

Logiciels de surveillance de réseaux informatiques

François-Xavier ANDREU *

été 2000

*(francois_andreu@hotmail.com) stagiaire à l'Unité RÉseaux du CNRS (<http://www.urec.fr/>) sous la direction de Jean-Luc ARCHIMBAUD (<http://www.urec.fr/jla/>).

Table des matières

1 AVERTISSEMENT	6
2 Introduction	7
3 Les différentes méthodes pour surveiller un réseau	7
3.1 Les méthodes actives	7
3.2 Les méthodes passives	7
4 Liste des outils	8
4.1 Outils d'analyse de trames	8
4.1.1 TcpDump	8
4.1.2 NStreams	8
4.1.3 NNStat	9
4.1.4 Arpwatch	9
4.2 Outils d'analyse de trafic	9
4.2.1 MRTG	9
4.2.2 Cricket	10
4.2.3 Tcptrace	10
4.2.4 NTop	11
4.2.5 MTR	11
4.2.6 Bing	11
4.2.7 WhatsUp Gold	11
4.2.8 Scion	12
4.2.9 NetraMet	12
4.2.10 Tele Trafic Tapper	12
4.2.11 Scotty	12
4.2.12 NetMet	12
4.2.13 IPtrafic	13
4.2.14 WebSNMP	13
4.2.15 Acct-cisco	13
4.3 Outils de supervision	13
4.3.1 Big Brother	14
4.3.2 NMAP	14
4.3.3 Mon	14
4.3.4 Netsaint	14
5 Une sélection	15
6 MTR	15

7 Ntop	17
7.1 Introduction	17
7.2 Welcome to ntop!	19
7.3 Fonctionnement	27
7.4 Options	28
7.5 Conclusion	29
8 Cricket	29
8.1 Introduction	29
8.2 Configuration	29
8.3 Navigation web	32
8.4 Exemples graphiques	34
8.5 Cricket vs MRTG	35
9 Mon	36
10 Acct-cisco	39
11 Conclusion	42
12 Annexes	43
12.1 Détection d'un scan	43
12.1.1 avec cricket	43
12.1.2 avec ntop	43
12.2 Tkined (Scotty)	44
12.3 InterMapper	45
12.4 Quelques liens	46

Table des figures

1	<i>commande : mtr alta-vista.serveur-nationaux.fr (début juillet)</i>	16
2	<i>cmd : mtr www.urec.cnrs.fr(16 juillet)</i>	16
3	<i>mtr avec l'option report (-r -c)</i>	16
4	<i>informations sur un hôte</i>	19
5	<i>protocoles employés par l'hôte</i>	19
6	<i>informations sur un hôte, suite.</i>	20
7	<i>ntop -> Data Sent</i>	20
8	<i>ntop -> stats -> multicast</i>	21
9	<i>ntop -> stats -> traffic</i>	21
10	<i>ntop -> stats -> traffic</i>	22
11	<i>ntop -> stats -> traffic</i>	22
12	<i>ntop -> stats -> traffic</i>	23
13	<i>ntop -> stats -> traffic</i>	23
14	<i>ntop -> stats -> traffic</i>	23
15	<i>ntop -> stats -> hosts</i>	24
16	<i>ntop -> stats -> Throughput</i>	24
17	<i>ntop -> stats -> Throughput Statistics Matrix</i>	24
18	<i>ntop -> stats -> Domain</i>	24
19	<i>ntop -> stats -> Plugins</i>	25
20	<i>ntop -> stats -> R to L</i>	25
21	<i>ntop -> stats -> L to R</i>	25
22	<i>ntop -> stats -> Matrix</i>	26
23	<i>ntop -> IP Protocol -> Distribution</i>	26
24	<i>ntop -> IP Protocol -> Usage</i>	27
25	<i>ntop -> IP Protocol -> Session</i>	27
26	<i>page principale de cricket</i>	32
27	<i>choix des routeurs</i>	32
28	<i>observations possibles pour ce routeur</i>	33
29	<i>interfaces observées sur un routeur</i>	33
30	<i>résumé du trafic pour une interface</i>	33
31	<i>choix des graphiques</i>	33
32	<i>utilisation du cpu d'un routeur</i>	34
33	<i>interface de sortie sur un routeur pendant les dernières 24h</i>	35
34	<i>...et sur une semaine</i>	35
35	<i>mémoire du routeur atm faisant la jonction du campus avec renater</i>	36
36	<i>utilisation du processeur sur le même routeur</i>	36
37	<i>interface de mon</i>	39
38	<i>courbe du trafic sur 24h</i>	41
39	<i>la variable icmpDestUnreachs</i>	43
40	<i>services contactés sur kaki</i>	44
41	<i>services utilisés sur le réseau</i>	45
42	<i>fenêtres de tkined</i>	46

TABLE DES FIGURES

5

43 surveillance d'un réseau avec intermapper 46

1 AVERTISSEMENT

Le travail demandé à l'auteur de ce rapport, François Xavier Andreu, était de **recenser les principaux logiciels du domaine public permettant de surveiller un réseau informatique, de décrire leurs fonctionnalités, de les classer et ensuite d'en tester quelques uns.**

Il a parfaitement réalisé ce travail, c'est la raison pour laquelle nous publions son rapport qui peut intéresser les administrateurs informatiques et réseaux ; en particulier du monde de la recherche et de l'enseignement qui ont des parcs hétérogènes à gérer, peu de moyens financiers et peu de personnel.

C'était en fait pour nous l'objectif de ce stage, donner à ces administrateurs, un document qui fasse un état des lieux sur le sujet.

Il est à noter que ce travail a été effectué en 3 mois par un étudiant en informatique, options réseaux mais qui ne connaissait pas du tout l'administration réseau. Donc :

- Le recensement n'est pas exhaustif, ce n'était pas le but.
- Il reflète l'expérience de l'auteur et n'est pas exempt d'erreur.

Plus positivement, on peut aussi en conclure que :

- Au vue des logiciels décrits **il y a tout ce qu'il faut pour correctement surveiller un réseau avec les outils du domaine public.**
- François Xavier a réussi assez facilement à les installer à les utiliser sans expérience dans ce domaine, donc tout administrateur devrait pouvoir le faire sans difficulté.

Les logiciels sont divers et aucun ne fait exactement la même chose que l'autre. La difficulté pour un administrateur sera de savoir ce dont il a le plus besoin et de trouver le logiciel qui réponde à ses demandes.

Nous avons demandé à François Xavier de tester plus particulièrement 5 logiciels que nous n'avons pas choisi au hasard. Le premier critère était qu'ils semblaient correctement fonctionner et qu'ils étaient utilisés dans notre communauté. Le second et le plus important est que **chacun a une fonction principale particulière** :

- **MTR** permettra de **déetecter rapidement où se situe une anomalie sur une liaison** : coupure, engorgement, ...
- **NTOP** permettra de **connaître très précisément à quoi est utilisé le réseau** : quelle est la charge, quelles sont les stations les plus bavardes, qui dialogue avec qui, avec quels protocoles, dans quelles proportions, ...
- **Cricket** indiquera l'**état des équipements réseau** en particulier (routeurs, commutateurs, ...) : charge, trafic, ...
- **Mon** renseignera sur l'**état des services sur les stations** (messagerie, Web, FTP, ...).

- **Acct-cisco** fera une **comptabilité et indiquera la répartition du trafic sur un routeur CISCO**. Il détectera aussi quelques attaques de pirates.

Ce kit devrait répondre à la grande majorité des besoins.

Bonne lecture

JL Archimbaud Directeur technique de l'UREC

2 Introduction

Supervision, statistiques, sécurité, analyse de charges, état des services... Voici les termes auquels sont confrontés les administrateurs réseaux. Comme ces notions, les solutions (matérielles et/ou logicielles) que l'on peut trouver en surveillance de réseaux sont nombreuses mais pas toujours bien adaptées.

Il y a d'abord la solution professionnelle : les plates-formes d'administration telles que HP Openview, SunNet Manager... Mais celle-ci est chère et compliquée de part sa configuration et sa maintenance. L'alternative consiste à choisir un ou plusieurs logiciels (libres ou non) plus facile à configurer et souvent moins lourd en ressources informatiques et humaines. Malheureusement ces logiciels sont nombreux et en trouver un qui réponde à ses besoins n'est pas toujours évident.

Je vous propose donc un petit tour d'horizon (non exhaustif) de ces logiciels, puis une étude de certains d'entre eux.

3 Les différentes méthodes pour surveiller un réseau

Ces méthodes peuvent être regroupées selon les deux familles suivantes :

3.1 Les méthodes actives

Elles consistent à démarer un logiciel pour observer une caractéristique précise du réseau à un moment donné. Elles ne permettent pas une observation globale du réseau. Ping, Traceroute et les connexions sur les équipements (en Telnet par exemple) en font partie. Les deux premiers utilisent le protocole ICMP bien que celui-ci ne soit pas un véritable protocole d'administration. Quand à Telnet il permet un diagnostic sur place par l'observation des paramètres de configuration ou du résultat de commandes systèmes.

3.2 Les méthodes passives

Les logiciels utilisant ces méthodes tournent généralement sans s'arrêter. L'administrateur peut les administrer et accéder aux résultats soit par le web, soit par

une interface graphique ouverte en permanence. Ce sont des outils de surveillance continue.

Il s'agit de sondes (matérielles ou logicielles), de logiciel interrogeant des MIB (Management Information Base) par le protocole SNMP (Simple Network Management Protocol), ou d'agents placés sur les équipements.

4 Liste des outils

Les logiciels sont classés en trois catégories : les outils d'analyse de trames (principalement pour le debug), les outils de surveillance du trafic (statistiques, accounting, alarmes...) et enfin ceux chargés de la surveillance des services. Certains logiciels offrent parfois des fonctionnalités s'étendant sur les trois catégories. Je les ai alors placés selon l'information principale délivrée.

4.1 Outils d'analyse de trames

Ces outils observent les trames et stockent certaines informations (adresses source, destination, longueur, protocole, heure...) mais ne font pas de statistiques ou autres opérations. Ils laissent à l'administrateur l'analyse de ces informations. Ils sont utilisés pour visualiser les problèmes de sécurité, de bug...

4.1.1 TcpDump

Analyse de paquets Ethernet par une station. Possède une interface graphique qui simplifie le maniement : Tcpview (mais qui est moins souple, bien entendu). Sous NT et Unix, logiciel libre.

→ <http://www-nrg.ee.lbl.gov/>

Utilisé par :

- Guy Brand, Fac de Chimie, ULP, Strasbourg
 <guybrand@chimie.u-strasbg.fr>

4.1.2 NStreams

Ce logiciel analyse les sorties Tcpdump (soit directement, les deux logiciels s'exécutant en même temps, soit en lisant le fichier de sortie de Tcpdump) ou écoute directement le trafic réseau. Il analyse le trafic suivant les protocoles tcp, udp et icmp. Il peut être considéré comme un mini logiciel de détection d'intrusion (reconnaissance des flux entrants et sortants et gestion des flags tcp). Il a été réalisé pour une écoute du réseau avant la mise en place d'un firewall, pour une configuration correcte de ce dernier. Il ne se prête donc pas à une analyse à long terme, mais peut

être utile pour une petite étude.

Sous licence GPL, tourne sur Solaris, FreeBSD, Linux (et tout système compatible POSIX avec la libpcap).

→ <http://www.hsc.fr/ressources/outils/nstreams/>

Utilisateurs :

- *Jean Guillou, CRI UPMF Grenoble <Jean.Guillou@upmf-grenoble.fr>*
- *Hervé Schauer, H.S. Consultants <Herve.Schauer@hsc.fr>*
- *Michel Gaudet <Michel.Gaudet@ehess.fr>*
- *Guy Brand, Fac de Chimie, ULP, Strasbourg <guybrand@chimie.u-strasbg.fr>*
- *Françoise Gazelle, Observatoire de Besançon <fg@obs-besancon.fr>* sous linux debian

4.1.3 NNStat

Outil d'acquisition pour faire des statistiques (assez ancien maintenant). Ne fait pas d'analyse de données ni de mise en forme graphique. Sous Unix.

Souple, gratuit, puissant mais dur à configurer d'après certains utilisateurs.

→ ftp://gatekeeper.dec.com/pub/DEC/net/NNStat_3.3beta.tar.Z

4.1.4 Arpwatch

Il capture les adresses Ethernet ou IP des trames pour une analyse ultérieure de l'administrateur.

Tourne sous Linux avec la libpcap installée.

→ <http://www-nrg.ee.lbl.gov/>

Utilisé par

- *Jean-Marc Vinet, Institut de Recherche pour le Développement <Jean-Marc.Vinet@paris.ird.fr>*
- *Jose Marcio MARTINS DA CRUZ, ENSMP <martins@paris.ensmp.fr>*

4.2 Outils d'analyse de trafic

Ceux-ci sont capables de faire des statistiques (qui sont souvent accessibles avec une interface web). Ils peuvent servir pour l'accounting, l'observation de la bonne configuration des services... Ils génèrent parfois des alarmes.

4.2.1 MRTG

Multi Router Traffic Grapher par Toby Oetiker. Programme en Perl et C utilisant SNMP pour interroger les compteurs des routeurs. Visualisation graphique.

Fonctionne sous la plupart des plates-formes Unix et Windows NT, Licence GPL.
→ <http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html>

Utilisé par :

- Bruno Bzeznik¹, Academie de Grenoble <Bruno@ac-grenoble.fr>
- Jerome Le Tanou, Academie de Grenoble <Jerome.Le-Tanou@ac-grenoble.fr>
- Jean-Marc Vinet, Institut de Recherche pour le Developpement <Jean-Marc.Vinet@paris.ird.fr>
- Françoise Gazelle, Observatoire de Besançon <fg@obs-besancon.fr> sous Digital Unix
- Nicolas Viers, université de Limoges <viers@unilim.fr>

4.2.2 Cricket

Analyseur de trafic s'appuyant sur RRDTool (Round Robin Database, réimplémentation de la partie graphique et log de MRTG). Il est composé d'un collecteur et d'une application graphique.

Sous licence GPL, tourne sur Solaris, Linux, HP-UX, *BSD, et sans doute sur WinNT et Win2000 (écrit en Perl).

→ <http://cricket.sourceforge.net/>

Utilisateurs :

- Olivier Page <Olivier.Page@esm2.imt-mrs.fr>
- Eric Vielet, CRIHAN <Eric.Vielet@crihan.fr>
- Christophe Dupreuil, université de Picardie <Christophe.Dupreuil@u-picardie.fr>

4.2.3 Tcptrace

Analyseur des sorties Tcpdump, snoop, etherpeek ou netm. Il donne pour chaque connexion, le temps, le nombre de bytes et/ou segments reçus et/ou envoyés, les retransmissions, le RTT...

Il propose trois graphiques :

- Time Sequence Graph (segments envoyés et Ack en fct du temps)
- Throughput (trafic instantanné)
- Round Trip Time (des ack)

→ <http://jarok.cs.ohiou.edu/software/tcptrace/>

Indiqué par Matthieu Herrb, LAAS-CNRS <matthieu@laas.fr>

¹Vous pouvez consulter la page sur les logiciels libres utilisés dans l'académie de grenoble : http://www.ac-grenoble.fr/carmi-internet/doc/admin_sys_libre.html

4.2.4 NTop

Analyseur de trafic suivant le protocole (IP, IPX, DecNet, NetBios, OSI, DLC), et analyse pour IP suivant les protocoles de la couche supérieure.
Possède un visualisateur Web et texte.

Tourne sur Unix (Lic GPL) et Win32 (l'auteur ayant développé la libpcap pour Windows).

→ <http://www-serra.unipi.it/~ntop/ntop.html>

Utilisé par :

- *Bruno Bzeznik, Academie de Grenoble <Bruno@ac-grenoble.fr>*
- *Guy Brand, Fac de Chimie, ULP, Strasbourg <guybrand@chimie.u-strasbg.fr>*
- *Nicolas Viers, université de Limoges <viers@unilim.fr>*

4.2.5 MTR

Observe la qualité des liens et sort des statistiques d'accès par ordinateur cible.
Utilise Traceroute plus Ping. (Linux)

→ <http://www.bitwizard.nl/mtr/>

Indiqué par *Matthieu Herrb, LAAS-CNRS <matthieu@laas.fr>*

4.2.6 Bing

Bandwidth pING. Calcule la bande passante avec ping.

→ <http://web.cnam.fr/Network/bing.html>

Indiqué par *Matthieu Herrb, LAAS-CNRS <matthieu@laas.fr>*.

Utilisé par *Guy Brand, Fac de Chimie, ULP, Strasbourg <guybrand@chimie.u-strasbg.fr>*

4.2.7 WhatsUp Gold

de IPSWITCH. Versions commerciale et d'évaluation pour 30 jours. Utilisé pour surveiller des réseaux locaux à Meudon, Toulouse et Angers.

Basé sur SNMP, il trace la carte du réseau et peut lancer des alarmes. Observe sans doute aussi les services.

Fonctionne sous winNT, 95, 98, 00.

→ <http://www.ipswitch.com>

Utilisateurs :

- *Eric Renaudin, CNRS <renaudin@dsi.cnrs.fr>*

- *Emmanuel SCHREQUE, Académie de Versailles*
<Emmanuel.Schreque@ac-versailles.fr>

4.2.8 Scion

de NetSCARF. Développé pour SunOS, BSDi, WinNT.
 Analyseur de trafic basé sur SNMP, visualiseur web.
 → <http://www.merit.edu/~netscarf/>

4.2.9 NetraMet

Collecte les informations grâce à SNMP, mesure du trafic suivant l'adresse éthernet et/ou l'adresse réseau et/ou l'adresse de transport (il est constitué d'un collecteur et d'un visualiseur). Unix ou DOS.

→ <http://www.auckland.ac.nz/net/Accounting/ntm.Release.note.html>

4.2.10 Tele Trafic Tapper

Monitoring temps réel, à distance avec support du multicast. Accepte les sorties Tcpdump. Classement automatique suivant les protocoles et machines.
 Sous FreeBSD-2.2.X, BSD, Solaris 2.5.1 .
 → <http://www.cs1.sony.co.jp/person/kjc/software.html#ttt>

4.2.11 Scotty

Scotty est une distribution incluant deux composants. Le premier est Tnm Tcl Extension. Il permet un accès aux sources d'informations des réseaux par une invite Tcl. Le deuxième composant est Tkined : un éditeur de réseau s'appuyant sur Tnm. Il peut découvrir le réseau et permet entre autre l'interrogation de MIB.

→ <http://wwwhome.cs.utwente.nl/\%7Eschoenw/scotty/>

Indiqué par :

- *Olivier Page <Olivier.Page@esm2.imt-mrs.fr>*
- *Michel Gaudet, Ecole des Hautes Etudes en Sciences Sociales*
<Michel.Gaudet@ehess.fr>

4.2.12 NetMet

Network Metrologie. Nouveau, développé par le CIRIL. En test actuellement. Pour les réseaux nationaux et métropolitains (aussi pour les petits réseaux d'après l'auteur). Il s'appuie sur la technologie NetFlow des matériels Cisco.

Contact : *Alexandre Simon, C.I.R.I.L. Alexandre.Simon@ciril.fr*

4.2.13 IPtrafic

Analyse du trafic IP :

- débit de la liaison
- répartition du trafic par protocoles et services
- consommation des machines (trafic vers/depuis l'extérieur).
- profil des échanges entre un site local et d'autres réseaux.
- ...

Développé par l'UREC et le CRU (architecture client serveur). Tourne sur un PC/Linux ou SunOS4.

→ <http://www.urec.cnrs.fr/iptraffic/>

Utilisé par :

- *Marc Romero, Institut de Biologie Physico-Chimique, Fondation Edmond de Rothschild <Marc.Romero@ibpc.fr>*
- *Françoise Gazelle, Observatoire de Besançon <fg@obs-besancon.fr> sous linux debian*
- *Nicolas Viers, université de Limoges <viers@unilim.fr>*

4.2.14 WebSNMP

de Atos, version gratuite pour windows pouvant gérer 10 agents SNMP.

WebSNMP est un outil permettant d'administrer des équipements SNMP (stations de travail imprimantes, routeurs, logiciels) à travers le Web. Ce produit est un serveur intermédiaire, qui dialogue avec les équipements par le protocole d'administration standard SNMP.

→ <http://www.snmp-products.com/Manager/WebSNMPfr.html>

Indiqué par *Christian Julien, enac <christian.julien@enac.fr>*

4.2.15 Acct-cisco

Réservé pour les possesseurs de routeurs Cisco, il interroge la table d'accounting de ces derniers par telnet, puis édite un rapport chaque jour. Il délivre des informations sur le débit de l'interface, la table de comptabilité, les transactions suspectes, les machines non enregistrées dans le DNS, le top 50 des connexions, et donne une courbe de trafic. Il tourne sur les systèmes Unix. Il a été développé par Pierre David de l'UVSQ.

→ <ftp://ftp.uvsq.fr/pub/cisco/>

Présentation page 10.

4.3 Outils de supervision

Ou outils de surveillance des stations à distance. Ces outils permettent l'observation des connexions, du bon fonctionnement des services, la charge des cpu, et

autres paramètres. Mais certains des logiciels déjà cités peuvent rentrer dans cette catégorie.

4.3.1 Big Brother

Supervision système et réseau. Permet de visualiser l'état des connexions, des cpu et des services installés sur les stations. Il peut fonctionner avec MRTG. Code source pour Linux et Unix, client disponible pour WinNT, Novell Netware, MacOS.

→ <http://www.maclawran.ca/bb-dnld/>

Utilisé par :

- *Jean Charles Delépine, Université de Picardie <delepine@u-picardie.fr>*
- *Marc Romero, Institut de Biologie Physico-Chimique, Fondation Edmond de Rothschild <Marc.Romero@ibpc.fr>*
- *Jean-Marc Vinet, Institut de Recherche pour le Développement <Jean-Marc.Vinet@paris.ird.fr>*

4.3.2 NMAP

Nmap a été conçu pour explorer de grands réseaux afin de découvrir quels hôtes sont accessibles et quels services ils offrent. C'est un scanner de ports.
Linux software.

→ <http://www.insecure.org/nmap/>

Utilisé par *Guy Brand, Fac de Chimie, ULP, Strasbourg <guybrand@chimie.u-strasbg.fr>*.

4.3.3 Mon

Démon d'observation écrit en Perl 5. Il observe (services, espaces disques, etc sur des ensembles de stations) et lance des alertes. Il possède aussi une petite interface web (script cgi).

Licence GPL. Portage a priori facile (perl).

→ <http://www.kernel.org/software/mon/>

Présentation page 9.

Utilisateurs :

- *Stephane Bortzmeyer, institut Pasteur <bortzmeyer@pasteur.fr>*

4.3.4 Netsaint

Observe le réseau suivant les services (SMTP,POP3, HTTP, NNTP...) ainsi que les ressources des postes (espace disque, charge cpu...). Lance des alarmes lors de problèmes. Interface Web pour le status courant du réseau, l'historique des pro-

blèmes, fichier de log...

Sous Linux (a priori Unix car écrit en C), Licence GPL, interface Web sécurisée.
→ <http://www.netsaint.org/>

Utilisé par :

- *Guy Brand, Fac de Chimie, ULP, Strasbourg*
<guybrand@chimie.u-strasbg.fr>.

5 Une sélection

Nous avons décidé de regarder de plus près certains des logiciels précédents. Chacun de ces logiciels nous offre une fonctionnalité différente. Mtr pour l'étude des liens, Ntop pour l'analyse de trafic, Cricket pour avoir des statistiques de la charge du trafic, Mon pour la surveillance de services et Acct-cisco pour l'accounting. Ce choix est un peu arbitraire et ne signifie en aucun cas que les logiciels choisis sont les meilleurs.

Je vous présente donc dans les sections suivantes ces cinq logiciels de surveillance de réseau.

6 MTR

Fonctionne sous Linux.

→ <http://www.bitwizard.nl/mtr/>

Mtr est un (petit) programme qui montre l'état de la bande passante jusqu'à une adresse voulue. Fonctionnant suivant le principe de Traceroute et Ping, il enregistre d'abord la route empruntée, puis envoie le même nombre de paquets à chaque routeur traversé. Il détermine ainsi le pourcentage de paquets perdus à chaque niveau.

Il y a quatre indicateurs de la santé de la connexion :

- le pourcentage de paquets perdus
- le meilleur temps réalisé par un paquet en millisecondes
- le plus mauvais temps
- le temps moyen

L'exemple de la figure 1 permet de voir que des paquets sont perdus à plusieurs endroits. Mais il faut replacer cet exemple dans son contexte : comme on le voit sur le deuxième exemple (figure 2) il y a beaucoup moins de paquets perdus. Tout dépend du jour et de l'heure de l'étude.

On peut également changer la taille des paquets envoyés (option -p avec le nombre de bits désirés), observant ainsi le comportement du réseau suivant la quantité des données envoyées.

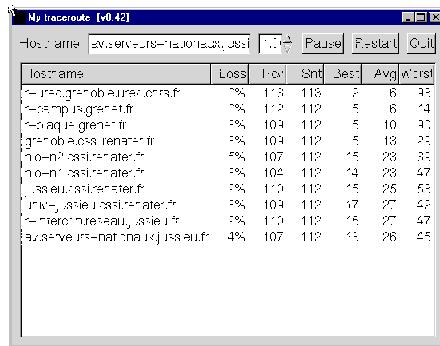


FIG. 1 – commande : mtr alta-vista.serveur-nationaux.fr (début juillet)

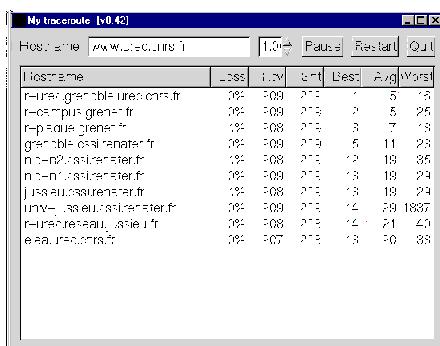


FIG. 2 – cmd : mtr www.urec.cnrs.fr(16 juillet)

L'écart entre les requêtes ICMP ECHO peut également être modifié.

Les options -r et -c permettent d'avoir un rapport de statistique sur la connexion choisie. Il fonctionne alors par cycles (d'une durée d'une seconde) envoyant le même nombre de ping. Bien sûr dans ce mode la charge rajoutée sur le réseau est conséquente (figure 3).

HOST	LOSS	RCV'D	SENT	BEST	AVG	WORST
r-urec.grenoble.urec.cnrs.fr	0%	30	30	1.95	2.37	6.29
r-campus.grenet.fr	0%	30	30	1.93	2.37	3.81
r-plaque.grenet.fr	0%	30	30	2.62	5.34	42.30
grenoble.cssi.renater.fr	0%	30	30	3.08	7.71	15.63
nio-i2.cssi.renater.fr	0%	30	30	11.61	16.23	23.64
nio-i3.cssi.renater.fr	0%	30	30	10.24	14.50	18.74
gix.cssi.renater.fr	0%	30	30	12.33	16.71	22.93
level3.gix-paris.ft.net	0%	30	30	11.62	17.33	23.57
loopback0.core1.Parisi.Level3.net	0%	30	30	12.20	16.86	25.35
loopback0.core1.London1.Level3.net	0%	30	30	27.49	31.25	40.49
loopback0.duaccess2.London1.Level3.net	0%	30	30	27.62	37.15	130.92
212.113.3.3	0%	30	30	28.70	55.84	334.12
212.113.10.122	0%	30	30	27.39	42.04	211.71
jumpfr.altavista.com	4%	29	30	26.98	35.33	45.72

FIG. 3 – mtr avec l'option report (-r -c)

Mtr est pratique, puisqu'en une seule commande il combine Traceroute et Ping.

Le résultat est clairement lisible et donne facilement l'état d'une connexion possible.

7 Ntop

→ <http://www-serra.unipi.it/~ntop/ntop.html>

7.1 Introduction

Ntop délivre une quantité impressionnante d'informations sur le trafic de votre réseau. Un bon emplacement consiste à le placer avant votre routeur de sortie sur internet. Vous pouvez ainsi observer pratiquement toutes les caractéristiques du trafic (entrant et sortant). Pour cela, une interface web est proposée (ntop peut se lancer également en mode ligne).

Ntop est développé par Luca Deri², administrateur réseau et chercheur à l'université de Pise (Italie). La version courante est la 1.3.1. Elle est normalement compilable sous toute plateforme Unix. Il existe cependant des paquets pour les OS suivant : Linux (Debian, RedHat, Slackware, SuSe), IRIX 6.2, Solaris 2.7 (i386 et SPARC), HP-UX 11.X, FreeBSD 3.X, AIX 4.1, et Windows 95/98/NT (Luca Deri a développé une libpcap pour Win32). Personnellement, je l'ai compilé sur un Linux RedHat sans problème.

Attention, Ntop peut poser des problèmes de sécurité lorsqu'il est lancé avec l'interface web. Il y a eu deux avis du CERT-Renater (<http://www.renater.fr>) concernant les distributions RedHat (<http://www.redhat.com>) et Debian (<http://www.debian.org/security/>).

²<deri@ntop.org>

Regardons les fonctionnalités en parcourant sa fenêtre de navigation :

About ntop	Une petite présentation de ntop, de son auteur et la “man page”.
Data Rcvd	Informations concernant les données entrantes sur les postes.
All Protocols	Celles du trafic sortant des postes.
IP	Des statistiques sur le multicast, les points vitaux du réseau, toutes les adresses capturées, un graphe de la bande passante, tous les noms de domaines répertoriés qui se baladent sur votre réseau, et l'accès à quelques extensions.
Throughput	
NetFlows	
Data Sent	
All Protocols	
IP	
Throughput	
Stats	
Multicast	
Traffic	
Hosts	
Throughput	
Domain	
Plugins	
IP Traffic	
R->L	Le trafic IP analysé suivant sa destination et sa source.
L->R	
L<->L	
Matrix	
Local Usage	
IP Protocols	Le trafic IP suivant les protocoles des couches supérieures.
Distribution	
Usage	
Sessions	
Routers	
Admin	Quelques fonctions d'administration.
Switch NIC	
Reset Stats	
Shutdown	
Users	
URLs	

7.2 Welcome to ntop !

À tout endroit dans les pages web, en cliquant sur un nom de machine, vous accéderez aux informations qui lui sont propres : son adresse IP, la dernière fois qu'un paquet en rapport avec lui a été vu, son domaine, sa Mac adresse, le vendeur, l'OS, le total des données échangées en bits, le trafic local et externe et le routeur par défaut (figure 4)...

IP Address	195.220.197.16	■ [unicast]
Last Seen	08/11/00 11:26:01	
Domain	grenoble.urec.cnrs.fr	
MAC Address	00:60:97:65:6A:D7	
Nw Board Vendor	3COM CORPORATION	
OS Name	[Windows NT4 / Win95 / Win98]	
NetBIos Name	PIN-NOIR [domain URECG] (Workstation)	
Host Location	Local (inside specified/local subnet)	
Total Data Sent	73.7 Kb/799 Pkts/0 Retran. Pkts [0%]	
Broadcast Pkts Sent	1 Pkts	
Data Sent Stats		
Total Data Rcvd	447.4 Kb/1,124 Pkts/0 Retran. Pkts [0%]	
Data Received Stats		
Used Subnet Routers	r-urec	

FIG. 4 – *informations sur un hôte*

puis les protocoles qu'il a utilisé (la figure 5 concerne un routeur)...

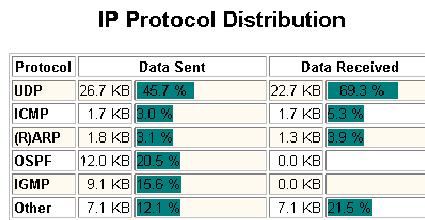


FIG. 5 – *protocoles employés par l'hôte*

et enfin trois tableaux : les dernières adresses contactées, les ports concernés et un historique des sessions IP (TCP et UDP) (figure 6).

Data Rcvd* et *Data Sent

Vous observerez ici le trafic reçu et envoyé par chaque machine (pas seulement celles de votre réseau). Il vous est présenté à chaque fois en trois tableaux.

Le premier tableau vous donne, pour chaque adresse transitant sur le réseau, les protocoles qu'elle utilise (figure 7). Le deuxième ne prend en compte que le trafic IP. Vous savez ainsi pour une machine, le service employé : HTTP, FTP, Telnet... Le

IP Protocol Distribution							
Protocol		Data Sent		Data Received			
TCP	75.6 KB	[REDACTED]	455.5 KB	[REDACTED]			
UDP	0.2 KB		0.0 KB				
(R)ARP	0.0 KB		0.0 KB				

Last Contacted Peers							
Receiver Name				Receiver Address			
kaki				195.220.197.1			
suroh.grenet.fr				193.54.189.10			
atlantide-2.grenet.fr				193.54.189.9			
<broadcast>				broadcast			

IP Service/Port Usage							
IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer		
http	80	10/36.1 Kb	suroh.grenet.fr				

IP Session History							
TCP Service	Role	# Sessions	Bytes Sent	Bytes Rcvd	Last Seen	First Seen	Peers
http	client	10	28.7 Kb	7.3 Kb	08/11/00 11:20:14	08/11/00 11:19:44	• suroh.grenet.fr

FIG. 6 – informations sur un hôte, suite.

volume du trafic est donnée en Kb et en pourcentage. Le dernier tableau montre pour chaque adresse le volume instantané du trafic, la moyenne et le maximum atteint (en bits et en paquets par seconde).

Host	Domain	Received ▾	TCP	UDP	ICMP	DLC	IPX	Decnet	(R)ARP	AppleTalk	OSPF	NetBios	IGMP	OSI	QNX	Other
Tree/OSI Route		4.8 MB 38.4 %	0	0	0	0	4.8 MB	0	0	0	0	0	0	0	0	0
enable.urec.cnrs.fr		3.1 MB 25.3 %	3.1 MB	0	0	0	0	0	0	0	0	0	0	0	0	0
cast.net		1.2 MB 9.4 %	0	0	0	0	0	0	0	0	1.2 MB	0	0	0	0	0

Host	Domain	Received ▾	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	SNMP	NFS	X11	SSH	Other IP	
pin-noir.grenoble.urec.cnrs.fr		3.1 MB 25.4 %	0	0	0	0	0	0	0	0.4 Kb	0	0	3.1 MB	
ospf-all.mcast.net		1.2 MB 9.4 %	0	0	0	0	0	0	0	0	0	0	1.2 MB	
atlantide-2		368.4 Kb 2.9 %	242	0	0	6.4 Kb	0	0	0	841	0	0	360.3 Kb	
multicaster.mcast.net		361.7 Mb 2.4 %	n	n	n	n	n	n	n	n	n	n	n	

Host ▾	Domain	Actual Thpt	Avg Thpt	Peak Thpt	Actual Pkt Thpt	Avg Pkt Thpt	Peak Pkt Thpt
all-systems.mcast.net		0.0 bps	0.0 bps	128.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
archiane		0.0 bps	0.0 bps	631.5 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.1 Pkts/sec
atlantide		0.0 bps	0.0 bps	230.4 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.1 Pkts/sec
atlantide-2		177.5 bps	0.0 bps	19.9 Kbps	0.0 Pkts/sec	0.0 Pkts/sec	3.0 Pkts/sec
Bridne Sn. Tree/OSI Route IMACI		744.7 mbps	187.3 mbps	2.0 Khps	0.2 Pkts/sec	0.0 Pkts/sec	0.5 Pkts/sec

FIG. 7 – ntop -> Data Sent

Stats

Sur ces pages sont regroupées les caractéristiques globales du trafic.

– Le trafic multicast :

Chaque machine qui envoie ou reçoit du trafic multicast est répertoriée dans

un tableau avec la quantité (en bits et paquets) de données correspondantes (figure 8).

Host	Domain	Pkts Sent	Data Sent	Pkts Rcvd	Data Rcvd
195.90.65.146		484	168.7 Kb	0	0
208.19.204.97		4	1.2 Kb	0	0
aigina.beinet.be	IT	926	860.1 Kb	0	0
all-routers.mcast.net	US	0	0	62	3.6 Kb
all-systems.mcast.net	US	0	0	30	1.8 Kb
bar02i.urz.uni-hamburg.de	DE	10	3.2 Kb	0	0
cheyenne.cs.fiu.edu	US	895	356.6 Kb	0	0
chouette.inria.fr	IT	8	3.8 Kb	0	0

FIG. 8 – *ntop -> stats -> multicast*

- Le trafic :

C'est ici que l'on trouve certains des signes vitaux du réseau : charge totale, broadcast, multicast. Il manque les collisions et les erreurs. Mais il s'agit quand même d'un véritable diagnostic de l'état du trafic :

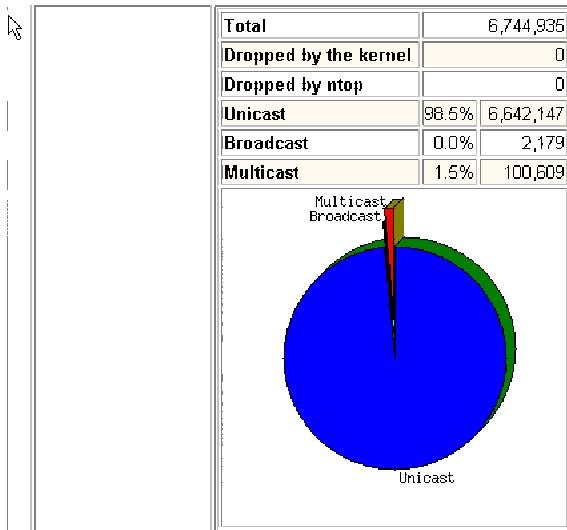
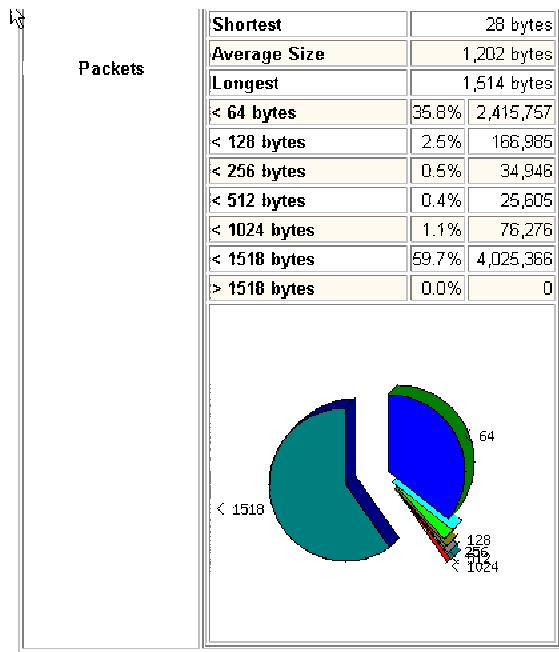
- quelques informations sur l'interface d'écoute, le nom de domaine, le temps écoulé depuis le démarrage de ntop (figure 9).

Global Traffic Statistics

Nw Interface Type	Ethernet [eth0]
Local Domain Name	grenoble.urec.cnrs.fr
Sampling Since	Tue Aug 1 14:27:54 2000 [23:03:01]

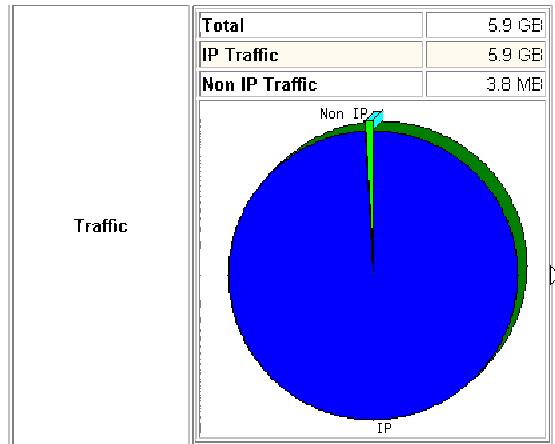
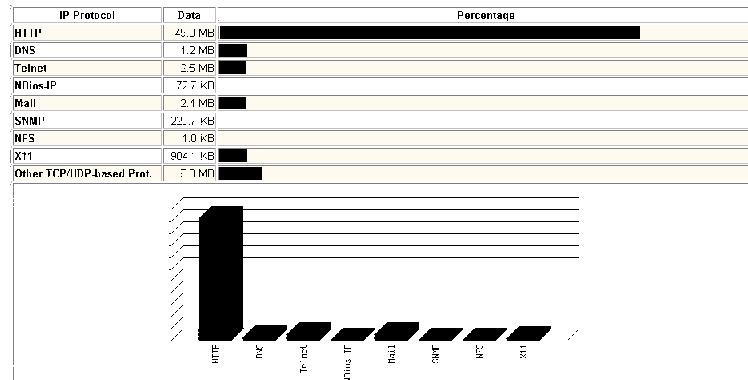
FIG. 9 – *ntop -> stats -> traffic*

- les informations sur le nombre de paquets capturés, le taux de multicast, de broadcast, avec un camembert. En un clin d'œil, vous savez si votre réseau se porte bien (figure 10).
- la taille des paquets circulant sur le réseau peut être aussi un bon critère pour la sécurité, un pourcentage élevé de petits paquets peut signifier que votre réseau est victime d'un scan (figure 11).
- vient ensuite le trafic en bits, et la comparaison entre le trafic IP et non IP (figure 12).
- le flux en bits et par paquets. Il est donné à l'instant même, sur une période d'une minute, sur les cinq dernières minutes et vous avez également le maximum (figure 13).
- deux tableaux-histogrammes avec sur l'un, les informations des protocoles du niveau réseau, et sur l'autre des protocoles encapsulés par IP (figure 14).

FIG. 10 – *ntop -> stats -> traffic*FIG. 11 – *ntop -> stats -> traffic*

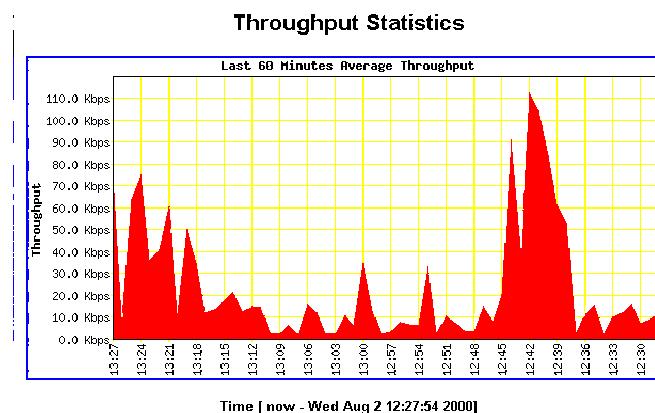
Vous savez ainsi le type et le pourcentage des données transitant sur le réseau.

- Hosts : un tableau de tous les hôtes “circulant sur le réseau”, avec leur adresse IP, le domaine, leur MAC adresse, un deuxième nom quand il est trouvé (numéro Apple ou nom microsoft), et une barre représentant la bande passante (figure 15).

FIG. 12 – *ntop -> stats -> traffic*FIG. 13 – *ntop -> stats -> traffic*FIG. 14 – *ntop -> stats -> traffic*

- Throughput : trois graphiques représentant le trafic sur l'interface (lors de la dernière heure, la journée et le mois. Ces graphiques ne sont pas très précis, et sont éphémères (figure 16). Mais vous pouvez cliquer dessus et atteindre une nouvelle page. Celle-ci classe pour chaque minute (de la dernière heure) les trois machines qui ont reçu ou envoyé le plus de trafic (figure 17).
- Domain : un tableau donnant les noms de domain rencontrés sur le réseau et la quantité de données pour chacun suivant les protocoles TCP, UDP, ICMP, IGMP et OSPF (figure 18).

Host	Domain	IP Address	MAC Address	Other Name(s)	Sent Bandwidth
atlantide-2		192.168.100.9	00:0C:97:4B:76:2B		
r-cicg		192.168.100.264	00:0C:97:4B:44:1C		
pin-noir.grenoble.urec.cnrs.fr		192.168.100.16			
titan		192.168.100.16	00:0C:97:4A:1C:2C	TITAN [WORKGROUP]	
suroh		192.168.100.102	00:0C:97:4B:23:04	SUROH [WORKGROUP]	
horus		192.168.100.1	00:0C:97:4B:09:4B	HORUS [WORKGROUP]	
io		192.168.100.8	00:0C:97:4B:74:07	IO [WORKGROUP]	
Cisco CDPD/VTP [MAC]		00:0C:97:4C:0C:0C		Cisco	

FIG. 15 – *ntop -> stats -> hosts*FIG. 16 – *ntop -> stats -> Throughput*

Sampling Period	Average Thpt	Top Hosts Sent Thpt			Top Hosts Rcvd Thpt		
		Host	Thpt	Host	Thpt	Host	Thpt
13:12 - 13:11	82.7 Kbps	r-urec			10.2 Kbps	rosier	10.0 Kbps
		kaki			8.1 Kbps	kaki	8.0 Kbps
		rosier			3.4 Kbps	sap.mcast.net	5.4 Kbps
13:11 - 13:10	80.2 Kbps	kaki			13.7 Kbps	rosier	9.0 Kbps
		r-urec			10.3 Kbps	kaki	8.7 Kbps
		av.serveurs.nationaux.jussieu.fr			3.7 Kbps	www.ip3000.com	3.8 Kbps
		kaki			25.5 Kbps	pin-noir	16.1 Kbps

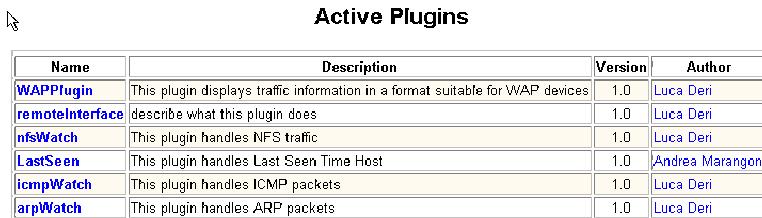
FIG. 17 – *ntop -> stats -> Throughput Statistics Matrix*

Internet Domain Stats													
Name ▾	Domain	Sent	Rcvd	TCP Sent	TCP Rcvd	UDP Sent	UDP Rcvd	ICMP Sent	ICMP Rcvd	OSPF Sent	OSPF Rcvd	IGMP Sent	IGMP Rcvd
atl.army.mil		562	1.2%	3	0.2%	0	0	563	0	0	0	0	-
risen.com		71	1.1%	7	0.7%	0	0	71	0	7	0	0	-
clara.net		87	1.3%	87	0.3%	0	0	87	27	0	0	0	-
ens-lyon.fr		11	0.1%	13	0.4%	0	0	11	12	J	U	U	-
lunet.li		1.7 K	0.1%	3	0.2%	0	0	1.7 K	0	C	0	0	-
grenoble.urec.cnrs.fr		33.2 K	91.2%	29.9	5.8%	25.6 K	29.5	355	259	72	70	156	0
insectnet		-	-	7	0.7%	7	7	7	7	0	0	0	-
univ.tln.fr		0	0.1%	71	0.2%	0	74	0	0	C	0	0	-
urec.cnrs.fr		6	0.1%	63	0.2%	50	60	J	U	U	U	U	-

FIG. 18 – *ntop -> stats -> Domain*

- quelques plugins tel que Wapplugin, remoteInterface, nfsWatch, LastSeen, icmpWatch, arpWatch. Attention, certains d'entre eux plantent souvent ntop.

Et pour les avoir, il faut lancer ntop depuis le répertoire d'installation (figure 19).



Name	Description	Version	Author
WAPPlugin	This plugin displays traffic information in a format suitable for WAP devices	1.0	Luca Deri
remoteInterface	describe what this plugin does	1.0	Luca Deri
nfsWatch	This plugin handles NFS traffic	1.0	Luca Deri
LastSeen	This plugin handles Last Seen Time Host	1.0	Andrea Marangoni
icmpWatch	This plugin handles ICMP packets	1.0	Luca Deri
arpWatch	This plugin handles ARP packets	1.0	Luca Deri

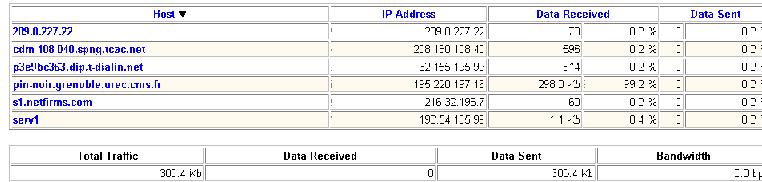
FIG. 19 – *ntop -> stats -> Plugins*

IP Traffic

Cette section et la suivante décortiquent le trafic sur IP. Celle-ci donne des informations sur le trafic venant de l'extérieur, sortant du réseau et le trafic local.

- R->L : Remote to Local.

Cette page présente les machines ayant communiqué avec votre réseau. Vous saurez l'adresse IP et la quantité de bits échangés pour chacune, ainsi que le trafic global (figure 20).



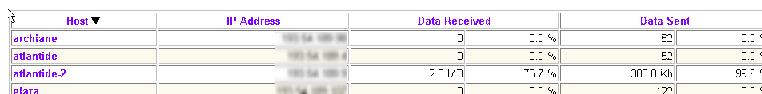
Host ▾	IP Address	Data Received	Data Sent
192.0.227.22	192.0.227.22	71	0.7%
cdm100.010.spmq.tcac.net	22.8.150.184	586	0.2%
pselletch3.dip.t-dialin.net	22.155.1.6.9	74	0.1%
pin.muis.yenublu.uvccam.us	125.220.17.12	280.0	29.2%
s1.lindfirms.com	216.32.193.7	62	0.2%
serd1	192.24.15.95	113	0.4%

Total Traffic	Data Received	Data Sent	Bandwidth
300.4 Kb	0	300.4 Kb	2.0 Mbps

FIG. 20 – *ntop -> stats -> R to L*

- L->R : Local to Remote.

Les mêmes informations vues de l'intérieur du réseau (figure 21).



Host ▾	IP Address	Data Received	Data Sent
archiane	192.168.100.10	0	0.0%
atlantide	192.168.100.4	0	0.0%
atlantide-2	192.168.100.9	71.17	71.17%
elara	192.168.100.12	71	0.0%

FIG. 21 – *ntop -> stats -> L to R*

- L<->L : Local to Local.

Le trafic interne global de votre réseau et suivant chaque poste. Le tableau est du même type qu'à la figure 20.

- Matrix : c'est une matrice 2D où sont présents tous vos postes. On peut observer ici le trafic entre chaque ordinateur (figure 22). Sur celle-ci, on voit nettement que kaki est un serveur : toutes les machines communiquent avec lui.

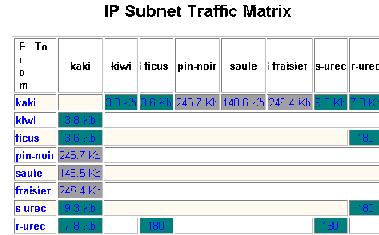


FIG. 22 – ntop -> stats -> Matrix

IP Protocols

Sur les pages web suivantes, les informations présentées concerne le trafic IP suivant les protocoles de la couche application.

- Distribution :

Cette page regroupe la classification des protocoles par histogramme. Cette information est donnée pour les flux entrant, sortant, et local (figure 23). Un camembert est aussi présent, indiquant d'un coup d'œil la part du trafic venant de l'extérieur par rapport au trafic local.

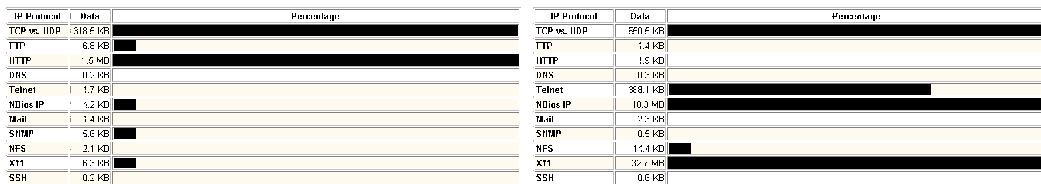


FIG. 23 – ntop -> IP Protocol -> Distribution

- Usage :

Un tableau où l'on trouve les ports (donc les protocoles) qui sont ou ont été utilisés avec les machines concernées (clients et serveurs, figure 24).

- Session :

Ce tableau répertorie toutes les sessions TCP actives. Vous avez le nom du client et du serveur, ainsi que les numéros de ports concernés de chaque côté, la quantité de données qui transite pendant la connexion, ainsi que la durée de celle-ci (figure 25).

IP Protocol Subnet Usage

Service	Clients	Servers
telnet	• faser	• xek
domain	• f-mlur • Telnet • http • faser • kml • kml	• xek
http	• f-mlur • f-mlc • sade • faser	• xek
119	• f-mlc	
123	• f-mls • kml • r-mlc • r-mls	• f-mls • xek • xek • xek
mathias.ns	• sade • faser • kml • kml	• f-mls • xek • xek • xek
141	• f-mls	• xek
snmp	• kml	• p-mlc • r-mlc
169	• faser	• xek
513	• kml	
514	• f-ml • kml	• kml • xek
598	• kml	• telnet
720	• kml	
1022	• f-ml	• xek
1023	• f-ml	• xek

FIG. 24 – ntop -> IP Protocol -> Usage

Client	Server	Data Sent	Data Rcvd	Active Since	Last Seen	Duration
titan:netbios-ssn	archiane:1651	93	0	08/10/00 12:35:50	08/10/00 12:35:50	39:35
titan:netbios-ssn	archiane:1653	93	0	08/10/00 12:47:51	08/10/00 12:47:51	27:34
titan:netbios-ssn	archiane:1654	93	0	08/10/00 12:59:52	08/10/00 12:59:52	15:33
titan:netbios-ssn	archiane:1657	120	0	08/10/00 13:11:39	08/10/00 13:11:39	3:46
pin-noir.grenoble.urec.cnrs.fr:2686	atlantide-2:3000	579	116	08/10/00 13:15:26	08/10/00 13:15:26	0 sec
surjh:7100	telesto:4236	8.6 Kb	0	08/09/00 14:21:58	08/10/00 13:11:53	22:53:27
surjh:7100	sade2:1117	8.8 Kb	0	08/09/00 13:31:58	08/10/00 13:11:53	23:43:27

FIG. 25 – ntop -> IP Protocol -> Session

– Routers :

Un petit tableau récapitulant quelles sont les postes internes qui communiquent avec le(s) routeur(s).

Admin

Dans cette section se trouve les commandes d'administration de ntop accessibles par le web. La page *Switch NIC* vous permet de changer l'interface d'écoute. *Reset Stats* permet de remettre à zéro toutes les statistiques. Vous pouvez également arrêter Ntop à partir du web, ajouter des utilisateurs, ainsi que des urls.

7.3 Fonctionnement

Ntop fonctionne dans un terminal ou bien en tant que démon (mode nécessaire pour l'interface web). Il est constitué de huit ou neuf processus (suivant les options) dont au moins un est constamment présent dans les processus actifs. Chacun prend la même quantité de mémoire, mais attention, ce chiffre augmente avec la quantité de trafic observé. Il est de 5% au lancement, et au bout d'un certain temps (dépendant

de l'ampleur du trafic), il dépasse les 20%. Et certaines fois deux ou trois processus tournent pendant quelques instants en même temps. Vous devez donc penser soit à le réinitialiser assez souvent, soit à lui dédier une machine.

Commande top :

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	LIB	%CPU	%MEM	TIME	COMMAND
18391	root	12	0	29516	28M	1156	R	0	5.5	23.0	35:36	ntop
11224	andreu	5	0	1080	1080	836	R	0	1.5	0.8	0:01	top
18396	root	1	0	29516	28M	1156	S	0	0.9	23.0	5:00	ntop
8257	root	1	0	1260	1260	836	S	0	0.1	0.9	0:47	save
11208	andreu	0	0	1920	1920	1472	S	0	0.1	1.5	0:00	xterm
...												

7.4 Options

Ntop peut lire les fichiers de sortie de tcpdump (la commande est *tcpdump -w file*). Vous avez donc l'interface web de ntop avec les informations délivrées par tcpdump. C'est utile si vous ne laisser pas tourner ntop, mais que vous avez capturé des paquets pour les analyser. L'interface de ntop est plus conviviale qu'un fichier de tcpdump.

Comme tcpdump, vous pouvez observer un trafic particulier à l'aide de filtres au lancement : *ntop src host pin-noir.urec.cnrs.fr or dst host pin-noir.urec.cnrs.fr*. Ce filtre permet de ne suivre que le trafic reçu ou envoyé par pin-noir.

Ntop permet également de surveiller la sécurité de votre réseau. Pour cela, il utilise un fichier de règles. Celles-ci sont de la forme *protocol nom_de_la_règle destination source définition action*.

Voici quelques exemples :

```
icmp route-advertisement ICMP_ROUTERADVERT !gateway/any action alarm
udp new-port-open any/any any/!usedport action mark
tcp tcp-short-fragment any/any any/any type fragment pktsize < 256 action alarm
tcp root-ftp any/ftp any/any contains "230 User root logged in" action alarm
tcp session-reset any/!any any/!any flags R pktcount > 30 unit 20 action alarm rearm 10
```

NetFlows List :

Ntop délivre souvent des informations globales sur le trafic. C'est à vous d'aller chercher dans les pages des machines les informations concernant un trafic particulier. Pour y remédier, vous pouvez lors du lancement définir les flux qui vous intéressent (option -F <liste de flux>). Par exemple :

ntop host X and (Y or Z) pour observer le trafic entre un poste X et deux hôtes possibles.

ntop 'icmp[0]!<8 and icmp[0]!>0' sélectionne tous les paquets icmp ne concernant pas un ping.

Il y a un vocabulaire assez consistant permettant facilement de visualiser un trafic spécifique (au niveau de la couche de transport et réseau).

7.5 Conclusion

Ntop est un logiciel complet et stable. Il lui manque peut-être deux fonctionnalités pour être un analyseur professionnel : une sauvegarde des données sur le long terme et la visualisation directe des trames.

On a parfois l'impression en parcourant les pages que l'information est redondante. Mais ce n'est qu'une impression. Tout tableau ou graphe n'est pas là par hasard. Ils sont tous utiles. En fait, tout dépend de l'information que l'on recherche.

8 Cricket

8.1 Introduction

Cricket est un logiciel de type MRTG. Il crée des graphiques d'après l'interrogation de variables SNMP. Ces graphiques sont accessibles par un navigateur web à l'url où vous avez mis le script cgi. Vous pouvez observer le trafic en tout point de votre réseau où une MIB et un agent SNMP sont installés : routeurs, switches...

Cricket est écrit en perl et se trouve sur le site suivant :

<http://cricket.sourceforge.net/>

Il y a aussi des programmes très utiles ainsi que le pack Solaris7 (avec tous les modules perl requis) sur le site :

http://www.gnac.com/techinfo/cricket_contrib/index.html

8.2 Configuration

Je conseille d'installer Cricket par défaut, c'est à dire sous le compte utilisateur cricket. Sinon il y a beaucoup de chemin à changer dans le code. La suite est simple. Voici l'arborescence des fichiers de configuration :

```
cricket-config/
cricket-config/Defaults
cricket-config/router-interfaces
cricket-config/router-interfaces/r-campus
```

```

cricket-config/router-interfaces/r-campus/Defaults
cricket-config/router-interfaces/r-campus/interfaces
cricket-config/router-interfaces/r-plaque
cricket-config/router-interfaces/r-plaque/Defaults
cricket-config/router-interfaces/r-plaque/interface
cricket-config/routers
cricket-config/routers/Defaults
cricket-config/routers/Targets
cricket-config/switches
cricket-config/switches/interface
cricket-config/switches/interface/Defaults
cricket-config/switches/interface/interfaces
cricket-config/config.db

```

Cette arborescence n'est pas importante. Vous pouvez modifier les noms des répertoires comme vous le voulez. La seule implication est la navigation au niveau du web. Par contre pour chaque type matériel interrogé vous devez avoir un fichier Defaults et un fichier Targets ou interfaces.

J'ai installé cricket sur le réseau de l'UREC où il y a un routeur, et au CICG (Centre Interuniversitaire de Calcul de Grenoble) où j'observe le trafic sur deux routeurs (r-campus et r-plaque). L'arborescence dans les deux cas est la suivante (pour les interfaces des routeurs) :

Pour l'UREC :

```

cricket-config/router-interfaces/Defaults
cricket-config/router-interfaces/interfaces

```

et le CICG :

```

cricket-config/router-interfaces/r-campus
cricket-config/router-interfaces/r-campus/Defaults
cricket-config/router-interfaces/r-campus/interfaces
cricket-config/router-interfaces/r-plaque
cricket-config/router-interfaces/r-plaque/Defaults
cricket-config/router-interfaces/r-plaque/interfaces

```

Le fichier Defaults n'est pas à modifier.

Le fichier interfaces peut être créé à la main, ou à l'aide d'un petit script qui se trouve dans le répertoire : cricket/util/listInterfaces. Celui-ci trouve sans problème toutes les interfaces de votre routeur. Même si celui-ci est un atm (il découvre aussi les sous interfaces, et le travail de configuration, dans ce cas là, consiste plutôt à retirer des lignes correspondantes à des interfaces que l'on ne souhaite pas particulièrement observées).

Voici un exemple :

```
target --default--
    router = r-urec

target Ethernet0
    interface-name = Ethernet0
    short-desc = "lien ethernet 0"

target Ethernet1
    interface-name = Ethernet1
    short-desc = "lien ether 1"
```

Pour un commutateur, c'est aussi simple. Le script à utilisé est listSwitchInterfaces. Le fichier ainsi créé est le suivant :

```
target --default--
    switch = s-urec

target noyer
    interface-name = Fa0/3
    short-desc = "FastEthernet0/3 100MB"
    order = 21

target rosier
    interface-name = Fa0/4
    short-desc = "FastEthernet0/4 N/A"
    order = 20

...
```

À chaque manipulation d'un fichier de configuration, il faut "recompiler" toute l'arborescence (./compile, puis ./collector pour vérifier le bon fonctionnement). Cricket interroge à intervalle régulier le matériel par un cron (l'intervalle est donc fixé à votre convenance). Le programme lancé s'appelle collect-subtrees. Ce dernier va d'abord lire le fichier subtrees-set qui contient les répertoires qui doivent être pris en compte :

```
set normal:
    /routers
    /router-interfaces
    /switches
```

Donc ne pas oublier de le modifier.

Cricket possède un répertoire log où les réponses snmp sont sauvegardés (les vingt dernières executions du cron). De plus il vous envoie un mail si quelque chose s'est mal passé.

Name	Description
<u>router-interfaces</u>	
<u>routers</u>	
<u>switches</u>	

FIG. 26 – *page principale de cricket*

Cricket peut donc tracer des graphiques à partir de n'importe quelle variable snmp intéressante. La seule difficulté est de trouver la variable. Pour cela la commande snmpwalk est nécessaire ou tkined (page 12.2). J'ai pu observer le trafic au niveau de commutateurs, routeurs, ainsi que l'utilisation des cpu et de la mémoire sur les routeurs (et la température suivant l'existance de cette fonctionnalité sur le routeurs).

8.3 Navigation web

L'interface web de cricket se manipule comme un explorateur de fichier. Sur la page principale, vous choisissez entre les interfaces des routeurs, les routeurs et les commutateurs (figure 26).

En cliquant sur routeurs nous avons le choix entre les routeurs observés (figure 27).

Name	Description
<u>r-campus</u>	
<u>r-plaque</u>	

FIG. 27 – *choix des routeurs*

Puis au niveau du routeur les graphes de l'utilisation du cpu, de la mémoire et de la température sont accessibles (figure 28).

Pour les interfaces d'un routeur ou d'un commutateur la présentation reste la même (figure 29).

Lorsque la MIB le permet, nous pouvons observer le trafic en octets, par paquets et les erreurs survenues sur le lien (figure 29). Les pages terminant cette arborescence proposent le trafic des dernières 24 heures, de la semaine et un résumé en chiffre (figure 30). Les autres graphiques sont facilement accessibles. Vous avez le choix

Name	Description
r-campus.grenet.fr [cpu] [temperature] [memory]	Router Campus
r-plaque.grenet.fr [cpu] [temperature] [memory]	Router plaque

FIG. 28 – observations possibles pour ce routeur

Name	Description
atm1_0.0-aa15_layer [Octets]	
atm1_0.100-aa15_layer [Octets]	: configuration des PVC vers SMHD
fastethernet2_0 [Octets] [UcastPackets] [Errors]	: vers 5000-com vlan02 p1/1

FIG. 29 – interfaces observées sur un routeur

entre la journée seule, la semaine, les deux ensembles (court terme, choix par défaut), le long terme (6 dernières semaines et l'année) ou tous les graphes sur la même page (figure 31).

Summary	
Values at last update:	
Average bits in (for the day):	Average bits out (for the day):
Cur: 98.66 bits/sec	Cur: 104.90 bits/sec
Avg: 98.74 bits/sec	Avg: 104.87 bits/sec
Max: 100.34 bits/sec	Max: 106.87 bits/sec
Last updated at Tue Aug 8 10:55:02 2000	

FIG. 30 – résumé du trafic pour une interface

[Hourly](#)
[Daily](#)
[Short-Term](#)
[Long-Term](#)
[All](#)

FIG. 31 – choix des graphiques

8.4 Exemples graphiques

Sur tous les graphiques, lorsqu'il s'agit de trafic, le bleu correspond au trafic sortant sur l'interface, et le vert au trafic entrant.

Le premier exemple est l'observation de l'utilisation du cpu du routeur de l'UREC (figure 32). Le graphe (sur les dernières 24 heures) montre deux augmentations de l'utilisation. La première qui dure presque toute la nuit, est due à une sauvegarde complète d'un serveur sur un autre lieu. La deuxième correspond aussi à une sauvegarde mais qui ne prend en compte que les changements depuis la précédente.

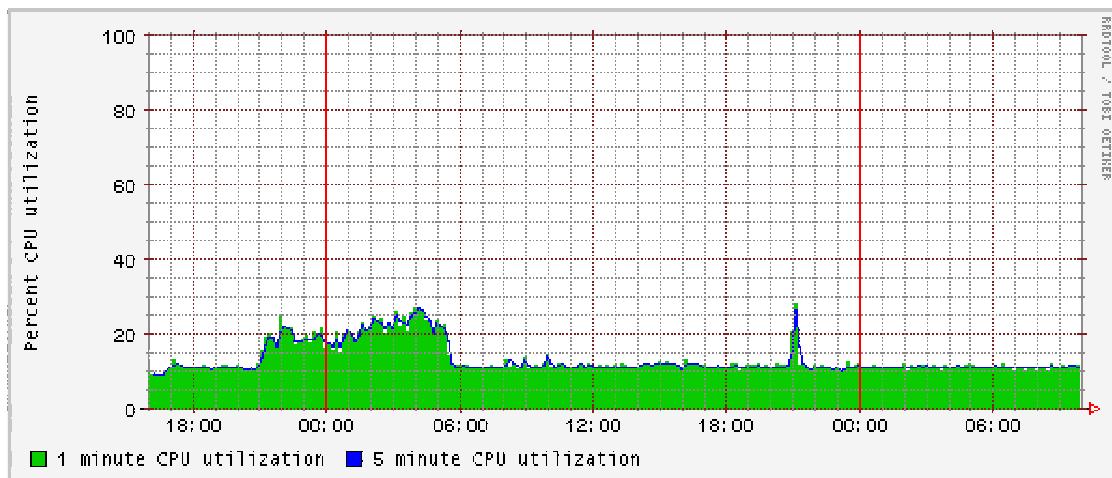


FIG. 32 – utilisation du cpu d'un routeur

Si on regarde à la même date le trafic sur l'interface de sortie du routeur, on obtient la figure 33. On observe bien un trafic conséquent sur les même période.

Le graphe suivant (figure 34) est l'observation sur une semaine du trafic sur l'interface du réseau de l'UREC avec le reste du monde. Les sauvegardes sont bien visibles chaque soir (pics bleus). Le dernier pic bleu est à 2,8Mb sur la figure 33, alors qu'il est à 1,3Mb sur le graphe de la semaine. Cela s'explique par le changement de l'échelle de temps, c'est logique mais il ne faut pas l'oublier.

Je vous présente maintenant quelques graphiques permettant de mettre à jour des anomalies sur le réseau. Bien sûr, l'analyse reste à chaque fois à faire par l'administrateur, mais les données présentées la facilitent.

La mémoire du routeur (au CICG) raccordant les réseaux du campus universitaire avec le réseau régional est donnée par la figure 35. On observe une augmentation de la mémoire utilisée, ceci jusqu'à la réinitialisation du routeur. Nous retrouvons après une utilisation normale de la mémoire. Celle-ci est constante.

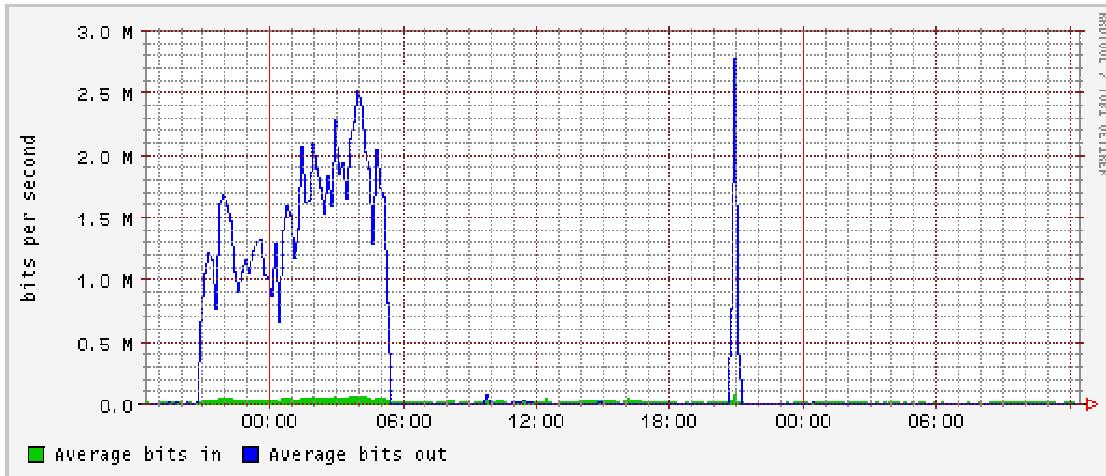


FIG. 33 – interface de sortie sur un routeur pendant les dernières 24h...

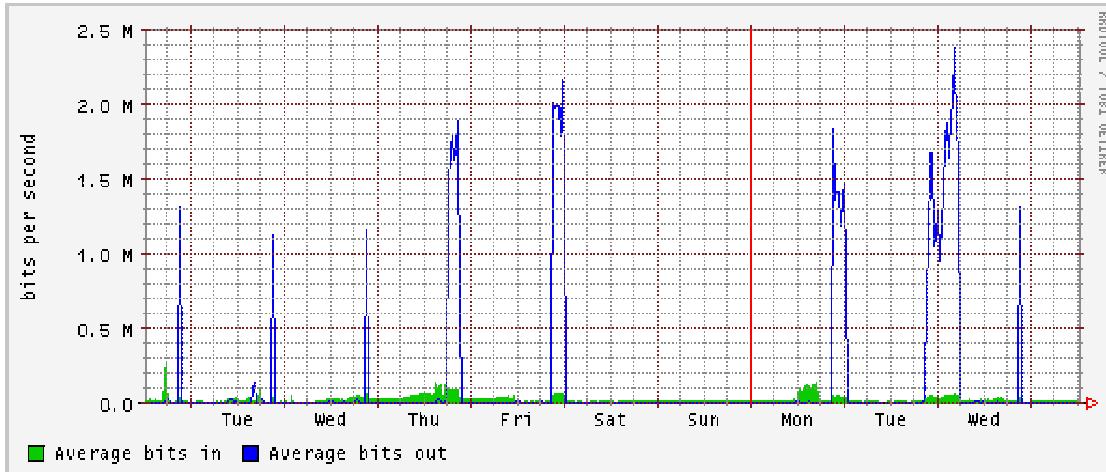


FIG. 34 – ...et sur une semaine

Ce problème n'est, par contre, pas visible sur l'utilisation du cpu (figure 36). La cause n'est pas donnée par cricket, mais nous avons là un bon indicateur.

8.5 Cricket vs MRTG

Si vous avez déjà MRTG, ce n'est peut-être pas nécessaire que vous changiez de logiciel, sauf si vous trouvez que les graphiques sont plus lisibles. Les fonctionnalités sont les mêmes.

Cricket est plus récent et utilise la réimplémentation de la partie base de données et le suivi est déjà conséquent. Donc, si vous n'avez rien pour observer votre réseau

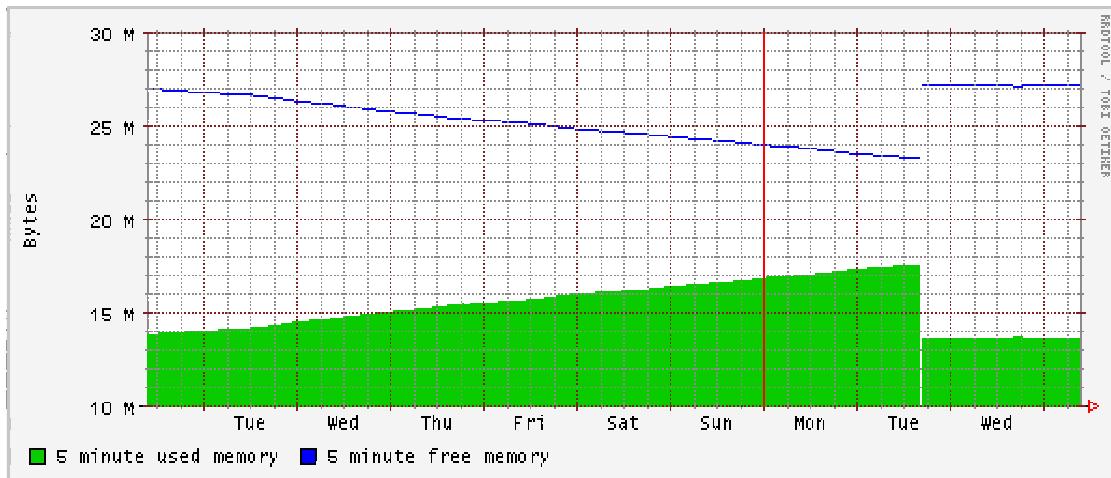


FIG. 35 – mémoire du routeur atm faisant la jonction du campus avec renater

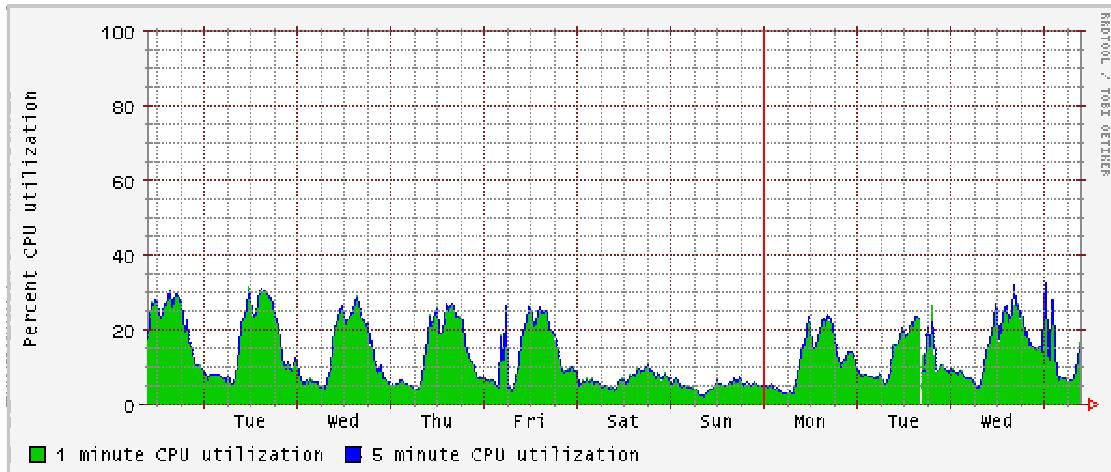


FIG. 36 – utilisation du processeur sur le même routeur

de cette façon, je vous le conseille. C'est le premier logiciel que j'ai installé, alors que je n'avais aucune notion de l'administration réseau. L'installation est vraiment simple (le seul petit problème est la recherche des modules perl manquants). Les fichiers de configuration sont lisibles et simples à modifier.

9 Mon

→ <http://www.kernel.org/software/mon/>

Mon est un logiciel de surveillance des services. Il interroge à intervalles réguliers le matériel et les applications et tient l'administrateur au courant du bon fonctionnement de ceux-ci. Il n'y a besoin d'aucun daemon sur les stations surveillées.

Je vous propose de découvrir ces fonctionnalités. Pour cela nous allons regarder son fichier de configuration.

Ce fichier commence par la définition de groupes. Chaque station, serveur ou routeur sur lesquels vous voulez surveiller le(s) même(s) élément(s) sont regroupés ensemble. Sur l'exemple suivant, le matériel appartenant au groupe *workstations* sera interrogé par les mêmes programmes avec le même intervalle.

```
hostgroup workstations noyer pin-noir saule fraisier
hostgroup serveurswww kaki www.urec.cnrs.fr av.serveurs-nationaux.jussieu.fr
hostgroup serveursmail kaki
hostgroup serveursldap kaki
```

La suite du fichier est composé de paragraphes. Ces derniers indiquent pour chaque groupe les services à surveiller, la durée des intervalles, le programme employé et les paramètres des alertes.

L'exemple qui suit concerne le groupe des serveurs web à surveiller. Toute les 10 minutes le script http est lancé. L'option *allow_empty_group* permet ce lancement même si le groupe est vide après des dysfonctionnements. Cette observation se fait durant toute la semaine. Cette période peut être ajustée (par exemple *period wd {Mon-Fri} hr {7am-10pm}*).

```
watch serveurswww
  service http
    interval 10m
    monitor http.monitor
    allow_empty_group
    period wd Sun-Sat
    alert mail.alert andreu@urec.cnrs.fr
    upalert mail.alert andreu@urec.cnrs.fr
#    alertevery 45m
    numalerts 1
```

Lors d'une défaillance du service, vous recevrez un mail à l'adresse voulue. Vous avez la possibilité de faire remonter l'alerte à un pager : *alert page.alert mis-pagers@domain.com*. Lorsque le service redémarre vous pouvez également être averti. La remontée de ces alarmes est paramétrable à volonté :

- *numalerts 1* signifie que vous ne voulez qu'une alerte par défaillance, même si celle-ci dure plusieurs heures.
- *alertevery 45m* pour un mail toutes les 45 minutes tant que le service n'est pas opérationnel.

- *alertafter 4*, vous êtes prévenu qu'àprès 4 défaillances consécutives.
- *alertafter 4 30m* pour une alarme si il y a 4 pannes en 30 minutes.
- *startupalert* pour une alarme lors du lancement de mon.

Voici un deuxième exemple plus fourni :

```

watch wwwservers
service ping
interval 2m
monitor fping.monitor
allow_empty_group
period wd Sun-Sat
#    alert qpage.alert mis-pagers
#        alert mail.alert andreu@urec.cnrs.fr
#            alertevery 45m
service http
interval 4m
monitor http.monitor
allow_empty_group
period wd Sun-Sat
#    alert qpage.alert mis-pagers
#        upalert mail.alert -S "web server is back up" andreu
#            alertevery 45m
service telnet
monitor telnet.monitor
allow_empty_group
period wd Mon-Fri hr 7am-10pm
alertevery 1h
alertafter 2 30m
alert mail.alert andreu@urec.cnrs.fr
#    alert page.alert mis-pagers@domain.com

```

Les services observables sont nombreux : ICMP echo, SMTP, Telnet, FTP, NNTP, HTTP, POP-3, IMAP, TCP-based services, Disk space, LDAP, DNS, mSQL, MySQL, Network latency, Sun RPC services, et quelques services basés sur SNMP.

Vous accédez à tout instant à son interface web (figure 37). Celle-ci vous montre dans un tableau les groupes définis ainsi que le programme de surveillance utilisé pour chacun. Ce dernier est rouge lorsqu'il y a un problème sur le réseau. En cliquant dessus vous accédez à la station qui est concernée dans le groupe. Cette interface vous propose aussi une liste de tous les problèmes déjà rencontrés.

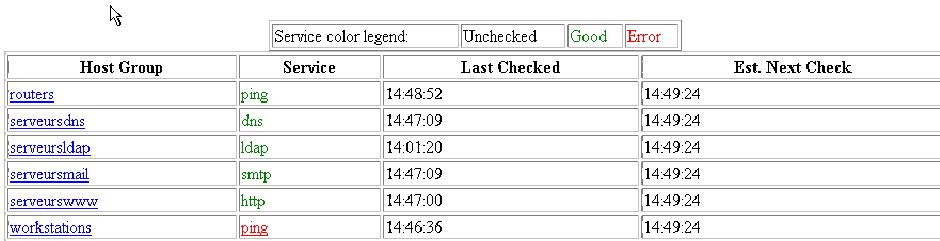
Voici deux en-têtes de mail envoyé par mon :

Subject:

ALERT serveurswww/http: www.urec.cnrs.fr (Wed Aug 16 15:58:01)

Subject:

UPALERT serveurswww/http: www.urec.cnrs.fr (Mon Aug 21 10:29:06)


FIG. 37 – *interface de mon*

Mon est écrit entièrement en perl et ne devrait pas poser de problèmes de portabilité. Je l'ai utilisé sur une distribution linux (Redhat) et je n'ai eu aucun problème. Il s'exécute en tant que démon et ne donne signe de vie que par votre boîte aux lettres. Je le trouve donc bien adapté à la surveillance de services. Vous êtes prévenus en temps voulu (si votre mail fonctionne) et selon vos désirs grâce à un fichier de configuration malléable.

10 Acct-cisco

Acct-cisco, comme son nom l'indique, ne fonctionne qu'avec les routeurs Cisco. Heureusement ils sont nombreux, ce qui explique sa place ici. De plus c'est un logiciel libre (adapté par Pierre David³, Université de Versailles Saint Quentin). Les informations qu'il fournit sont intéressantes et ne se retrouvent pas délivrées sous cette forme de comptabilité dans les logiciels déjà cités.

C'est par mail que vous recevrez chaque jour les informations de acct-cisco. Il interroge chaque minute par telnet la table d'accounting présente sur les routeurs cisco. Il stocke les données dans un fichier (dont la taille peut être importante suivant le trafic) et les traite par défaut la nuit, puis envoie le résultat. Enfin les données sont compressées et archivées, ce qui permet une étude ultérieure si cela est nécessaire (problème de sécurité...).

Voici le répertoire où sont gardés les traces (réseau UREC Grenoble). La dernière ligne correspond au fichier du jour, il sera compressé le lendemain matin. Ce fichier a une taille d'environ 30 Mo en fin de journée à l'UVSQ sur une liaison RERIF à 2 Mbit/sec.

```
andreu-2 ls -l /usr/local/acct/log/
total 1600
-rw-r--r-- 1 root      root      53501 Aug  3 23:59 acct.20000803.gz
-rw-r--r-- 1 root      root      92443 Aug  4 23:59 acct.20000804.gz
-rw-r--r-- 1 root      root      44613 Aug  5 23:59 acct.20000805.gz
-rw-r--r-- 1 root      root      42130 Aug  6 23:59 acct.20000806.gz
-rw-r--r-- 1 root      root     118490 Aug  7 23:59 acct.20000807.gz
```

³Pierre.David@prism.uvsq.fr

```
-rw-r--r-- 1 root      root      83959 Aug  8 23:59 acct.20000808.gz
-rw-r--r-- 1 root      root      21791 Aug  9 10:32 acct.20000809.gz
...
-rw-r--r-- 1 root      root     238232 Aug 22 12:31 acct.20000822
```

La table d'accounting d'un routeur cisco relève les adresses IP (source et destination) des paquets, et pour chaque liaison, comptabilise le nombre de paquets et d'octets.

La première information extraite de la table est le débit utile (en kilo-octets par seconde) :

Debit utile en Ko/s :

```
Moyenne      : 29,544170724
Ecart-type   : 82,3323361419
Minimum      : 0,0
Maximum      : 393,788655599
```

puis des données relatives à la table elle-même. Le nombre d'entrées et si la table fut saturée. Si ce dernier cas arrive il faut augmenter sa taille. Pour cet exemple, la taille de la table est de 512 entrées (à chaque interrogation, la table est vidée).

Nombre d'entrees dans la table d'accounting :

```
Moyenne      : 11,2668097282
Ecart-type   : 8,33033479552
Minimum      : 0
Maximum      : 79
```

Saturations dans la table d'accouting : 0.

Lorsque le routeur n'est pas atteignable ou que la machine sur laquelle tourne acct-cisco les dates sont enregistrées :

Pannes du routeur : 1. Les dates sont :
de 2028 à 2030

Viennent ensuite les transactions suspectes. Celle-ci sont définies dans le fichier de configuration.

Transactions suspectes : 1.

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
1412	M 195.220.197.1	212.213.10.0	1	71

Le nombre de machines non enregistrées dans le DNS et leurs adresses sont don-

nées, puis les 50 plus grosses connexions :

Machines non enregistrées dans le DNS : 0.

Les 50 plus grosses connexions

Adresse 1	Adresse 2	Trafic 1->2	Trafic 2->1	%
kaki.grenoble.urec.cnrs.fr	janus.paris.urec.cnrs.fr	273.943.731	0	86,32
kiwi.grenoble.urec.cnrs.fr	janus.paris.urec.cnrs.fr	27.097.977	0	8,54
kaki.grenoble.urec.cnrs.fr	? (212.111.41.156)	2.825.352	0	0,89
kaki.grenoble.urec.cnrs.fr	ns.felk.cvut.cz	691.370	0	0,22

Les plus grosses connexions internes et externes sont aussi présentes :

Les 50 plus gros consommateurs internes

Machine	In	Out	%
kaki.grenoble.urec.cnrs.fr	0	288.988.578	91,06
kiwi.grenoble.urec.cnrs.fr	0	27.097.977	8,54

Vous accédez en fin de mail à la courbe du trafic en ascii (figure 38) :

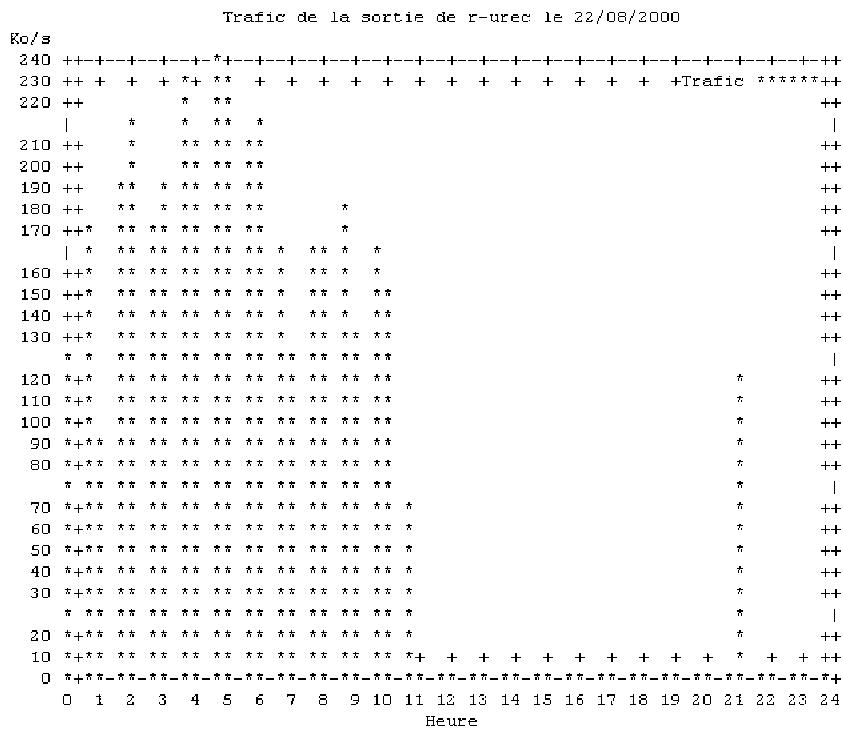


FIG. 38 – courbe du trafic sur 24h

Acct-cisco est là encore facile à installer et configurer. Il ne faut pas oublier de démarrer la table d'accounting sur votre routeur (c'est une commande d'interface et non générale). La documentation qui accompagne les sources est très claire (est présent également l'article de Pierre David paru lors de JRES99).

11 Conclusion

J'espère que cette présentation vous a satisfaits. Comme vous avez pu le constater, les logiciels du domaine public sont nombreux, mais avec des fonctionnalités diverses. Ils permettent une surveillance correcte de votre réseau. Je pense que les cinq logiciels précédents forment un kit de surveillance qui couvrent tous les besoins.

12 Annexes

12.1 Détection d'un scan

12.1.1 avec cricket

Cricket n'est pas conçu pour détecter les scans. Mais cet exemple montre que l'on peut repérer certain type de scan. Celui-ci est réalisé artificiellement avec nmap depuis une machine extérieure au réseau. C'est un scan TCP. Normalement, le routeur possédant des filtres, nmap ne voit que les ports non filtrés. C'est effectivement ce qui se passe.

J'observe avec cricket la variable `icmpDestUnreach` sur le routeur. Celle-ci indique le nombre de réponses du routeur (suivant le protocole ICMP) lorsqu'il reçoit des paquets ayant une adresse de destination filtrée. J'ai trouvé cette variable à l'aide de Tkined (page 12.2).

Comme on le voit sur la figure 39, le scan correspond au dernier pic. Le pic précédent est aussi un scan (de moi également).

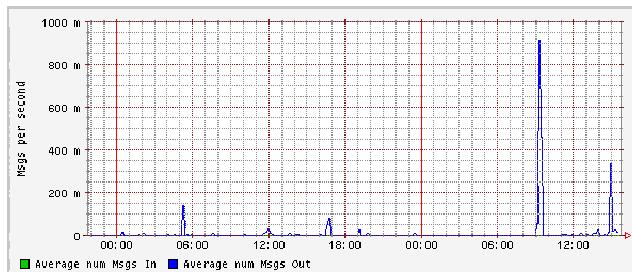


FIG. 39 – la variable `icmpDestUnreachs`

Bien sur cette méthode de détection n'est pas très fiable. Un scan relativement lent (pour la durée entre chaque paquet envoyé) passera sans doute inaperçu. Mais on peut déjà détecter les scans par défaut des logiciels tel que nmap.

12.1.2 avec ntop

Ntop est placé derrière le routeur, à l'intérieur du réseau. Nous ne devrions pas capter la moindre information sur le scan. Et pourtant ntop vous montre bien la tentative de scan avec nmap. En effet, lorsque le routeur arrête les paquets, il renvoie un paquet icmp, auquel nmap répond par un paquet TCP avec le syn RST. Ce dernier paquet passe à travers le routeur pour fermer une connexion TCP (qui n'existe pas en l'occurrence). Et c'est ce paquet qui est vu par ntop.

Les informations sur le scan se trouvent à plusieurs endroits : sur la page correspondant au poste scanné, dans le tableau IP Service / Port Usage (figure 40) et sur la page IP protocol subnet usage (figure 41). Les mille premiers ports sont présents avec à chaque fois le même nom de machine.

Cette détection est néanmoins moins fiable que la précédente car elle dépend du comportement de l'outil de scan et du filtre sur le routeur.

IP Service/Port Usage					
IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
1	1			4/600	atlantide-2.grenet.fr
2	2			6/840	atlantide-2.grenet.fr
3	3			8/960	atlantide-2.grenet.fr
4	4			6/720	atlantide-2.grenet.fr
5	5			3/540	atlantide-2.grenet.fr
6	6			6/840	atlantide-2.grenet.fr
7	7			4/240	atlantide-2.grenet.fr
8	8			4/720	atlantide-2.grenet.fr
9	9			6/720	atlantide-2.grenet.fr
10	10			4/600	atlantide-2.grenet.fr
11	11			4/600	atlantide-2.grenet.fr
12	12			6/840	atlantide-2.grenet.fr
13	13			6/720	atlantide-2.grenet.fr
14	14			4/600	atlantide-2.grenet.fr
15	15			4/600	atlantide-2.grenet.fr
16	16			3/540	atlantide-2.grenet.fr
17	17			6/720	atlantide-2.grenet.fr
18	18			3/240	atlantide-2.grenet.fr
19	19			1/60	atlantide-2.grenet.fr
ftp-data	20			5/600	atlantide-2.grenet.fr
ftp	21			4/600	atlantide-2.grenet.fr
22	22			4/600	atlantide-2.grenet.fr
telnet	23			4/600	atlantide-2.grenet.fr
24	24			6/840	atlantide-2.grenet.fr

FIG. 40 – services contactés sur kaki

12.2 Tkined (Scotty)

→ <http://wwwhome.cs.utwente.nl/\%7Eschoenw/scotty/>

Scotty n'ayant pas été choisi, je ne vous le présente pas comme les autres. Je vais vous parler simplement d'une de ces fonctionnalités que je trouve bien utile.

Le “module” Tkined permet de superviser votre réseau comme bien d'autres logiciels (interrogation des équipements par ping et le protocole snmp). Il peut découvrir le réseau, mais la carte tracée est aplatie, je vous conseille de la créer à l'aide de votre souris (même si vous n'êtes pas dans un logiciel de dessin et qu'apparemment le déplacement d'objets n'existe pas : il est nécessaire d'employer le redimensionnement pour y palier). La fonctionnalité intéressante est que Tkined propose une fenêtre présentant l'arbre de la MIB-2 (figure 42). Vous accédez ainsi à n'importe quelles variables. Après avoir sélectionner un de vos équipement, vous pouvez alors

IP Protocol Subnet Usage		
Service	Clients	Servers
1	1	• kaki
2	2	• kaki
3	3	• kaki
4	4	• kaki
5	5	• kaki
6	6	• kaki
7	7	• kaki
8	8	• kaki
9	9	• kaki
10	10	• kaki
11	11	• kaki
12	12	• kaki
13	13	• kaki
14	14	• kaki
15	15	• kaki
16	16	• kaki
17	17	• kaki
18	18	• kaki
19	19	• kaki
ftp-data	20	• kaki
ftp	21	• kaki
22	22	• kaki
		• 127.0.0.1

FIG. 41 – services utilisés sur le réseau

interroger la variable désirée (à condition que celle-ci existe dans la mib installée, dans le cas contraire vous n'aurez aucune réponse).

La description de chaque variable est présente :

```
Descriptor: ifInOctets
MIB Module: RFC1213-MIB
Identifier: 1.3.6.1.2.1.2.2.1.10
SMI Macro: OBJECT-TYPE
Max. Access: read-only
ASN.1 Syntax: Counter32
File: /usr/lib/tnm2.1.10/mibs/rfc1213.mib
```

The total number of octets received on the interface, including framing characters.

et voici la réponse sur cette dernière du routeur r-urec :

```
r-urec.grenoble.urec.cnrs.fr [195.220.197.254:161] [Tue Aug 22 15:55:04 CEST 2000]:
  ifInOctets.1 : 1477723830
  ifInOctets.2 : 2910427382
  ifInOctets.3 : 0
  ifInOctets.4 : 0
```

12.3 InterMapper

→ <http://www.dartware.com/intermapper/>

InterMapper découvre votre réseau internet et en trace la carte. Utilisant SNMP, il présente l'état des équipements et des liens et garde un fichier log. Il fonctionne

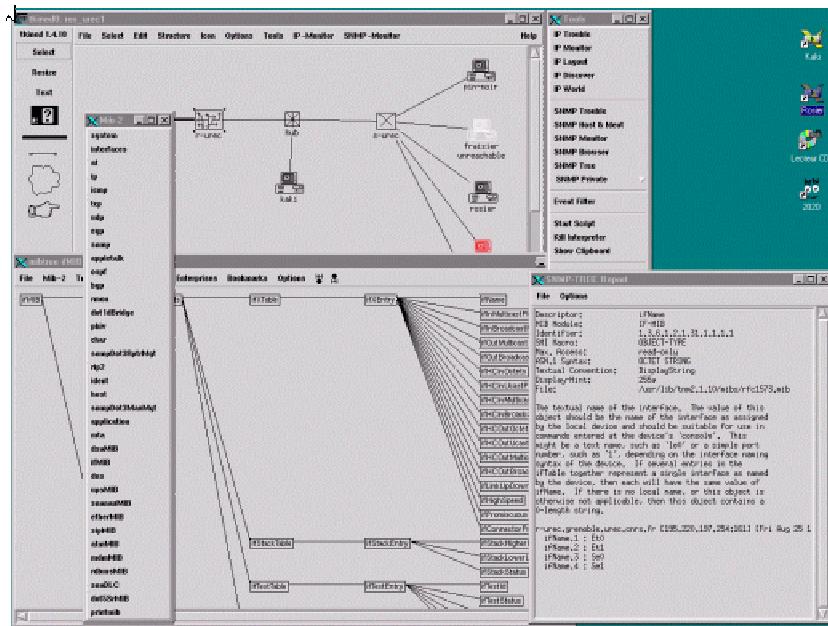


FIG. 42 – fenêtres de tkined

sur Mac uniquement, et n'est pas gratuit (son prix est inférieur à 10.000 FF). Mais sa carte peut en ravir plus d'un (fig. 43).

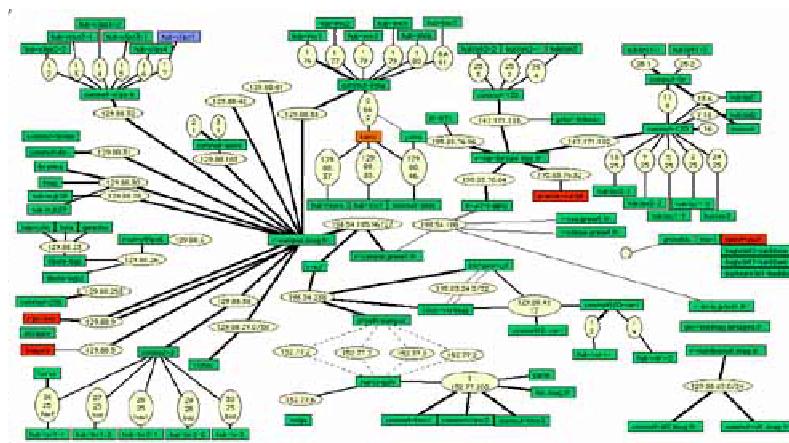


FIG. 43 – surveillance d'un réseau avec intermapper

12.4 Quelques liens

- des sites où sont répertoriés de nombreux logiciels (surveillance, analyse de réseaux, ...):
 - <http://www.caida.org/home/>

- http ://linux.davecentral.com/ pour Linux
- http ://www.linux-center.org/fr/networking/net-monitoring/index.html
- des rapports sur l'administration réseau et les plates-formes d'administration par des élèves de l'EPITA :
 http ://www.sda.cc/dossiers/
- la page perso de Imed Romdhani, étudiant à l'Université Louis Pasteur (Strasbourg) :
 http ://www.geocities.com/imed_romdhani
- des exposés des auditeurs du CUEFA :
 http ://gaston.cuefa.inpg.fr/ plisson/reseaux/expose.htm
- un cours sur les réseaux haut débit, l'administration et la sécurité :
 http ://www.ensicaen.ismra.fr/ lefebvre/cour3-5-6.html
- les logiciels libres dans l'académie de Grenoble :
 http ://www.ac-grenoble.fr/carmi-internet/doc/admin_sys_libre.html