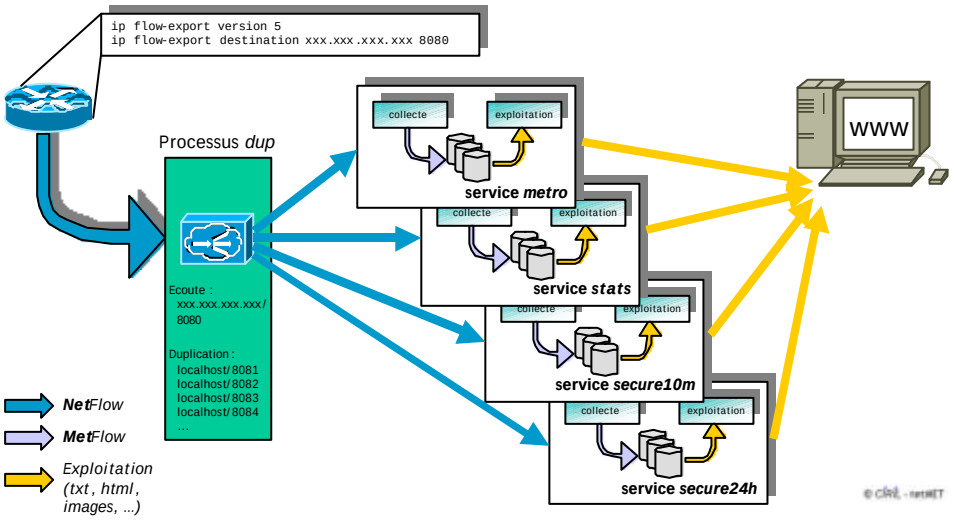
netMET, concepts et fonctionnement

- 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, 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, concepts et fonctionnement



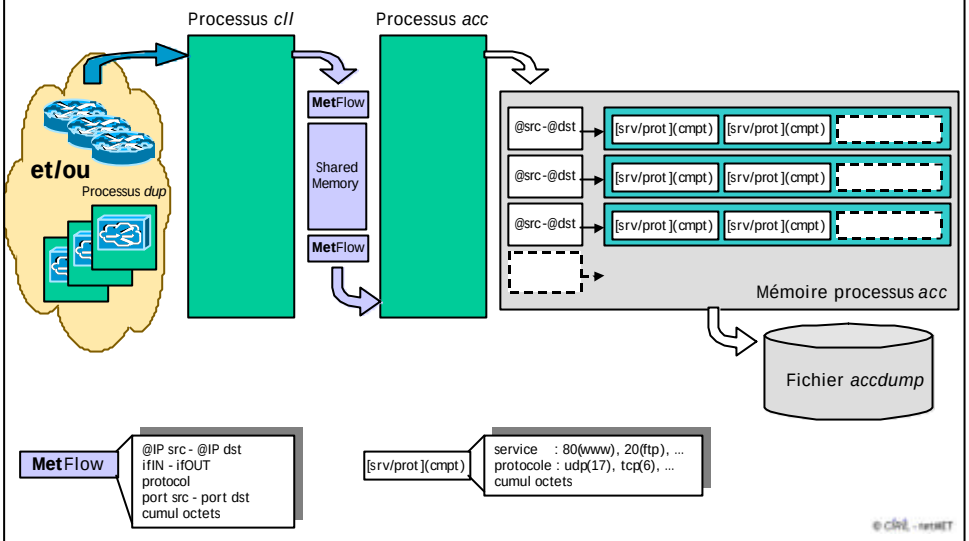
netMET, concepts et fonctionnement

- 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

netMET, concepts et fonctionnement

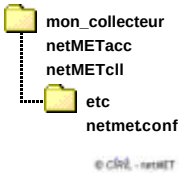
- La collecte et l'accounting : netMETcll - netMETacc
  - le collecteur netMET se décompose en 2 processus
    - un processus de collecte des datagrammes *UDP NetFlow*
      - décode les paquets datagrammes aux formats 1, 5 et 7
      - applique des règles de traitement et agrégation sur les flows
      - 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

netMET, concepts et fonctionnement



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* »

netMET, concepts et fonctionnement

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

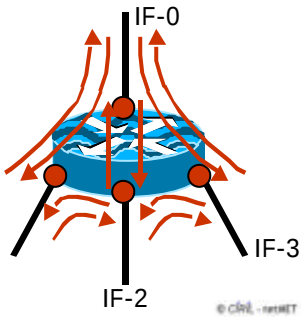
```
NETFLOW_LISTEN_ADDR_PORT { hhh.hhh.hhh.hhh/pppp }

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 */
{
  ...
} ]
```

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 47

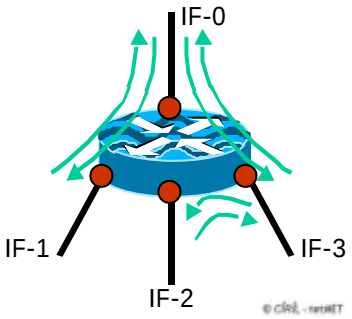
netMET, concepts et fonctionnement

- 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



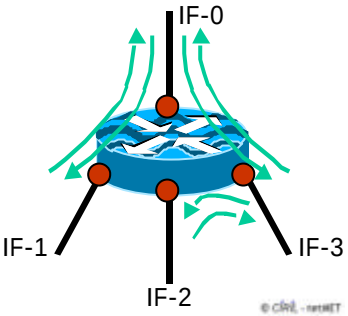
On ne veut conserver que les communications suivantes avec agrégation de l'interface IF-1 par 192.168.0.1 et IF-2 par 192.168.0.2



21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 48

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)
   }
}
```

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 49

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
    - du nombre de machine sur le réseau
    - des attaques
  - Contraction du volume d'info.
    - *NetFlow* sur une journée (≈1,6Go) ⇨ fichier *accdump* (≈8Mo)

21 juin 2001 netMET - Un an après... Fonctionnement, projet et évolutions 50

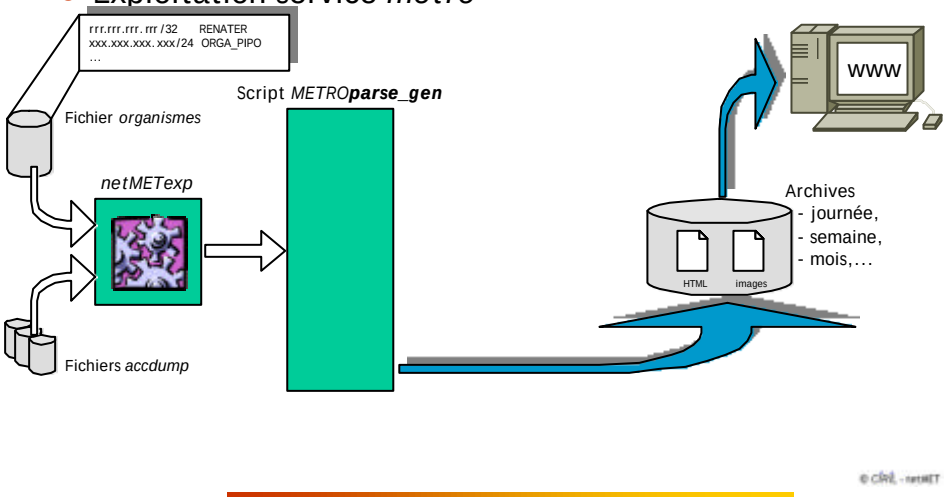
netMET, concepts et fonctionnement

- 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;
}
```

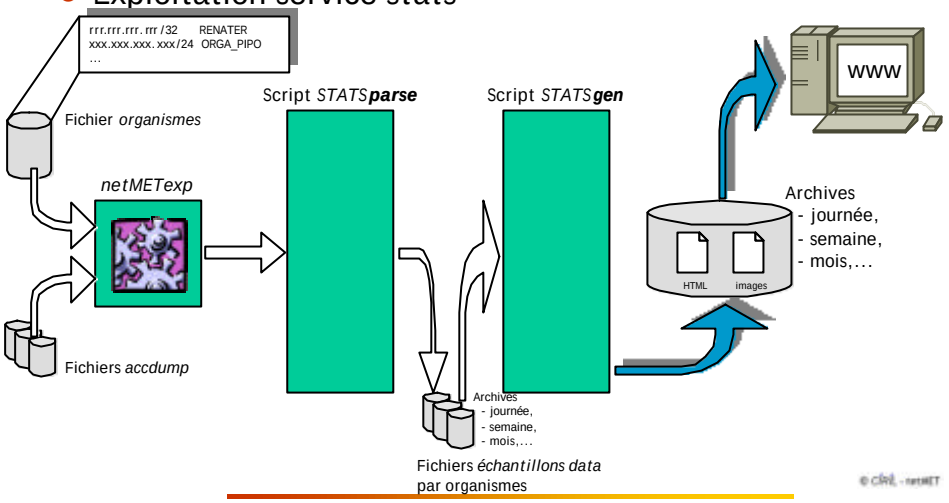

netMET, concepts et fonctionnement

- Exploitation service *metro*



netMET, concepts et fonctionnement

- Exploitation service *stats*



netMET, concepts et fonctionnement

- Exploitation service *secure10m* et *secure24h*
  - pour l'instant rien !
  - utilisable et très complet pour *netMET LookUp*
  - utiliser à terme pour l'approche sécurité :
    - détection de scans
    - détection de problèmes de *sécurité sur profils*

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

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

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 p/r au 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)
```


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, …)

netMET, concepts et fonctionnement

- Les scripts *perl* netMET
  - appels des scripts...
    - « nom_du_scripts 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***

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 le 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

netMET Network's METrology

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- Dimensionnement d'un serveur netMET

netMET Network's METrology

Domaine, web et mail netMET

- *netmet-solutions.org*
  - déposé depuis avril-mai 2001
  - le domaine de référence de la solution de métrologie netMET
- *www.netmet-solutions.org*
  - le web officiel de netMET (dispo. au plus tard pour 09/2001)
  - réécriture et portage de l'ancien web en cours
  - vocations de ce nouveau web :
    - présentation
    - documentation
    - téléchargement distributions et outils officiels
    - support
    - contacts

Domaine, web et mail netMET

- *netmet@netmet-solutions.org*
  - concepteur et gestionnaires du projet (dispo. actuellement)
  - disponibilité plus grande, mise au courant et contact de tous les gestionnaires (plus de copies en Cc)
  - traitement des demandes plus simple pour les gestionnaires
- *netmet-list@netmet-solutions.org*
  - mailing-list sous Sympa de la solution netMET (dispo. au plus tard pour 09/2001)
  - remplace l'actuelle *netmet@ciril.fr*
  - contact entre utilisateurs, wg et gestionnaires projet netMET

Plan

Projets et actions à venir

- Basculement sur domaine *netmet-solutions.org*
  - finir le web de netMET
  - e-mail et liste de diffusion sous Sympa
- Modification de la structure du répertoire *html*
  - faciliter l'accès restreint
  - authentifications/permissions sur la base d'*apache*
- Modification de la distribution netMET
  - faire de moins en moins de système : juste des recommandations
  - ne packager que l'essentiel : netMET, structures, perl, install.

Projets et actions à venir

- Approche sécurité : détection de scans
  - approche déjà étudiée en août-septembre 2000
  - idée :
    - sur la base des collectes *metro*, *stats*, *secure10m* et *secure24h*
    - faire une liste des réseaux scannés avec comme infos :
      - réseaux scannés
      - service/protocole scannés
      - machine source
      - périodes et heures du scans
  - reste à faire :
    - portage définitif du source *C* : *netMETscn*
    - écriture de l'exploitation en perl
    - doc.

Projets et actions à venir

- Approche sécurité : système d'apprentissage et construction de profils
  - idée :
    - sur la base des collectes *metro*, *stats*, *secure10m* et *secure24h*
    - apprendre l'utilisation normale du réseau
      - construire un profil pour chaque machine/réseau
    - envoyer une alerte sur dépassement d'un profil normal
      - déterminer les « bonnes » métriques
      - déterminer les dérives normales de ces métriques
      - déterminer les seuils d'alertes
  - reste à faire :
    - tout !

21 juin 2001 netMET - Un an après… Fonctionnement, projet et évolutions 67

Projets et actions à venir

- Métrologie pour matrice de flux interne
  - aujourd'hui, l'exploitation netMET est orientée « mesure d'un lien unique/multiple vers un réseau fédérateur (l'Internet) »
  - idée :
    - proposer un schéma de déploiement du *NetFlow*
    - sur la base de nouvelles collectes
    - construire toutes les informations de métrologie d'échanges de flux entre sites : multi-liens, multi-sites
  - reste à faire :
    - le collecteur netMET est déjà adapté à cette approche
      - ??? à voir ??? extension du collecteur pour faire de l'agrégation à la volée sur la base du fichier d'organisme
    - écriture de l'exploitation en perl
    - doc.

21 juin 2001 netMET - Un an après… Fonctionnement, projet et évolutions 68

netMET Network's METrology

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- Dimensionnement d'un serveur netMET

netMET Network's METrology

Licence netMET et conditions d'accès

- Licence et conditions d'accès en cours d'élaboration
- Premières approches :
  - définir au CIRIL (sous la tutelle de l'UHP) les idées générales de licence et d'utilisation de netMET
    - ok... + appel à une juriste UHP
  - définir le mode de distribution de la solution (libre, formulaire, mot de passe, ...)
    - pas ok...

Licence netMET et conditions d'accès

- et après… :
  - la notion de Licence en France se signifie rien, il nous faut :
    - déposer la marque netMET
    - déposer le CIRIL-UHP comme auteur (pour les droits d'auteur) de netMET
  - écrire la Licence (sous forme US) et les conditions d'accès (sous forme FR)
  - mettre en place le mode de distribution de la solution

Licence netMET et conditions d'accès

- Aujourd 'hui :
  - Licence et conditions d'accès
    - aucune garantie
    - pas de distribution des sources *C*
    - pas de redistribution de la solution / documentation autre que par le CIRIL
      - dernières version/patch/documentation disponibles
      - versions « officielles »
    - toutes utilisations de netMET doit être mentionnée
      - utilisation de la solution
      - utilisation des résultats
    - tous produits dérivés de netMET doit être mentionné
      - « développement à base de netMET »

Licence netMET et conditions d'accès

- Aujourd 'hui :
  - Distribution de la solution
    - pas encore de mode de distribution
    - sur simple demande au CIRIL
    - respect du contrat moral

Plan

- Introduction
- NetFlow Cisco
- NetFlow Cisco, news
- metaMET, le coût de la métrologie
- netMET, concepts et fonctionnement
- Domaine, web et mail netMET
- Projets et actions à venir
- Licence netMET et conditions d'accès
- 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 machine 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 peut 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)

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