

# Métrieologie

# des Systèmes

# d'Information



Rapport de stage  
technicien :

Métrologie  
des Systèmes  
d'Information

## **Remerciements**

Tout d'abord, je tiens à exprimer toute ma reconnaissance envers M. SCHNEIDER Johan, pour m'avoir accueilli au sein de CSI Systèmes et Réseaux.

Je souhaiterais ensuite remercier Melle NEVEU Anne-Sophie, grâce à qui j'ai découvert CSI lors du 13<sup>ème</sup> Forum de Haute-Normandie.

J'aimerais remercier M. DELAUNAY Arnaud, mon tuteur, pour sa disponibilité et son implication dans ce stage, et M. MORIN Christophe d'Avolys pour sa documentation.

Enfin, je remercie Melle GUIRADO Aurélie, les collaborateurs de CSI Systèmes & Réseaux et l'ensemble du personnel de CSI.

## Sommaire

Introduction	P 6
<b>A / Présentation de l'entreprise : Altitude</b>	<b>P 7</b>
<b>1 ) Altitude Télécom</b>	P 8
<b>2 ) Avolys</b>	P 9
<b>3 ) CSI</b>	P 10
1 ) CSI Décisionnelle	P 11
2 ) CSI Ingénierie Logicielle	P 11
3 ) CSI Systèmes et Réseaux	P 12
<b>B / Sujet du stage : Métrologie des Systèmes d'Information</b>	<b>P 15</b>
<b>1 ) Le cahier des charges</b>	P 15
1 ) Périmètre de l'étude et dimensionnement de la configuration	P 15
2 ) Expressions des besoins	P 15
<b>2 ) Etude des différents outils</b>	P 15
<b>3 ) Moyens mis à ma disposition par CSI</b>	P 16
<b>C / La supervision de réseaux et de systèmes</b>	<b>P 17</b>
<b>1 ) Qu'est-ce que la supervision de réseaux ?</b>	P 17
<b>2 ) Qu'est-ce que la supervision de systèmes ?</b>	P 17
<b>D / Les outils de supervision étudiés</b>	<b>P 19</b>
<b>1 ) « Big Brother is watching you »</b>	P 19
➤ Qu'est-ce que Big Brother ?	P 19
➤ Licence Big Brother	P 19
➤ Comment fonctionne Big Brother ?	P 20
➤ Utilisation de Big Brother : Réponse au cahier des charges	P 21
<b>2 ) MRTG</b>	P 22
➤ Qu'est-ce que MRTG ?	P 22
➤ Comment fonctionne MRTG ?	P 22
<b>3 ) RRD Tool</b>	P 25
➤ Qu'est-ce que RRD Tool ?	P 25
➤ Comment fonctionne RRD Tool ?	P 25
➤ Qu'est-ce que la représentation polonaise ?	P 26
<b>4 ) Treshold</b>	P 27
➤ Qu'est-ce que Treshold ?	P 27
➤ Comment utilise-t-on Treshold ?	P 27
Conclusion	P 28
Bibliographie	P 29
Annexes	P 30

## **Introduction**

Dans le cadre du cursus INSA, et à l'issue de la 3<sup>ème</sup> année, les étudiants sont invités à découvrir le monde du travail grâce à un stage technicien d'un mois minimum. Dans l'optique du Département Architecture des Systèmes d'Information, mon stage s'est déroulé pendant 6 semaines chez CSI « Systèmes et Réseaux ».

CSI est une société de service en ingénierie informatique, qui apporte aux entreprises un soutien logistique et technique en matière de solutions informatiques.

C'est lors d'une relation avec un client, qu'un cahier des charges leur a été soumis. Le client, après un accroissement important de son parc de machines, demande une solution afin de pouvoir superviser son réseau et ses systèmes. Le projet que l'on m'a confié était donc de répondre à ce cahier des charges, par la rédaction de procédures d'installation. Afin que quiconque puisse installer la solution, les procédures se devaient d'être claire, simple et illustrée.

Après une présentation du groupe Altitude et de la société CSI « Systèmes et Réseaux », nous définirons le sujet du stage, les outils étudiés et enfin les moyens mis à disposition.

Pour des raisons de compréhension du projet, nous définirons la supervision de réseaux et de systèmes.

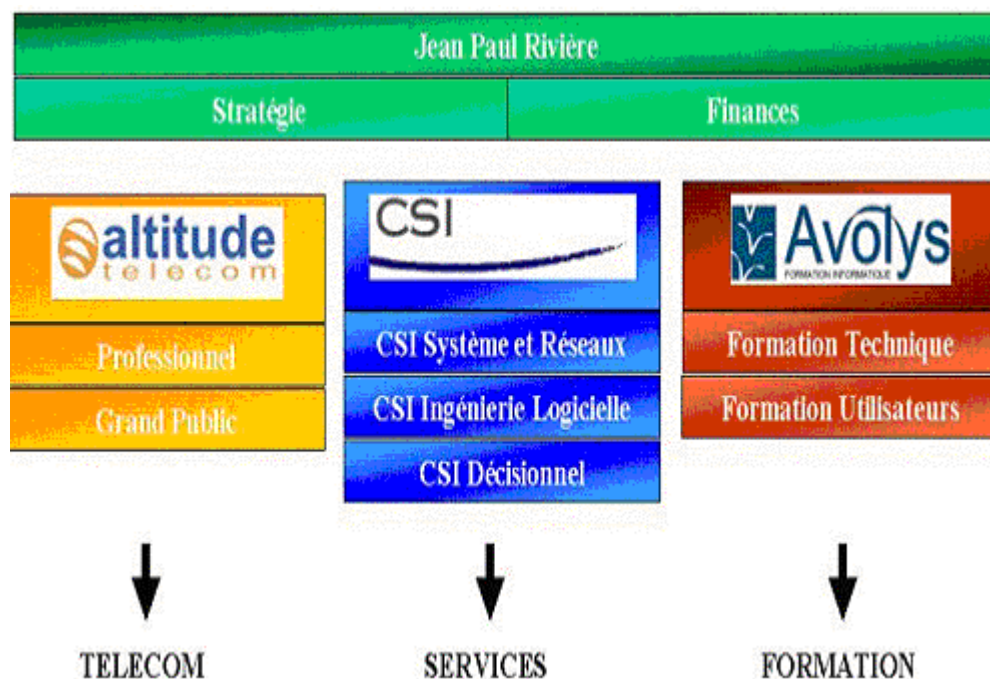
Enfin, nous étudierons différents outils pour répondre aux exigences du cahier des charges.

## A / Présentation de l'entreprise : Altitude

Pour mener à bien une mission lors d'un stage en entreprise, il est nécessaire de connaître la société et ses activités.

Dans le cas présent, mon stage se déroulait au sein de CSI « Systèmes et Réseaux ». Cette SSII ( Société de Service d'Ingénierie Informatique ) est une branche de la société CSI qui fait partie du groupe Altitude.

### Organisation du groupe Altitude



Le groupe Altitude est situé à Mont Saint-Aignan au Parc Technologique de la Vatine. Altitude est une société de gestion et de direction qui est au service de trois sociétés commerciales distinctes, afin d'optimiser leurs fonctionnements. Altitude est le regroupement de plusieurs sociétés mais plus particulièrement Altitude Télécom, Avolys et CSI.

- **Altitude Télécom** est un fournisseur d'accès et de services sur Internet pour les professionnels et le grand public,
- **Avolys** est une société spécialisée dans les formations informatiques, bureautiques et techniques,

- **C.S.I.** (Conseils Services Informatiques) est une société prestataire de services informatiques.

Créée en janvier 1995 et dirigée par M. Jean-Paul Rivière, Altitude emploie quatre autres personnes qui exercent, pour les trois entités commerciales, les fonctions de direction générale, et de direction financière. Ce groupe représente 240 personnes.

Pour 2001, le chiffre d'affaires du groupe s'élève à 15 Millions d'euros (150 millions de francs).

Implanté dans la région rouennaise depuis sa création, le groupe s'impose aujourd'hui comme le leader de la région Nord-Ouest dans ses métiers. L'atout "proximité" est largement appréciée par les clients et se fait grâce aux différentes agences d'Evreux, du Havre, de Lille, de Caen et depuis peu Paris.

#### Organigramme du Groupe Altitude



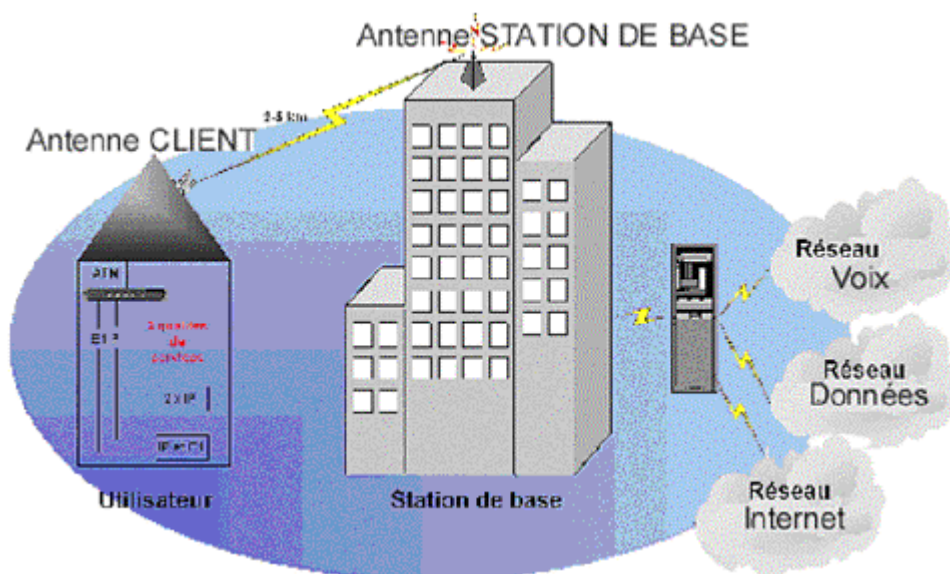
### **1) Altitude Télécom**

Altitude Télécom est le premier fournisseur privé d'accès Internet en Haute-Normandie pour les entreprises et les particuliers. Altitude Télécom développe son savoir-faire sur quatre activités qui sont :

- l'accès à toutes les fonctions d'Internet pour les professionnels et les particuliers
- l'hébergement et la maintenance de serveur Web
- les services télécoms tels que sécuriser ou superviser un réseau.
- la boucle locale radio ( Transmission hertzienne point multi point qui permet aux usagers d'une unité urbaine d'accéder à tous les services de Télécommunications ) permettant l'accès à tous les types de télécommunications



### Représentation de la boucle locale radio



Altitude Télécom est aussi un partenaire privilégié dans les technologies d'avenir comme l'ADSL, la fibre ou le câble.

Aujourd'hui, Altitude Télécom est en pleine évolution puisqu'elle n'existe que depuis octobre 1996 et compte déjà plus de 4000 clients dont 700 entreprises. Son chiffre d'affaires en 2001 était de 2.44 Millions € avec un effectif de 50 personnes.



## 2) Avolys

Depuis l'année 2000, la société Avolys est le regroupement des branches formations de 4 entreprises (CSI Formation-Résolution, P.C.S. Entreprise, Expertease, Homecom), toutes fortement implantées et reconnues sur leur région. Le but de ce regroupement est de constituer une implantation nationale de professionnels de la formation, à travers de nombreux franchisés ( entreprise ayant acheté le droit de se nommer Avolys ) dans toute la France.

Elle donne accès à des formations techniques et utilisateurs de haut niveau par l'intermédiaire d'ingénieurs formateurs :

- Systèmes et réseaux (administration de système, maîtrise d'OS Windows, Unix..., implémentation de réseaux (interconnexion TCP/IP),
- Messagerie Electronique (administration ou migration),
- Langages et développement (C, C++, JavaScript, VB, etc....)
- Bases de données (Microsoft, Oracle, etc..)

- Bureautique (environnements, tableurs et traitements texte, bases de données utilisateur, gestion de projets),
- Messagerie (Lotus, Outlook, etc...)
- Internet (mieux comprendre pour utiliser, HTML, etc....)
- Utilisation de Windows (98, NT, 2000, etc....)



### 3 ) CSI

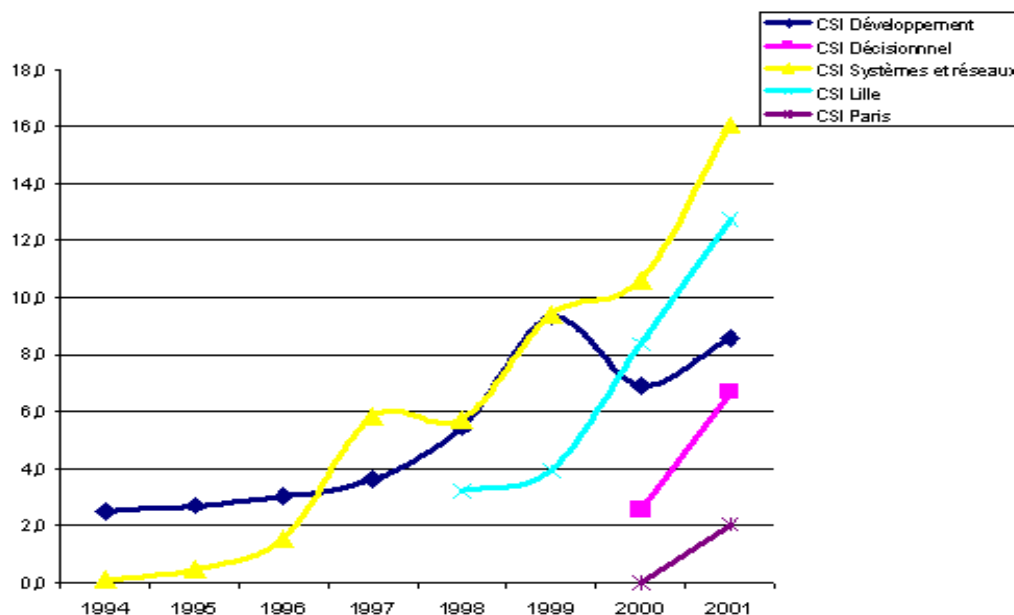
Créée en 1989, la société CSI est en constante évolution (12 personnes en 1995, 35 personnes en 1998, 140 personnes en 2002). Elle possède des agences sur Rouen, Le Havre, Lille, Caen et Paris.

Elle propose son savoir-faire afin que les entreprises puissent optimiser leur parc informatique, elle s'affirme comme le relais technique des plus grands éditeurs de logiciels. Les compétences de CSI s'articulent autour des domaines suivants :

- l'informatique décisionnelle
- l'ingénierie logicielle
- les systèmes et les réseaux

#### Croissance du chiffre d'affaires de CSI durant ces dernières années

Millions de Francs



## 1) CSI Décisionnelle

La partie décisionnelle, créée en 2000, est un centre de formation agréé Business Objects. Business Objects est un outil intégré d'aide à la décision permettant d'exploiter, d'analyser et de partager des gisements d'informations qu'abritent les différentes bases de données d'une organisation.

C'est une solution idéale pour générer des tableaux de bord (Documents informatiques utilisés dans les entreprises servant à suivre les données chiffrées de l'entreprise) faciles à utiliser, rassemblant en un coup d'œil les indicateurs clés ou pour interroger les bases de données et manipuler les résultats obtenus. Cela permet aux entreprises de prendre des décisions grâce aux résultats de leurs données (production, ventes...) que leurs ont fournis les logiciels informatiques.

L'équipe "décisionnelle" est composée d'une quinzaine de personnes dont 5 formateurs certifiés Business Objects.

Quelques interventions courantes de l'équipe :

- La réalisation de projet décisionnel dans son ensemble
- le conseil (conduite de projet, conception de base, maquettage)
- l'assistance technique (conception d'univers, développement de requêtes)
- la vente de licences Business Objects
- l'audit
- les formations techniques et utilisateurs Business Objects.

Les chiffres :

	<b>2000</b>	<b>2001</b>	<b>Evolution</b>
<b>Prestation de Service</b>	<b>127 K€</b>	<b>360 K€</b>	<b>+ 180 %</b>
<b>Formation</b>	<b>136 K€</b>	<b>250 K€</b>	<b>+ 85 %</b>
<b>Licences</b>	<b>106 K€</b>	<b>318 K€</b>	<b>+ 300 %</b>

## 2) CSI Ingénierie logiciel

CSI Ingénierie logiciel vient de la division de CSI en trois pôles : décisionnel, ingénierie logiciel et systèmes & réseaux en 2000.

L'équipe "développement" est composée de 26 personnes. Elle est spécialisée dans les langages de programmation et l'élaboration de bases de données. Elle peut également faire de l'administration, de l'optimisation et de la migration de bases de données.

Quelques interventions courantes de cette équipe:

- Elaboration de schéma directeur informatique.
- Conseil dans l'élaboration d'un dossier d'appel d'offres orientée prestation intellectuelle
- Rédaction de spécifications fonctionnelles.
- Administration, optimisation, migrations de bases de données relationnelles.
- Assistance à la mise en oeuvre d'application bureautique.
- Développement d'outils et application de gestion.
- Développement d'application client / serveur.

### **3 ) CSI Systèmes et Réseaux**

Cette branche de l'entreprise sera plus détaillée car c'est cette agence qui m'a permis d'effectuer mon stage au sein de son équipe.

CSI systèmes et réseaux, apparu en 2000, n'a pas cessé de croître et de se développer. CSI systèmes et réseaux assiste les entreprises pour l'intégration de leurs serveurs et le déploiement de leur parc micro-informatique. Parmi les collaborateurs, 30 sont sur des projets d'info-gérance, 20 en délégation de personnel et 10 en projets.

Les principaux partenaires de CSI :



Tout d'abord, CSI systèmes et réseaux est aujourd'hui dirigée par Johan Schneider en tant que directeur d'agence, qui a succédé à Alexandre Deshayes au mois d'Avril 2002. Assisté par Aurélie Guirado, il s'occupe de 50 collaborateurs dispersés dans toute la Normandie.

CSI S&R a pour but de fournir aux entreprises un service informatique. Ce service peut se décomposer en trois métiers différents :

- Info-gérance d'exploitation
- Délégation de personnel
- Consulting et expertise

D'une part, les projets d'info-gérance consistent à fournir des techniciens aux entreprises clientes afin de gérer entièrement le parc informatique de celle-ci.

D'autre part, les délégations de personnel sont des contrats à durée déterminée avec l'entreprise cliente où le technicien s'occupe des tâches courantes dans son réseau informatique. Contrairement à l'info-gérance, c'est l'entreprise cliente qui gère son parc micro-informatique, toutes les décisions sont prises par l'entreprise.

Enfin, le consulting et l'expertise sont des prestations assez courtes pour effectuer une activité ponctuelle chez le client.

Le Département Systèmes et Réseaux de CSI assiste ses clients dans :

- Le conseil, l'expertise, l'audit d'architecture, l'audit sécurité, la préconisation,
- Le déploiement, la migration, l'exploitation, la supervision et la maintenance de parc,
- La mise en place de centres d'appels,
- La sécurisation, la sauvegarde, le stockage, le clustering, les clients légers,
- Dans la maintenance des existants (optimisation, restauration...).
- La délégation de ressources informatiques
- La gestion de l'externalisation des moyens informatiques

Les chiffres de CSI « systèmes et Réseaux » :

	2000 Réalisé	2001 prévu	2001 réalisé
Chiffre d'affaires	1.52 M€	2.23 M€	2.43 M€
Résultats	0.08 M€	0.3M€	0.29 M€

Quelques exemples de prestations :

**Valois :** CSI gère aujourd'hui le support utilisateur (intervention de niveau 2 chez l'utilisateur), les déploiements de PC et l'administration des serveurs de Niveau 1 des 1000 PC de la société Valois.

Effectif CSI : 9 personnes.

**Hurel-Hispano :** CSI gère le parc micro-informatique de Hurel-Hispano (650 PC). On retrouve dans cette prestation une fonction supplémentaire : le support expert chargé non pas de faire du curatif sur les problèmes mais de trouver des solutions qui éliminent les sources des problèmes. Cette fonction est gérée par un technicien expert complètement détaché sur ce poste. Cela lui permet de faire progresser l'ensemble de la prestation (exemple : amélioration d'un master).

Effectif CSI : 8 personnes.

**EDF :** CSI gère les interventions terrains (niveau 2) de tous les centres de production d'électricité (CNPE de Paluel, Penly Flamanville, Dunkerque, Gravelines, le Havre...) soit 7000 PC et 350 serveurs NT 4.0. Pour cela, une équipe de 12 techniciens gère les interventions non résolues par l'équipe help desk téléphonique.

Les techniciens se doivent de résoudre des incidents ouverts par l'équipe Help Desk via un outil de gestion de parc (et d'incidents) évolué. CSI est engagé contractuellement sur les temps de résolution des incidents.

Effectif CSI : 27 personnes.

**Sidel** : CSI a délégué deux personnes dans l'équipe SIDEL bureautique. Ils sont chargés des intégrations et livraisons de machines ainsi que des interventions de niveau 2 chez l'utilisateur.

CSI a déployé une équipe de 11 Ingénieurs et Techniciens pour mener à terme la Migration de l'architecture système vers Windows 2000 Server et Windows 2000 Professionnel.

Effectif CSI : 11 personnes



## **B / Sujet de stage : Métrologie des Systèmes d'Information**

### **1 ) Le cahier des charges**

Au début de l'année 2002, CSI « systèmes et réseaux » a reçu un cahier des charges provenant d'une grande entreprise parisienne. Celle-ci a connu un déploiement important de nouvelles machines opérationnelles (Serveurs, unités de disque...), causée par la multiplication des applications réseaux.

Devant l'accroissement important du nombre de machines d'une part, et de la complexité de certaines applications d'autre part, le client souhaite se doter d'un nouvel environnement de supervision réseau. Celui ci devra être fiable, performant et devra permettre d'avoir une vue globale sur l'état de fonctionnement de l'ensemble des services et systèmes existants.

Cet outil devra être en mesure d'alerter rapidement en cas de dysfonctionnement, entraînant une indisponibilité de service, mais il devra également alerter au travers de messages électroniques et SMS, des opérations préventives à réaliser pour éviter ces blocages ( remplissage des espaces disques, surcharge CPU et mémoire ...).

L'objectif pour CSI « systèmes et réseaux » est donc de trouver l'outil répondant aux besoins afin d'assurer par la suite, son intégration dans l'environnement de l'entreprise.

### **1 ) Périmètre de l'étude et dimensionnement de la configuration**

La partie serveur de cet outil devra être implémentée sur un serveur AIX ou Solaris et devrait être capable d'assurer la surveillance d'un environnement composé de 70 serveurs NT, une centaine de serveurs UNIX et de divers équipements réseaux.

### **2 ) Expression des besoins**

Pour répondre aux besoins de surveillance du client, l'outil devra réaliser les différentes fonctions comme contrôler les processus en cours, analyser les fichiers logs, contrôler la charge CPU et l'espace disque disponible ainsi que la mémoire utilisée. Toutes ces conditions sont notées dans le cahier des charges qui se trouve en annexe de ce rapport.

## **2 ) Etudes des différents outils**

Le but d'une Société de Service en Ingénierie en Informatique est de vendre un service à un client. Dans notre cas, le client a bien précisé sa demande, mais laisse à CSI le choix de l'outil de supervision.

Le client a montré le désir, dans le cahier des charges, d'avoir une ou plusieurs consoles de supervision tournant sur des plates-formes différentes. Ce seront donc ces machines qui joueront le rôle de récupérer les différentes données des clients hétérogènes.

CSI utilisant principalement le système d'exploitation Windows, il était très intéressant pour eux de connaître la manière d'installer et d'utiliser le produit final sous Linux.

Au final, on doit donc obtenir un outil répondant au mieux au cahier des charges et utilisant des logiciels gratuits.

L'objectif de mon stage sera donc de répondre à ce cahier des charges. Pour cela, il m'a été nécessaire de m'informer sur la supervision de réseau et ses outils. Ensuite, j'ai dû installer, tester et utiliser les différents outils trouvés afin de rédiger les procédures d'installation, de configuration et d'intégration des différents logiciels. Celles-ci se trouveront en annexes.

## **3 ) Moyens mis à ma disposition par CSI**

J'avais à ma disposition :

- 2 machines
- Un graveur, une imprimante...
- Accès au web, à une boîte de messagerie
- Accès à de nombreux logiciels, CD d'installation de système d'exploitation, etc...



## C / La supervision de réseaux et de systèmes

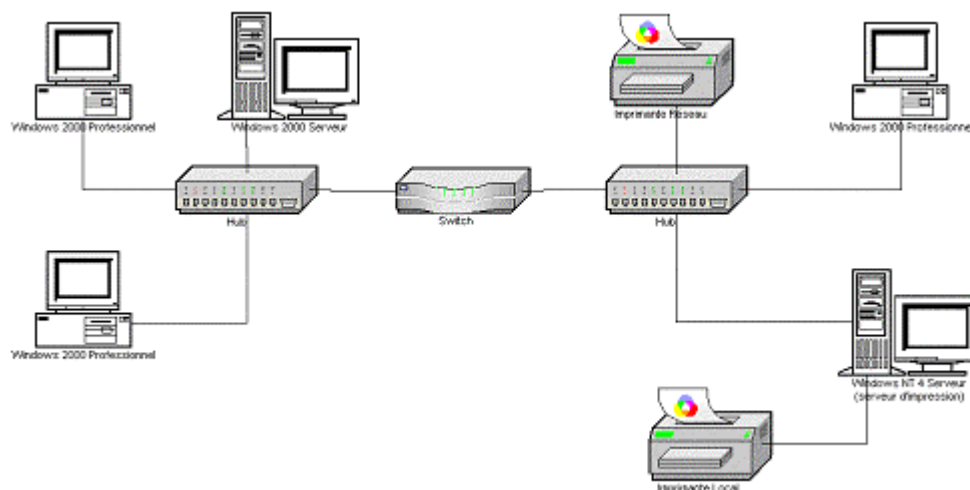
### 1 ) Qu'est-ce que la supervision de réseaux ?

Aujourd'hui, la disponibilité des réseaux informatiques devient de plus en plus cruciale pour chaque entreprise. Il est donc nécessaire de suivre en permanence l'évolution et le fonctionnement du réseau à partir de notifications d'alarmes et de messages collectés par une application.

Pour cela, on met en place des systèmes d'administration et de supervision performants, capables d'observer l'activité des éléments constitutifs du réseau.

Un réseau peut se simplifier de la manière suivante :

Schéma simplifié d'un réseau d'entreprise



En observant le schéma ci-dessus, on s'aperçoit de l'importance de la supervision car par exemple, si l'administrateur supervise le switch (élément actif et donc supervisable) et si celui-ci a une défaillance quelconque, il en sera tout de suite averti et pourra donc tout faire pour remédier à ce problème dans les plus brefs délais.

Pour transporter toutes ces informations concernant le matériel du réseau (serveur, matériel actif), ces systèmes utilisent les structures propres du réseau existant et permettent ainsi une mise en place simple et peu onéreuse de la supervision d'un réseau. Ces systèmes utilisent principalement deux protocoles :

#### ➤ **TCP / IP :**

Combinaison de 2 protocoles, TCP (Transmission Control Protocol) étant le protocole de la couche de transport orienté connexion qui assure une transmission fiable en duplex des données et IP (Internet Protocol) étant le protocole de la couche réseau et offrant un service

d'inter réseau en mode non connecté ; IP fournit des fonctions pour l'adressage, la spécification de type de service, la fragmentation, le ré assemblage et la sécurité

➤ **SNMP :**

Simple Network Management Protocol, protocole de gestion utilisé exclusivement sur les réseaux TCP / IP et permettant de surveiller, de contrôler, de collecter des statistiques concernant les éléments du réseau.

## 2 ) Qu'est-ce que la supervision de systèmes ?

La supervision de systèmes permet de connaître l'état de son poste. En effet, la supervision réseaux indique l'état du réseau global ( les différentes connexions) alors que la supervision système permet de se renseigner sur les machines constituant le réseau.

Cette surveillance peut aller du trafic réseau entrant et sortant d'une interface, jusqu'aux processus ou services s'exécutant sur l'ordinateur, etc...

Pour cela, deux architectures de supervision existent :

- Le Client / Serveur.
- L'utilisation du protocole SNMP.

## **D / Les outils de supervision étudiés**

### **1) « Big Brother is watching you »**



#### **➤ Qu'est ce que Big Brother ?**

Big Brother est un logiciel de supervision de réseau édité par Quest Software téléchargeable à l'adresse mail suivante : <http://www.bb4.com> , fonctionnant sur pratiquement tous les systèmes de type Unix (solaris, hpux, redhat, debian, mandrake) et Windows 2000.

Il fonctionne sur le modèle Client-Serveur et est simple d'utilisation. Ce logiciel utilise des scripts pour connaître en temps réel l'état des différents composants de votre machine et de votre réseau (connexion, charge cpu, taux remplissage des disques, mémoire, trafic...).

Le gestionnaire du réseau installe donc un client Big Brother sur chacun des composants qu'il veut surveiller, et installe bien évidemment sur une machine dédiée à la supervision la partie serveur de Big Brother, qui récoltera toutes les informations.

Pour chaque information, 3 états sont définis : un état de fonctionnement normal, un état « warning » et enfin un état critique (« panic »). Les seuils de chacun de ces états sont définis lors de la configuration du client et du serveur BB.

Le serveur Big Brother récupère donc ces infos et leur associe un code couleur (vert, orange et rouge). Une page HTML est donc créée, dans laquelle est inséré un tableau : en ligne les différentes postes supervisés et en colonne les données à surveiller sur les machines, à l'intersection une icône symbolisant l'état du matériel. Cette icône est le lien vers une page web détaillant le résultat du script.

Le fond de ces pages HTML prend la couleur la plus alarmante relevée lors de tous les contrôles, permettant à l'administrateur du réseau de connaître tout de suite l'état général du réseau. L'administrateur peut être également prévenu par mail lorsqu'un problème survient. Il est également possible de connaître l'historique des données sur la dernière journée ou sur plusieurs jours.

L'installation de Big Brother faisant l'objet d'une procédure, vous trouverez celle-ci en annexe.

### ➤ License Big Brother

Le logiciel Big Brother ne nécessite aucune licence pour un usage non lucratif. Par contre les entreprises vendant le produit, un service ou encore une aide en ligne, doivent acquérir la licence.

- Serveur / Client sous Unix = 695 \$ / unité
- Serveur Windows = 695 \$ / unité
- Client NT = 69 \$ / unité

Cette licence est dite 'Better than Free' ( mieux que gratuite ) car si la somme demandée est trop importante, des mesures de paiement peuvent être proposées d'une part, et plus 10% de cette somme sera versée à une des trois œuvres caritatives suivantes :

- Chid haven internationale : Crée des maisons pour les enfants en difficulté
- AmericaWork for Kid : Opère contre le travail des enfants.
- American Cancer Society : Ligue Américaine contre le cancer.

Dans le cas de CSI « Systèmes et Réseaux », la licence est gratuite car, c'est la mise en place de Big Brother chez le client qui est vendue, et non la supervision du réseau du client à l'aide du logiciel. Le client ne devra en aucun cas acquitter la licence, car il utilise Big Brother en interne.

### ➤ Comment fonctionne Big Brother ?



Big Brother fonctionne sur le schéma Client-Serveur, c'est à dire que le client envoie ses informations au serveur régulièrement. Le serveur met à jour l'affichage des pages web en fonction des caches, qu'il remplit lorsqu'il reçoit un message d'un client.

L'architecture de Big Brother, peut être très différente selon les choix. En effet, les fonctionnalités d'affichage ( BBDISPLAY ), de récupération des données ( BBNET ) et enfin de notification ( BBPAGER ) peuvent être soit séparées, soit réunies sur la même machine.

Pour la transmission des données, Big Brother utilise le port 1984 pour communiquer avec les machines à surveiller.

L'affichage de l'état des éléments est faite sur le serveur BBDISPLAY par l'intermédiaire d'une page HTML. Sur cette page, les machines et les services surveillés sont notifiés. L'état de ces services est représenté par un indicateur. Celui-ci peut prendre 6 valeurs, par degré d'importance (+ au - ) :

- : Service non-connecté
- : Service non-disponible
- ✱ : Service sans rapport
- : Service ayant atteint le deuxième niveau d'alerte

-  : Service ayant un atteint le premier niveau d'alerte
-  : Service OK

De plus en cliquant sur cet indicateur, la page de description de l'état du service est visible. Il est également possible de réunir les machines à surveiller en groupe, ce qui peut-être très utile (ex : les serveurs, Salle , Bâtiment, personnel...)

La notification est un service de Big Brother qui le différencie des autres logiciels de supervision. En effet, le serveur BBPAGER permet l'envoi de mails pour alerter le gestionnaire réseau d'un éventuel problème réseau ou système.

### ➤ **Utilisation de Big Brother : Réponse au cahier des charges.**

#### Utilisation des scripts existants

Dans chaque client, des scripts existent déjà et sont très utiles pour la supervision des éléments basiques comme la charge cpu, les processus ou services, la mémoire,... Voici donc une petite liste des scripts existants ainsi que les paramètres possibles à changer dans les fichiers correspondant .

- ✓ La charge CPU
- ✓ La capacité des disques
- ✓ Les fichiers de log
- ✓ Les processus en cours
- ✓ Autres services...

Il est également possible de tester les différents serveurs. En effet, grâce à Big Brother nous pouvons connaître l'état des services dns, ftp, nntp, smtp, pop3, http et avant tout la connexion réseau ( ping ). C'est le serveur BBNET qui effectue cette tâche.

Cependant, BB ne fournit pas tous les scripts répondant au cahier des charges, j'ai donc du en concevoir de nouveaux et les intégrer.

#### Création des scripts externes

Pour la création de scripts externes, j'ai dû lire et comprendre celui fournit en exemple par BB. Un script externe est composé du script et de son fichier de configuration, tous deux placés dans des répertoires spécifiques.

Le fichier de configuration spécifie les niveaux d'alertes et les paramètres du script alors que le script se charge de récupérer l'information, de la traiter et de la communiquer au client BB, qui la transmet au serveur BB.

Grâce à une recherche sur le langage Perl, j'ai découvert l'existence d'une librairie SNMP. J'ai ainsi pu réaliser une batterie de script source, en traduisant tous les commentaires pour permettre une mise en place plus aisée, et ou la personne n'a qu'à spécifier l'OID.

### Avertissement par mail d'une alerte

La machine envoyant les e-mails est la machine spécifiée dans bb-host.cfg par la clause BBPAGER. La configuration de cette fonctionnalité se fait grâce à 2 fichiers : bbwarnrules.cfg et bbwarnsetup.cfg. Les différentes options du service de notification se trouvent en annexe ( procédure d'installation du serveur Big Brother ).

Comme on vient de le voir, Big Brother permet de répondre à une bonne partie du cahier des charges mais d'un point de vue historique, on ne connaît que les différents états d'un couple ( machine, élément surveillé ). Il nous manque par exemple la charge du processeur en fonction du temps. C'est pour cette raison, que des logiciels de génération de graphiques ont été recherchés.

## 2 ) MRTG



### ➤ **Qu'est ce que MRTG ?**

MRTG, Multi Router Traffic Grapher, est un outil permettant la supervision d'un réseau. Il génère des pages HTML contenant des images au format PNG fournissant une représentation visuelle, en temps réel, du trafic, de l'espace disque, de la charge mémoire ...

MRTG peut superviser plus de cinquante systèmes différents sur un réseau et générer autant de pages. De plus il ne se limite pas au tracé des courbes puisqu'il utilise le protocole SNMP. Si le gestionnaire SNMP possède les OID ( *Object Identifier* ) et si les clients ont un agent SNMP et une MIB ( *Management Information Base* ), il devient possible d'obtenir de nombreuses informations en temps réel sur les entités du réseau : utilisation processeur, RAM disponible, espace disque utilisé... Il devient possible de visualiser des courbes journalières, hebdomadaires, mensuelles et annuelles.

### ➤ **Comment fonctionne MRTG ?**

L'installation de MRTG est nécessaire uniquement sur une machine, car il s'appuie sur le protocole SNMP, utilisant les réponses aux requêtes envoyées par le serveur sur lequel il est installé. Le serveur va donc, grâce au protocole SNMP, interroger la MIB du client pour

recueillir l'information correspondante à l'Object Identifier (OID) inscrit dans le fichier de configuration de MRTG.

Ce sont les extensions Perl, qui traduisent les réponses SNMP en coordonnées permettant la création des courbes.

Pour comprendre le fonctionnement de MRTG, il est nécessaire de savoir comment fonctionne le protocole SNMP, et de définir une MIB et un OID.

### Le protocole SNMP

Le protocole SNMP (Simple Network Management Protocol), défini en 1988 et approuvé en 1990 en tant que standard Internet par l'IAB (Internet Activities Board), permet de répondre aux besoins de mise au point d'une plate-forme de gestion de réseau efficace destinée à des réseaux hétérogènes TCP / IP.

SNMP est donc une norme de gestion de réseaux ; elle constitue une méthode de gestion de nœuds de réseau (serveurs, stations de travail, routeur, passerelle, switch) à partir d'une console de gestion de réseau.

SNMP décrit le langage que les agents et les consoles de gestion utilisent pour communiquer. C'est le protocole de type question / réponse asynchrone. Les consoles de gestion interrogent les agents pour observer leur fonctionnement et leur envoient des commandes pour leur faire exécuter certaines tâches. Les agents renvoient les informations requises aux consoles de gestion.

Certains événements du réseau peuvent déclencher des alarmes envoyées aux consoles de gestion. Cependant, l'envoi de message de façon spontanée de l'agent vers la console de gestion est vite limité. Les consoles de gestion interrogent donc périodiquement les agents de manière à vérifier leur état.

Lorsque l'agent exécute une opération, il stocke le résultat dans une base de donnée appelée MIB (Management Information Base) ; c'est celle-ci que la console interroge pour obtenir le résultat. La base de donnée MIB est en fait un conteneur d'objets représentant chacun un type particulier d'informations nécessaire au système de gestion. Un objet MIB peut par exemple, représenter le nombre de sessions actives sur un agent, tandis qu'un autre représente la quantité d'espace disponible sur son disque dur. Toutes ces informations qu'une console de gestion peut demander d'un agent sont stockées dans la MIB.

Un système SNMP supporte trois types de requêtes : GET, SET et TRAP.

- ✓ **GET** : message de requête SNMP de base.
- ✓ **SET** : message utilisé pour adresser et attribuer une mise à jour de valeur MIB à l'agent lorsque l'accès en écriture est autorisé
- ✓ **TRAP** : cette commande sert à la notification d'événements spontanés par un agent.

Les agents comme les consoles de gestion SNMP utilisent les messages SNMP pour inspecter et communiquer des informations concernant les objets gérés. Ces messages SNMP sont acheminés par le biais du protocole UDP (User Datagram Protocol). Le protocole IP achemine les messages entre la console de gestion et l'agent. Lorsqu'une console adresse une

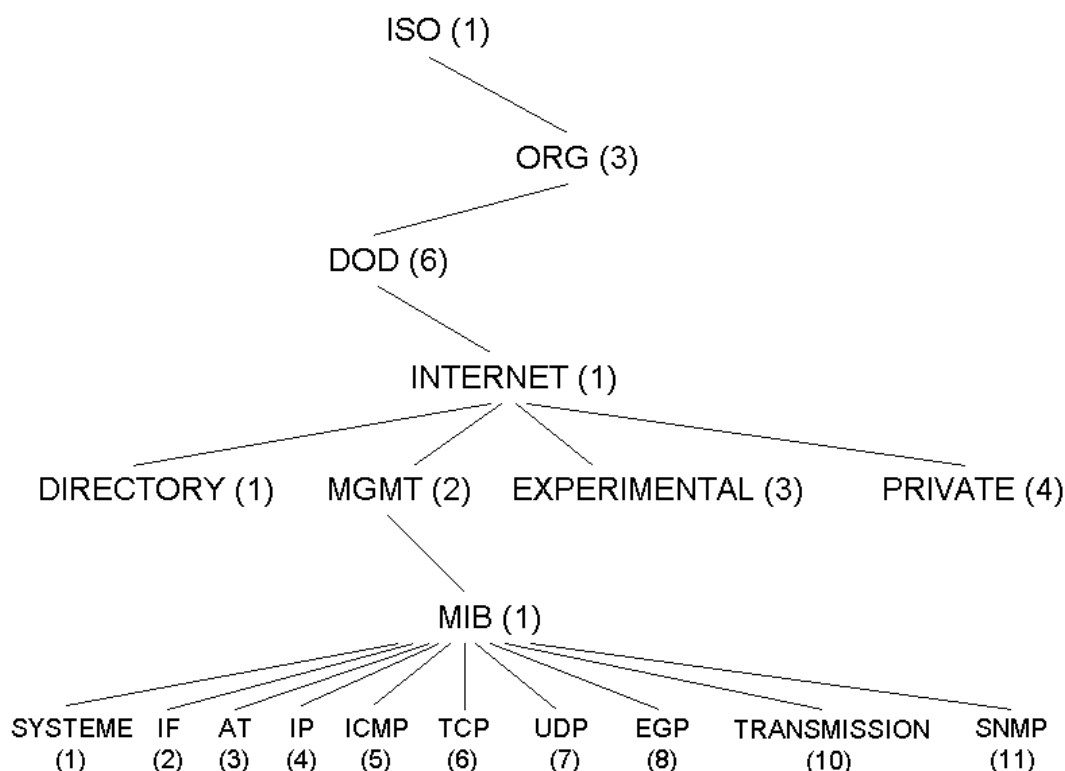
requête à un périphérique réseau, le programme agent de ce périphérique reçoit la requête et récupère l'information demandée dans la MIB, puis la renvoie à la console de gestion demandeuse.

Il est possible d'attribuer des groupes d'hôtes à des communautés SNMP à des fins d'administration et de contrôle de sécurité. Les communautés sont identifiées par le nom que l'administrateur leur attribue ; celui-ci est « public ».

### la MIB : Management Information Base

Une collection ordonnée d'informations pourrait être une définition succincte d'une MIB, mais nous allons voir que cela ne s'arrête pas là.

En fait, la MIB est une arborescence de données organisée selon un standard par l'ISO. Chaque objet de la MIB est identifié par une suite de nombres appelée OID qui indique une arborescence qui va de *ISO* à l'objet considéré en passant par *ORG* (Organisations), *DOD* (Department Of Defense), *INTERNET* et *MGMT* (Management) :



Les différents objets de la MIB II et leur OID correspondant ont été défini par l'ISO dans la RFC 1213.

Tous les OID de l'arborescence complète de la MIB II possèdent des « alias ». Par exemple, la requête `snmpget superviseurL.csi.fr csi.fr 1.3.6.1.2.1.1.5` signifie que SNMP ira rechercher l'information présente dans la MIB du serveur superviseurL.csi.fr dont la



communauté est *csi.fr* au niveau de l'OID *1.3.6.1.2.1.1.5* appelé *sysName* c'est-à-dire le nom de l'élément ici *SuperviseurL.csi.fr*

La MIB II constitue un standard pour le contrôle de réseau étant donné qu'elle est installée de façon quasi-systématique sur les systèmes. C'est en cela que l'on peut considérer MRTG comme un outil universel . Tout matériel muni d'une MIB et d'un agent SNMP peut être contrôlé via MRTG.

Grâce à MRTG, on a donc une information temporelle sur l'état d'un élément supervisé. Mais il m'a été demandé d'étudier un composant spécifique de MRTG, la génération des images avec un nouvel outil offrant beaucoup plus de fonctionnalités : RRD Tools.

### 3 ) RRD Tool



#### ➤ **Qu'est ce que RRD Tool ?**

Tout d'abord, RRD Tool signifie Round Robin Database Tool, outil de base de données fonctionnant avec un tourniquet. Le tourniquet est une technique qui utilise toujours le même nombre de données ( la taille de la base de données est constante ) et un pointeur vers la donnée courante.

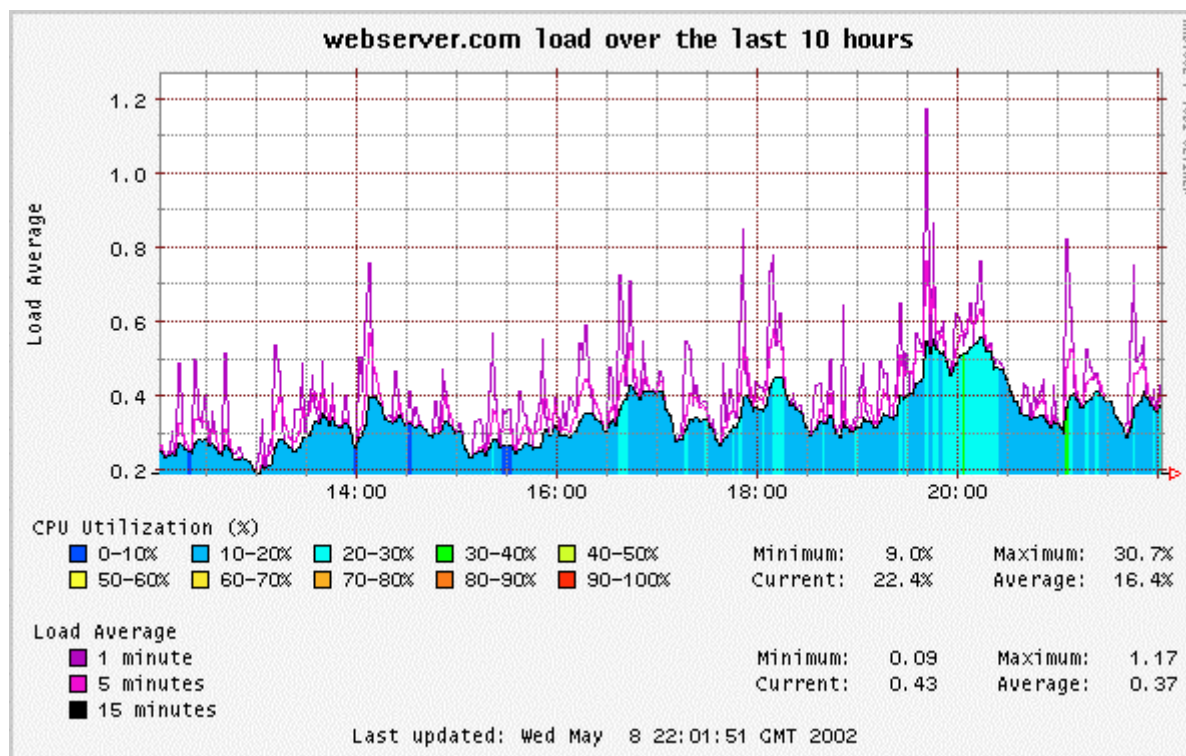
Pour illustrer cette notion, pensez à une montre à aiguille : les chiffres ou les traits symbolisent le lieu de stockage des données, et l'aiguille ( C'est une montre spéciale à une seule aiguille ;-)) ) symbolise le pointeur. Quand on a lu la donnée courante, l'aiguille tourne vers la donnée suivante. Comme on est sur un cercle, il n'y a pas de début ni de fin... Après un certain temps, l'aiguille aura fait un tour et tous les emplacements de stockage seront occupés. On va alors réutiliser ses espaces occupés. De cette façon, la base de données n'augmente pas en taille et ne requiert pas de maintenance. RRDTool fonctionne avec ce type de base : Il y enregistre et y récupère les données.

#### ➤ **Comment fonctionne RRD Tool ?**

A l'origine, RRD Tool fonctionne avec un exécutable que l'on utilise à la ligne de commande avec différentes options : *create* pour créer la base, *update* pour entrer des données, *graphe* pour générer les images, etc...

Il est donc possible, à l'aide du langage Perl et de sa librairie SNMP, de lancer des requêtes sur la MIB de n'importe quelle machine d'un réseau et ensuite de stocker la réponse dans la base. Enfin, un script peut mettre à jour l'image en requêtant la base.

A l'aide d'un langage spécifique à RRD Tool et de la représentation polonaise, on peut générer des graphiques avec des valeurs seuils, un nombre illimité de courbes, mettre en évidence des surfaces, etc....



### ➤ Qu'est-ce que la représentation polonaise ?

Il y a quelques années ( et peut-être encore actuellement ), la représentation polonaise était utilisée sur les caulettes Hewlett Packard. C'est une syntaxe de calcul qui nécessite de taper pour une addition entre 2 et 3: 2, 3, +. Cette syntaxe est basée sur un langage parlé : « Tu prends 2, tu prends 3 et tu me les ajoute ! ».

L'inconvénient de RRD Tool est d'utiliser cette représentation peu intuitive et donc peu usitée, pour tous ses calculs, les structures de conditions : ( T , 25 , GT, « Il fait chaud », « il fait froid », IF ). Si T ( la température) est plus grand que 25°C alors on retourne « Il fait chaud », sinon on retourne « Il fait froid ». On trouverait donc ce genre de code à l'intérieur de la fonction « exec » de Perl, ce qui fait 2 langages à maîtriser pour exploiter au mieux RRD Tool.

Suite à cet inconvénient majeur, il a été décidé de laisser tomber RRD Tool et de ne pas l'intégrer à notre solution de supervision, composée pour l'instant de Big Brother et MRTG. Durant mes recherches bibliographiques sur RRD Tools, j'ai eu l'occasion de trouver

des compléments à MRTG, lui apportant d'autres fonctionnalités et notamment l'envoi de mail avec Treshold.

#### 4 ) Treshold



##### ➤ **Qu'est-ce que Treshold ?**

Treshold est un ensemble de programmes en Perl qui s'ajoutent à MRTG. La version de MRTG doit être supérieure à la 2.7.4 pour permettre à Treshold de fonctionner.

Grâce à de nouvelles options reconnus par MRTG, ce dernier lance les programmes de Treshold. Celui-ci teste si la réponse numérique SNMP est supérieur ou inférieur à un seuil défini. Si la valeur dépasse le seuil, il regarde si l'unité de temps (minute, heure, etc....) spécifié à changer depuis la dernière exécution. Si c'est le cas, un mail est envoyé.

##### ➤ **Comment utilise-t-on Treshold ?**

Au niveau des fichiers .cfg de MRTG, il suffit de rajouter les seuils maximum et minimum de la réponse SNMP et 2 chemins d'accès aux fichiers « Treshunder.bat » et « Treshover.bat ». On est ensuite averti par mail d'un dépassement de seuil.

Comme les seuils sont spécifiés au niveau de chaque fichier de configuration, on peut donc indiquer des seuils de charge CPU différents pour chaque machine.

Treshold présente l'avantage d'être simple d'utilisation et fournit les mêmes fonctionnalités que Big Brother. Néanmoins, il est intégré à la solution pour une meilleure fiabilité dans la notification par mail.

## **Conclusion**

Les objectifs d'un stage en entreprise sont nombreux. Parmi eux, le stagiaire doit apporter à l'entreprise de nouvelles compétences liées à sa formation, mais il doit aussi acquérir de nouvelles connaissances liées aux activités de la société.

N'ayant pas eu de cours de réseaux, ces six semaines de stage furent très positives, me permettant à la fois d'acquérir des connaissances sur les réseaux informatiques, les protocoles comme SNMP, la supervision réseau, tout en mesurant ma capacité d'adaptation face à un sujet que je ne maîtrisais pas et sur un environnement d'étude ( windows2000 Server ) différent de celui employé en formation.

Ce stage fut une période d'échange très enrichissante : d'une part, CSI m'a permis de découvrir le monde des SSII, et d'autre part, j'ai eu l'occasion de réaliser un site web en PHP avec un employé de CSI qui ne connaissait pas du tout ce langage.

A l'issue du stage, je pense que mon objectif n'était pas de répondre au cahier des charges, mais de permettre à CSI de pouvoir proposer la mise en place d'une solution de supervision réseau, dans un délai minimum et avec des logiciels libres, ou le client peut spécifier les composants à contrôler parmi un large choix.

Au cours de mes différentes recherches bibliographiques, j'ai pu recenser différentes solutions aux problèmes de supervision. Ces solutions utilisant des technologies différentes : librairie SNMP de PHP, le logiciel NetSaint, etc...., il est donc possible de compléter la solution ou d'en proposer une 2<sup>ème</sup> suivant les exigences du client ( plate-forme, langage, etc.... ).

## **Bibliographie**

### Ouvrage :

- *Réseaux*, d'Andrew Tanenbaum traduit par Jean-Alain Hernandez et René Joly, Dunod, 1999, 3<sup>ème</sup> édition

### Sites Internet :

- Big Brother
  - <http://www.bb4.com>
  - <http://www.deadcat.net>
- MIB
  - <http://www.itu.int/ITU-T/asn1/>
  - [http://www.etsi.com/frameset/home.htm?/ptcc/ptccmib\\_structure1.htm](http://www.etsi.com/frameset/home.htm?/ptcc/ptccmib_structure1.htm)
  - <http://asn1.elibel.tm.fr/fr/index.htm>
- MRTG
  - <http://mrtg-fr.agarik.com>
  - <http://snmpboy.msft.net>
  - <http://www.cruzio.com/~jeffl/mrtg/docs/w95mrtg.htm>
  - <http://www.wtcs.org/snmp4tpc/>
  - <http://www.mrtg.org>
  - <http://www.linux-sottises.net/mrtg.php>
  - <http://xavier.dusart.free.fr>
- RRD Tool
  - <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>
- SNMP
  - <http://www.htr.ups-tlse.fr/pedagogie/cours/admin/protos/snmp/snmp41.htm>
  - <http://www.switch.ch/misc/leinen/snmp/perl/>
  - <http://cui.unige.ch/~pinfo97/public/reseau/pages/snmp.html>
  - <http://www.wtcs.org/snmp4tpc/testing.htm>
- SNMPHP
  - <http://nemesis.enix.org/~skaya/PROJTUT/projtut-snmphp.html>
- Treshold
  - <http://www.wtcs.org/snmp4tpc/treshol.htm>

**Annexes**

Annexe 1 : Le cahier des charges

Annexe 2 : Procédure « Installation du serveur Big Brother sous W2000 »

Annexe 3 : Procédure « Installation du client Big Brother sous W2000 »

Annexe 4 : Procédure « Installation du client Big Brother sous Linux »

Annexe 5 : Procédure « Installation du serveur Big Brother sous Linux »

Annexe 6 : Procédure « Installation de Treshold »

Annexe 7 : Procédure « Installation de RRD Tool sous W2000»

Annexe 8 : Procédure « Installation de SNMP sous Linux »