ACCT-CISCO : une comptabilité IP libre

■ Pierre DAVID, Pierre.David@prism.uvsq.fr
Université de Versailles, St Quentin en Yvelines

Cette présentation décrit acct-2.0, un logiciel pour récupérer et exploiter les informations de comptabilité IP maintenues par les routeurs CISCO.
Le rapport journalier envoyé (par mail) à l'administrateur réseau comprend des informations de trafic, bien sûr, mais également des rapports d'anomalie (trafic martien, réseaux non routables, machines non enregistrées dans le DNS, etc.).
Deux effets secondaires de cette comptabilité IP sont très intéressants :
- *d'une part, la trace du trafic peut servir à analyser l'origine de problèmes de sécurité,*
- *et d'autre part, ces informations permettent de suivre la charge d'une liaison et d'optimiser son débit.*

La version 2.0 présentée ici apporte une bien plus grande rapidité de traitement par un recodage des fonctions essentielles en langage C.

■ Introduction

La mesure du trafic sur une liaison est un problème auquel sont confrontés tous les ingénieurs réseau. A l'heure actuelle, deux classes d'outils sont disponibles :

- ceux bâtis sur une machine interceptant des paquets : on peut citer *NNStat*, ou *IPtrafic,* ce dernier étant développé conjointement par l'UREC et le CRU. Ces outils sont très performant et précis, mais le revers de la médaille est qu'ils sont souvent lourds à mettre en œuvre, et la technologie employée les contraint à ne traiter que des trafics peu volumineux, ou alors à procéder à des échantillonnages lorsque les trafics sont plus importants ;
- ceux utilisant le protocole SNMP pour interroger périodiquement les compteurs associés aux interfaces des routeurs que l'on souhaite surveiller. Le plus connu est certainement *MRTG* (Multi Router Traffic Grapher), très facile à mettre en place. Malheureusement, des outils tels que MRTG ne peuvent donner qu'une vue très grossière du trafic. De plus, MRTG impose une démarche volontariste : l'ingénieur réseau doit s'armer de son butineur Web pour explicitement consulter les pages HTML générées.

Le logiciel « acct-cisco » utilise une troisième technique, liée fortement aux routeurs de marque Cisco. Ces routeurs ont en effet la caractéristique de pouvoir comptabiliser tout le trafic en transit. En récupérant périodiquement ces informations de comptabilité sur une machine Unix, on peut obtenir simplement, par courrier électronique, des rapports détaillés sur le trafic tout en évitant les problèmes exposés ci-dessus.

De plus, si ces informations sont archivées, le responsable sécurité d'un réseau dispose de données qui se révèlent précieuses :

- pour détecter des problèmes, tels que des flux anormaux, ou des *scans* complets de réseaux ;
- en cas d'incident, pour repérer les flux de et vers la station attaquée ;
- ou lors de la publication d'un avis du CERT, pour vérifier si le réseau est susceptible d'avoir été attaqué ou non.

Ces exemples sont réels, l'auteur en ayant fait l'expérience...

La première version du logiciel « acct-cisco » a été développée en 1994. Elle a été mise en service sur deux sites tests (Jussieu et l'UVSQ) puis rendue disponible en ftp anonyme et installée dès lors sur quelques sites. Lorsque le trafic à traiter est devenu trop important, les temps de traitement quotidiens sont devenus prohibitifs. Une partie a été réécrite en langage C, et les temps de calcul à l'UVSQ (liaison RERIF à 2 Mbit/sec) sont à l'heure actuelle d'environ 10 minutes (sur un PC récent sous FreeBSD) pour traiter le trafic de la journée écoulée et établir le rapport.

■ Comptabilité CISCO

Les routeurs de marque Cisco ont la possibilité de comptabiliser les datagrammes IP en transit. Pour ce faire, ils mémorisent une table à quatre colonnes :

adr. IP source	adr. IP destination	nombre de paquets	nombre d'octets

Cette table, dont le nombre d'entrées est par défaut 512, est mise à jour à chaque fois qu'un datagramme IP est routé. Les deux premières colonnes correspondent à un couple de machines ayant échangé des données. Les troisième et quatrième colonnes contiennent, respectivement, le nombre de datagrammes IP et le nombre d'octets ayant transité. Lorsqu'une communication est bidirectionnelle, ce qui est le cas le plus fréquent, on trouvera deux entrées pour le même couple de machines.

En récupérant cette table à intervalles suffisamment rapprochés (par exemple toutes les minutes), il est possible de traiter les informations pour en extraire un rapport quotidien. Le logiciel décrit dans le reste de cet article a pour objet de récupérer cette table, puis de la traiter et d'en extraire le rapport quotidien.

■ Rapport quotidien

Cette section décrit le rapport quotidien et ses différentes sous-parties. Ce rapport est envoyé automatiquement, toutes les nuits, après le traitement. Il se décompose en sous-parties :

- informations de débit : débit utile mesuré, en kilo-octets par seconde. Le débit correspond à la somme du débit entrant et du débit sortant ;
- informations sur la table de comptabilité : nombre d'entrées utilisées, saturations éventuelles de la table, pannes du routeur, etc.
- transactions suspectes : datagrammes IP avec une adresse source ou une adresse destination suspecte (ou les deux)
- machines non enregistrées dans le DNS : machines locales ayant émis des données, alors qu'elles ne sont pas enregistrées dans le DNS
- top50 des connexions : les 50 plus gros consommateurs internes et externes, ainsi que les 50 plus grosses connexions.
- courbe de trafic : la courbe est générée en ASCII pour tenir dans un courrier « normal »...

Ces différentes sous-parties sont toutes facultatives. Il est possible d'éliminer, par exemple, le rapport des machines non enregistrées dans le DNS, ou encore le top50 des connexions. Le reste de cette section décrit les sous-parties du rapport.

Informations de débit

La première partie correspond au débit mesuré :

```
Débit utile en Ko/s :
       Moyenne : 137,479042719
       Ecart-type : 111,231546957
       Minimum : 1,93919270833
       Maximum : 645,172151693
```

Le débit utile correspond au débit réel (nombre d'octets réel) ayant transité sur la ligne. Les données fournies dans ce rapport doivent être toutefois considérées avec circonspection, car elles dépendent fortement de la précision avec laquelle sont effectuées les relèves de la table de comptabilité. Une machine chargée au moment de la relève traitera l'interrogation du routeur plus lentement, ce qui fera que le trafic constaté pendant la période sera plus important. D'où un débit maximum qui sera exagéré. L'écart type s'en ressentira d'autant.

Informations sur la table de comptabilité

```
Nombre d'entrées dans la table d'accounting :
     Moyenne :    490,105628909
```

```
Machines non enregistrées dans le DNS : 5. Ce sont :
    193.51.30.90
    193.51.31.193
    193.51.34.57
    193.51.37.107
    193.51.39.97
```

```
Lignes invalides dans le fichier de log : 2. Les lignes concernées sont :
     422457
     422458

Pannes du routeur : 1. Les dates sont :
     0534
```

Cette sous-partie donne des indications sur le nombre d'entrées utilisées dans la table de comptabilité. Si celle-ci est saturée, il faut envisager d'en augmenter la taille (la commande à utiliser est décrite dans la section « installation »). Cette sous-partie référence également les lignes invalides dans le fichier contenant les tables de comptabilité récupérées, ce qui ne devrait théoriquement jamais arriver, mais qui arrive parfois dans la pratique : par exemple, si une récupération est trop lente, pour une raison ou une autre, la récupération suivante peut commencer sans que la précédente soit terminée, ce qui provoque des écritures concurrentes dans le fichier. Enfin, si la table de comptabilité a une date donnée n'est pas trouvée, cela signifie qu'un problème est survenu, soit sur le routeur, soit sur la machine récupérant les informations de comptabilité.

Transactions suspectes

Une transaction suspecte correspond à un datagramme ayant une au moins des adresses IP source ou destination suspecte. Dans l'exemple ci-dessus, la première transaction, datée de 0h0m, correspond à un datagramme avec une adresse source « non routable » au sens de la RFC 1918. Le deuxième exemple correspond à une adresse source et une adresse destination toutes deux extérieures au réseau : un tel paquet ne peut théoriquement pas passer par ce routeur, sauf si une machine locale est mal configurée, ou si une attaque intervient. Enfin, le troisième cas correspond à une adresse source ou destination se terminant par 0 ou 255, ce qui correspond *généralement* à des adresses invalides.

Machines non enregistrées dans le DNS

Cette sous-partie indique les machines locales non enregistrées dans le DNS ayant émis des datagrammes. Cela permet, par exemple, de faire la chasse aux machines installées sans que l'administrateur en soit averti.

Top 50 des connexions

Cette sous partie référence les connexions elles-mêmes, sous forme de couples :

```
Transactions suspectes : 451.
   M = adresse martienne (x.y.z.0 ou x.y.z.255)
   E = paquet extérieur -> extérieur
   R = réseau non routable
 Heure MER IP src                    IP dest        Pqts       Octets
   0000         R   172.26.136.38   193.51.24.1       6          336
   1202       E     195.16.7.16     195.42.160.104    2           80
   1410    M        193.51.27.98    193.51.27.255    25         2544
```

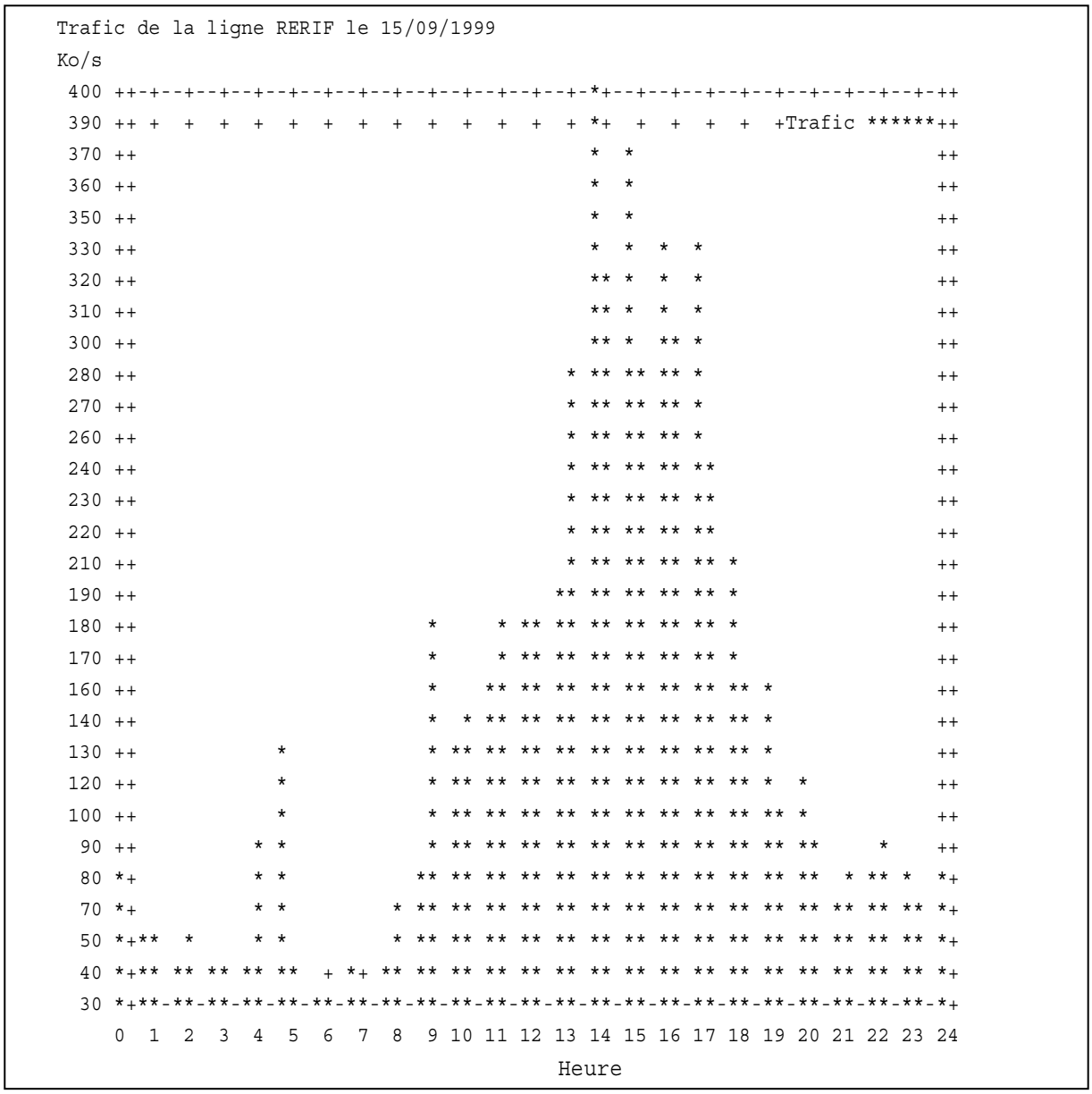
Puis sont indiqués les plus gros consommateurs internes et externes :

```
Les 50 plus grosses connexions
Adresse 1        Adresse 2            Trafic 1->2          Trafic 2->1   %
soleil.uvsq.fr   exemple.fictif.fr    1.845.528.321        12.398.016 17,03
soleil.uvsq.fr   ? (193.220.102.109)  647.108.59           10.993.562  6,03
soleil.uvsq.fr   autre.exemple.com    551.548.467          7.378.324  5,12
...
```

```
Les 50 plus gros consommateurs internes
Machine                                  In                   Out   %
soleil.uvsq.fr                   551.930.687       5.531.922.709 55,78
...

Les 50 plus gros consommateurs externes
Machine                                  In                   Out   %
exemple.fictif.fr              1.845.528.321          12.398.016 17,03
? (193.220.102.109)              647.108.592          10.993.562  6,03
...
```

Courbe de trafic



La courbe est générée en ASCII de façon à être lisible dans un courrier « normal ». Il est clair que ces courbes ne brillent pas par leur élégance, mais elles permettent de donner rapidement, chaque matin, une idée du trafic de la veille. Un utilitaire est également fourni pour générer, à la demande, des courbes en PostScript (ou tout autre langage compris par l'utilitaire Gnuplot).

■ Ce qui n’est pas mesuré

Le rapport détaillé dans la section précédente donne une vision du trafic global, ainsi que des problèmes potentiels détectés dans la phase d'analyse.

Dans certains cas, on désire affiner l'étude du trafic : flux par type de protocole, et non par machine. Le logiciel décrit ici ne permet pas de fournir cette information. Deux solutions complémentaires sont envisageables :

- utiliser un outil comme IPtrafic décrit en introduction ;
- utiliser la capacité des routeurs Cisco à envoyer des messages « syslog » lors des violations d'access-lists. Il suffit alors de mettre une access-list de type « permit » sur un port donné, et on peut

alors avoir une idée du nombre de datagrammes IP sur un ou plusieurs ports. Cette astuce ne donne pas un débit précis, mais donne quand même une indication.

Installation et configuration

L'installation est décomposée en plusieurs étapes :

- configuration de la comptabilisation sur le routeur Cisco ;
- installation de la relève des informations comptables ;
- installation et configuration du traitement quotidien.

Prérequis

Pour utiliser ce logiciel, vous devez disposer des utilitaires suivants sur votre système Unix :

- Perl (version 4 ou 5) ;
- Tcl (toutes versions) ;
- gcc (ou tout compilateur supportant le type « `long long` ») ;
- gnuplot (optionnel, seulement si on désire des courbes de trafic) ;
- système avec une commande « date » compatible avec les spécifications POSIX.

En ce qui concerne le routeur, toute version d'IOS postérieure à la version 9 devrait fonctionner.

Si toutes ces conditions sont remplies, vous pouvez procéder à l'installation. Il n'est pas nécessaire d'avoir les droits de l'administrateur (« root ») pour ce faire. Nous ne décrivons pas ici toute l'installation, nous renvoyons pour cela le lecteur intéressé au fichier « README » accompagnant la distribution. En revanche, les principes sont détaillés, ainsi que le fichier de configuration du traitement quotidien.

Configuration du routeur

La mise à jour de la table de comptabilité n'est pas activée par défaut sur les routeurs. Il faut donc la mettre en place explicitement par les commandes suivantes :

```
enable
conf
ip accounting
^Z
write mem
quit
```

Comme indiqué précédemment, la table fait par défaut 512 entrées. Si cette taille est insuffisante, il faut donner l'ordre de configuration :

```
ip accounting-threshold 2048
```

pour passer la table à 2048 entrées.

Relève des informations

La relève des informations de comptabilité fonctionne en émulant une session « telnet » sur le routeur. Les commandes envoyées au routeur sont :

```
clear ip accounting
show ip accounting checkpoint
clear ip accounting checkpoint
```

La première commande envoyée sauvegarde la table de comptabilité dans une table temporaire (la table « checkpoint »), et remet à zéro la table principale. La deuxième commande affiche la table temporaire. La troisième et dernière commande remet à zéro cette table pour ne pas surcharger la mémoire du routeur.

Ce mécanisme est automatisé par l'utilitaire « getacct ». Attention : il faut disposer de suffisamment de place dans le système de fichiers de l'ordinateur hôte pour stocker des données au format :

`date` *`aaaammjj hhmm`*

... puis la table de comptabilité.

Ce fichier peut atteindre une taille importante. Par exemple, à l'UVSQ, pour une liaison RERIF à 2 Mbit/sec, il dépasse couramment les 30 Mo en fin de journée.

Configuration du traitement quotidien

Le traitement quotidien est réalisé par l'utilitaire « daily ». Cet utilitaire :

- explore tous les fichiers de comptabilité non compressés, et les traite tous, sauf le dernier (qui est celui en cours de constitution pour la journée courante),
- pour chaque fichier, il génère un rapport, avec l'utilitaire « accsum »,
- pour chaque fichier, si nécessaire, il complète le rapport avec une courbe de trafic en ASCII, avec l'utilitaire « gengraph »,
- et enfin, il comprime le fichier traité.

Le fichier de configuration « bin/conf.* » contient la configuration pour l'utilitaire « accsum ». Il est conseillé de tester la syntaxe après toute modification en lançant « accsum » avec un seul paramètre, le nom de ce fichier de configuration. La distribution contient un fichier exemple abondamment commenté, on s'y référera pour toute modification. Toutefois, il convient de souligner deux points.

Le premier concerne le langage de filtrage. En effet, les utilitaires sont sans cesse occupés à ranger une adresse IP dans une classe (classe des adresses internes, classes des adresses externes, classes des adresses non routables au sens de la RFC 1918, etc.). Pour ce faire, une spécification de classe est une liste. Chaque élément de liste contient 3 champs : + ou -, une adresse et un masque. Un exemple simple permet d'introduire ce mini-langage :

La classe des adresses considérées comme non routables (voir RFC 1918) est composée :

- des adresses 127.0.0.0/8 (8 premiers bits significatifs),
- des adresses 10.0.0.0/8,
- des adresses 172.16.0.0/12,
- pas de l'adresse 192.168.0.0/20 (l'UVSQ utilise les réseaux de classe C 192.168.1.0 à 192.168.15.0

```
set conf(noroutables) {
     + 127.0.0.0    0.255.255.255
     + 10.0.0.0     0.255.255.255
     + 172.16.0.0   0.15.255.255
     - 192.168.0.0  0.0.15.255
     + 192.168.0.0  0.0.255.255
}
```

  pour ses besoins internes),
- de toutes les autres adresses 192.168.0.0/16,
- et c'est tout : toute autre adresse n'appartient pas à cette classe.

L'ordre est important : la première occurrence trouvée provoque l'arrêt de la recherche.

Le second point à souligner concerne les tables de hachage. Une partie de la récriture en C a eu pour objet d'améliorer l'accès aux informations de comptabilité étant donné une ou deux adresses IP. Pour ce faire, des tables de hachage ont été définies et utilisées. Le paramètre important de ces tables est leur taille : plus elle est grande, moins il y aura de collisions, et plus rapide sera l'accès aux informations. En revanche, si elle est trop grande, de la place mémoire sera occupée pour rien. Le rapport peut indiquer (paramètre « stathash » du fichier de configuration) l'occupation de ces tables. En pratique, il n'est conseillé de modifier ces paramètres que si la longueur des listes est constamment supérieure à quelques unités.

■ Consolidation des résultats

Le traitement quotidien gère une quantité importante de données, et le temps de calcul est en conséquence. Pour faciliter l'établissement de statistiques sur une longue période, sans pour autant traiter à nouveau les données brutes, le traitement quotidien génère un fichier (un par jour) synthétisé contenant des lignes de la forme :

hhmm n

où *hhmm* est l'heure et la minute, et *n* le nombre d'octets ayant transité pendant la minute.

L'utilitaire « gengraph » utilise ce fichier pour établir la courbe.

Il est possible d'exploiter ces fichiers pour tracer des courbes sur de plus longues périodes, pour calculer des moyennes horaires, etc. Le script « cumuls » fourni avec le logiciel représente une base pour cette consolidation de résultats.

Implémentation

Cette section décrit succinctement l'implémentation des différents composants du logiciel.

Le script de récupération des tables de comptabilité est écrit en shell de Bourne. Il utilise un utilitaire, « ciscot » (élément d'un logiciel « Pride Tools »), pour récupérer le résultat d'une session « telnet ».

Le script qui génère le rapport quotidien, « accsum », est de loin le plus complexe et le plus gourmand en temps de calcul. Il s'agit d'un script Tcl (environ 1300 lignes, dont environ un tiers de commentaires) utilisant des fonctions réécrites en langage C. Ces fonctions sont :

- `int64` : implémente une algèbre 64 bits (opérations classiques : +, -, *, /, %, comparaison, etc.) sur des machines 32 bits. Cette fonction utilise le type C « `long long` », extension de gcc et candidat pour la prochaine version de la norme C ANSI ;
- `traffic` : cumule des compteurs associés à des couples d'adresses IP ; cette commande utilise intensivement des tables de hachage pour accéder rapidement aux informations associées aux couples. Bien sûr, les compteurs sont en arithmétique 64 bits ;
- `ipfilter` : vérifie si une adresse IP correspond à une classe ou non.

Ces trois commandes (et leurs sous-commandes associées) concentrent l'essentiel de la complexité temporelle du rapport quotidien. Le fait de les recoder en C a permis un accroissement de performances d'un facteur 10, et un gain de place en mémoire de l'ordre d'un facteur 2.

Le dernier script, « gengraph », est lui aussi implémenté en Tcl. Sa rapidité fait qu'il n'y a pas eu besoin de chercher à l'optimiser. Il utilise « gnuplot » pour générer des courbes à la demande.

Sécurité

Comme expliqué dans l'introduction, le logiciel « acct-cisco » peut apporter une aide précieuse en matière de sécurité. Toutefois, il ne faut pas oublier la sécurité de l'outil lui-même : les utilitaires contenus dans « acct-cisco », du fait des connexions sur le routeur, nécessitent de mettre les mots de passe du routeur (mot de passe normal et mot de passe administrateur) en paramètre. Ceci a un impact non négligeable au niveau de la sécurité :

- mention des mots de passe dans la crontab de l'utilisateur ;
- mention des mots de passe sur la ligne de commande lorsque des utilitaires comme « getacct » sont lancés (et donc visibles avec « ps ») ;
- envoi en clair des mots de passe sur le réseau à intervalle régulier.

Pour ces raisons, il est donc conseillé de mettre en œuvre ce logiciel sur une station d'administration où ne peuvent se connecter que le ou les ingénieurs réseau, et de placer cette station le plus près possible du routeur, de manière à ce qu'une capture de paquets par un attaquant ne soit pas possible. Sous ces conditions, la sécurité de l'ensemble est acceptable.

Conclusion

Le logiciel « acct-cisco » en est aujourd'hui à sa deuxième version, dont l'annonce coïncide avec JRES'99. Il s'agit d'un logiciel facile d'installation, peu coûteux en matière de ressources, et qui génère un rapport quotidien fort instructif sur l'utilisation d'une liaison. Les traces qu'il permet de conserver se sont révélées plusieurs fois extrêmement utiles en cas d'incident de sécurité.

Une évolution envisageable serait d'utiliser une base de données de type RRD (base de données pour des données temps réel), et de pouvoir utiliser les outils venant avec cette base de données.

Enfin, signalons que « acct-cisco » est en production depuis 1994 à l'UVSQ, entre autres sites, et génère donc un rapport quotidien depuis maintenant 5 ans. Son utilisation s'est révélée précieuse, tant en terme d'évolution du réseau qu'en terme de sécurité.

Le logiciel est disponible sur ftp://ftp.uvsq.fr/pub/cisco/ .

Références

[MRTG] http:// www.mrtg.org

[IPTrafic] http://www.urec.fr/iptrafic

[Perl]ftp://ftp.lip6.fr/pub/CPAN

[Tcl] ftp://ftp.lip6.fr/pub/tcl/distrib
[gcc] ftp://ftp.lip6.fr/pub/gnu
[gnuplot] ftp://ftp.gnuplot.vt.edu/pub/gnuplot
[PrideTools] ftp://ftp.ripe.net/pride/tools
[RRD] http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool
[RFC1918] ftp://ftp.lip6.fr/pub/rfc/rfc/rfc1918.txt.gz