RAPPORT DE STAGE

Titre : **Métrologie des systèmes et réseaux de la ville de Rezé**

Tuteurs : Laurent MAUGER
(Chef du service systèmes, réseaux et télécommunications à Rezé)
Pierre BILAND
(Enseignant Réseaux et Télécommunications à l'IUT de Blois)

Stagiaire : Romain RUDIGER
(Etudiant DUT Réseaux et Télécommunication année 2005 à 2006)

Mots clés : Métrologie, Supervision, Monitoring, Network Management, Réseau, Surveillance, Mesure,performance, SNMP…

L'hôtel de ville de Rezé avec le Corbusier en arrière plan.

REMERCIEMENTS :

Je remercie tout le personnel du service de la Direction des Systèmes d'Information de m'avoir accueilli durant ces trois mois. En particulier Monsieur MAUGER qui malgré sont emploi du temps chargé a toujours trouvé du temps pour répondre à mes interrogations, me conseiller et ainsi enrichir mes connaissances techniques, du monde de l'entreprise et des collectivités locales.

Je remercie également Monsieur BILAND, enseignant de l'IUT, pour m'avoir rendu visite durant mon stage et pour ses conseils de rédaction de ce rapport.

Je tiens à remercier l'IUT de m'avoir offert cette formation qui a très bien répondu à mon attente : alliance de la théorie avec la pratique et assez de culture générale pour la poursuite de mes études.

DESCRIPTIF DU STAGE

Titre du rapport : Métrologie des systèmes et réseaux de la ville de Rezé

Auteur : RUDIGER Romain

Raison sociale de l'entreprise : commune de Rezé.

Adresse : Hôtel de ville – BP159
Code Postal : 44403
Ville : Rezé Cedex

Lieu du stage : Hôtel de ville

Nom et prénom du maître de stage : Laurent MAUGER

Domaine(s) d'activités abordés durant le stage :
☐ Type informatique (développement, installation logiciel, SGBD…)
☒ Type réseaux (installation, maintenance, sécurité, administration…)
☐ Type Internet (développement de site avec base de données …)
☐ Type téléphonie (centre d'appel, installation, autocommutateur…)
☐ Type commercial (vente + installation…)
☐ Type maintenance gros systèmes propriétaires (AS400, SNA…)
☐ Type opérateur radiocommunication (GSM …)
☐ Type maintenance et gestion de matériel réseau ou téléphonie de grande capacité
☐ Type prestation de services

Résumé :

Les réseaux et les systèmes informatiques de la Ville de Rezé sont en constante expansion. Ils sont devenus des éléments indispensables au fonctionnement de tous les services municipaux. Ce rapport traite la problématique de la supervision et de la métrologie des réseaux. La supervision doit permettre de détecter rapidement les incidents pouvant apparaître sur les réseaux et ainsi les traiter efficacement. La métrologie doit fournir à la Direction des Systèmes d'Informations des indicateurs lui permettant d'anticiper les évolutions techniques et les budgets et de confirmer la performance du système d'information.

Visa du Président du Jury de soutenance :

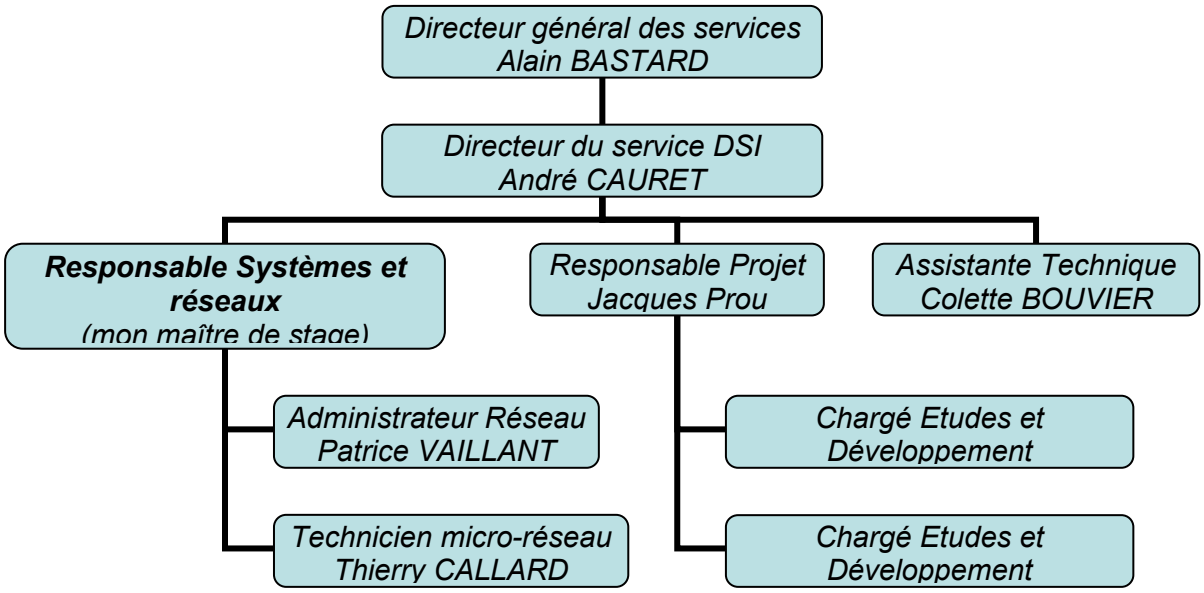
Nom : ..... Prénom : ..... Date : .....

TABLE DES MATIERES

1. Introduction

Mon stage s'est déroulé à l'hôtel de ville de Rezé où travaillent plus de 750 agents municipaux permanents au service d'une ville de plus de 40 000 habitants. La direction des Systèmes d'information m'a accueilli pour effectuer mon stage de trois mois dans de très bonnes conditions puisqu'elle a mis à ma disposition un bureau avec un bon ordinateur et ses membres étaient toujours prêts à prendre du temps pour répondre à mes questions. Cette direction est composée de deux services, le premier assure la gestion et le déploiement des matériels et logiciels, l'administration des ressources, la maintenance des équipements et l'assistance aux utilisateurs. Le second mène l'étude et la mise en œuvre des projets applicatifs, et assure la maintenance des applications et l'assistance aux utilisateurs.

Voici l'organigramme de la Direction des Systèmes d'Information (DSI) :



Ces cinq dernières années le réseau de la ville s'est beaucoup développé : passage de 5 à 35 serveurs, création de liens entre les différentes structures publiques qui étaient auparavant isolées... Les systèmes d'information ainsi mis en place sont maintenant des éléments stratégiques pour l'ensemble des services municipaux qui seraient paralysés si un disfonctionnement survenait. Le réseau informatique s'étant complexifié, il est devenu nécessaire d'avoir une solution de supervision et de métrologie complète permettant de maintenir une bonne qualité de service, de mieux dimensionner le réseau et ses services mais aussi de prévenir d'éventuelles défaillances. La solution en place n'étant pas assez complète, le service réseau avait depuis un certain temps le projet de la remplacer, c'est ce qui m'a été confié.

Dans un premier temps il m'a fallu découvrir le réseau de la ville pour comprendre son fonctionnement physique et logique avant de chercher à comprendre pourquoi il est nécessaire de surveiller un réseau. Dans une seconde partie j'ai défini les besoins du service systèmes et réseaux. Pour finir j'ai mis en place une solution répondant aux besoins mais cela n'était pas le principal but du stage.

Au moment de mon stage, mon service a été impliqué dans plusieurs petits projets, j'ai suivi certains de ces projets que je détaille à la fin de ce rapport.

2. Découverte de l'infrastructure

2.1. Petit historique des réseaux

Un réseau informatique permet la communication entre des équipements informatiques pour échanger des informations. Un réseau permettant de faire transiter de plus en plus de données : le débit des réseaux locaux (LAN) est passé de 2 Mb/s en 1975 à 1 Gb/s en 2004 et cela sur de plus en plus de supports : filaire, hertzien, infrarouge, satellite… Il est de plus en plus difficile de savoir comment il est utilisé, par qui et si personne ne l'utilise à votre insu !

2.2. Le réseau de la ville de Rezé

Le réseau en place est récent, il date de 2001 lors d'une restructuration, il y avait pas moins de 9 systèmes d'exploitation utilisés : Unix, Linux, Novell (4.11 et 5.0), Windows 95, 98, NT4, 2000 professionnel et serveur. Cette diversité était ingérable pour 2 techniciens, il a donc été décidé à l'occasion du déménagement du service dans de nouveaux locaux d'homogénéiser aussi bien les protocoles que les systèmes d'exploitation.

2.2.1. La topologie du réseau

Pour comprendre plus rapidement la topologie, les services offerts mais aussi les types d'équipements actifs constituant ce réseau, j'ai décidé de faire un schéma représentant le cœur du réseau, les principales interconnexions, les serveurs et les sites distants reliés en fibre optique (voir le schéma en dernière page).

Les différents services de la ville sont répartis dans plusieurs bâtiments plus ou moins éloignés du cœur de réseau situé à l'hôtel de ville, le lieu de mon stage. Les services devant communiquer ensemble et par souci de centralisation des serveurs, chaque bâtiments est relié au cœur par une liaison ADSL, spécialisée ou par fibre optique pour les sites proches du tramway où le réseau métropolitain (MAN) de Nantes métropole passe (c'est le réseau O-MEGA).

Toutes les liaisons ADSL sont fournies par Mégalis qui n'a pas pour but de faire du chiffre d'affaire mais de mettre à disposition des services à un prix très attractif à toutes les collectivités et associations qui le désirent. Il fournit aux écoles, centres sociaux, cantines, centres culturels (théâtre, école de musique…), crèches…un accès ADSL avec une IP fixe à une vitesse de 512 bits/s en montant et 128 bits/s en descendant. Le débit suffit puisque ces sites utilisent la liaison pour relever leurs courriels, consulter l'intranet et bien entendu surfer sur toile. Les liaisons sont sécurisées par un tunnel VPN entre les routeurs sur le site et le pare-feu du cœur de réseau.

Les services de la mairie elle-même sont reliés par des fibres optiques du réseau O-MEGA et un par une liaison spécialisée France Télécom à 2 Mbits/s, les fibres sont activées à 100 Mbit/s. La mairie dispose de deux liaisons extérieures, une SDSL de Mégalis à 2 Mbit/s pour tous les liens VPN, et la communication vers internet, l'autre est une fibre optique à 100 Mbits/s sur le réseau O-MEGA. Ces deux liaisons arrivent sur le pare-feu (un PIX de Cisco) ce pare-feu est chargé de mettre en place les tunnels VPN, de filtrer les connexions venant d'internet mais aussi l'accès à internet des postes informatiques de l'hôtel de ville qui par défaut ne peuvent utiliser que le protocole http. Pour la communication interne de l'hôtel de ville, les bâtiments sont interconnectés par fibres optiques.

Le service Systèmes et réseaux gère un parc constitué de plus de 550 Micro-ordinateurs dont 450 connectés, d'une centaine d'imprimantes réseau et de 36 serveurs fournissant 12 services réseau et plus d'une centaine d'applications métiers.

2.2.2. La sécurité

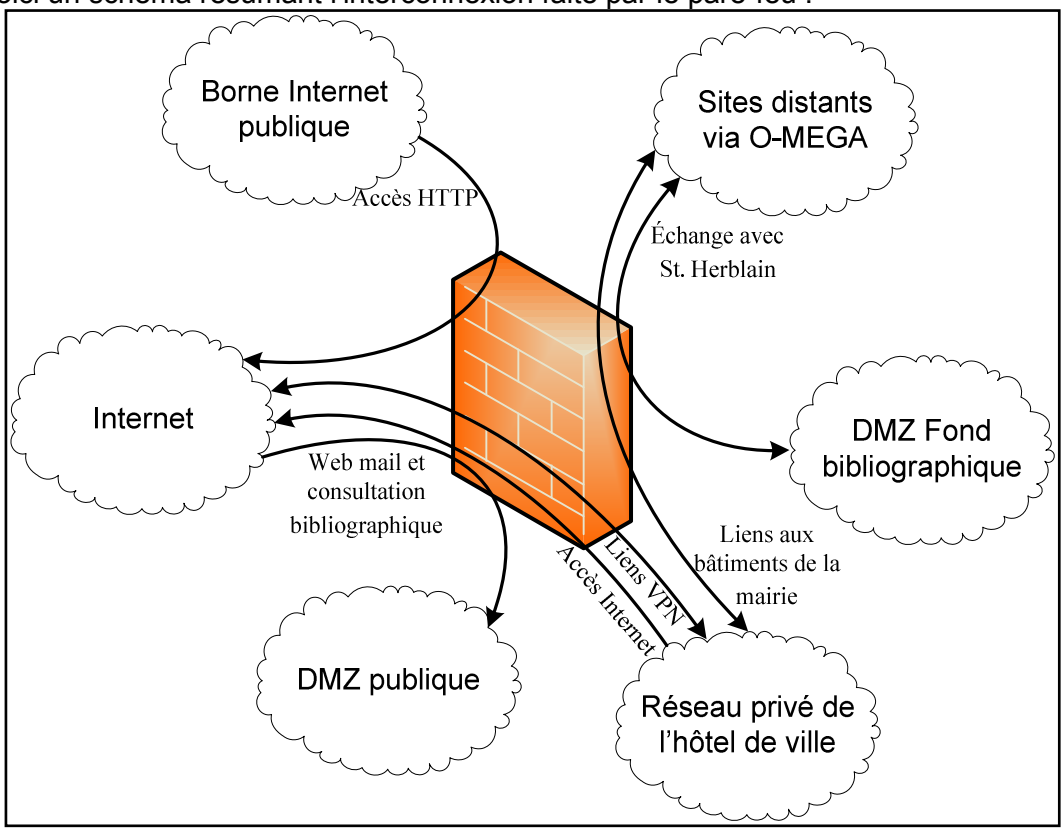
2.2.2.1. Logique

L'élément principal mettant en place la notion de sécurité au niveau logique est le firewall qui sépare :

- Une zone démilitarisée (DMZ) hébergeant le web mail et la consultation du fond bibliographique de la médiathèque accessible au publique.
- Une autre zone démilitarisée concerne l'accès à un serveur hébergeant un service de fond bibliographique pour la mise en commun du fond de la ville et celle de St. Herblain.
- Les sites distants reliés via le réseau O-MEGA.
- L'internet et donc les sites reliés par ADSL par Mégalis.
- Une borne internet publique qui n'a donc accès qu'a internet en http.
- Le réseau de l'hôtel de ville comprenant tous les serveurs et postes de travail, une plateforme antivirus analyse tout ce traffic.

Les serveurs ne faisant pas partie des deux DMZ ne sont pas vulnérables de l'extérieur. Il n'en est pas de même en interne puisque rien ne les cloisonne des postes de travail. Les serveurs sont protégés eux même par un pare-feu logiciel et système d'authentification.

Voici un schéma résumant l'interconnexion faite par le pare-feu :



2.2.2.2. Physique

Il est très difficile de protéger une machine lorsqu'elle est physiquement accessible, il faut aussi penser que certaines informations sont sensibles et strictement privées (Action sociale, Santé, réglementation…). Une alarme a été installée il y a 2 ans, elle protège le cœur du réseau ainsi que tous les serveurs, un système de sécurité électrique par onduleur est aussi en place mais celui-ci est maintenant sous dimensionné et n'est pas capable de fonctionner assez longtemps pour que les serveurs s'arrêtent proprement.

2.2.2.3. Sauvegarde

L'utilisation de l'informatique étant devenue omniprésente quelque soit le service de la mairie, un système de sauvegarde efficace est nécessaire. Tous les utilisateurs travaillent en réseau, c'est-à-dire que tous les paramètres, courriels et leurs fichiers sont stockés sur les serveurs, il en est de même pour les applications métiers. Il est donc primordial de sauvegarder l'ensemble de ces données et d'être capable en cas de défaillance d'un serveur ou d'un sinistre de tout restaurer.

Deux composants sont utilisés :

- 1 serveur NAS (Network Access Server) : de 6 To sur un site distant relié directement par fibre optique pour les sauvegardes journalières, hebdomadaires et mensuelles.
- Une librairie de sauvegarde sur bande d'une capacité de 14 bandes de 200 Go natives et jusqu'à 400 Go compressé.

Une sauvegarde différentielle (seul les nouveaux fichiers ou les fichiers modifiés par rapport à la dernière sauvegarde complète sont sauvegardés) est faite tous les soirs en dehors des heures de production, de tous les serveurs (messagerie électronique (message par message pour pouvoir restaurer uniquement la boite d'un utilisateur), documents des utilisateurs, données et applications métiers…) sur bande et sur le serveur NAS.

Une sauvegarde complète des ces serveurs est faite le samedi.

Une sauvegarde mensuelle sur bande (sauvegarde conservée 12 mois) et sur la NAS (avec deux mois d'historique).

Les bandes sont stockées chaque jour dans une armoire ignifugée et blindée dans un autre bâtiment.

2.2.3. Le fonctionnement de l'assistance technique

Le service dans lequel je suis a aussi bien à sa charge la mise en place du matériel, le déploiement des logiciels… que la maintenance, la gestion des pannes et des problèmes rencontrés par les utilisateurs. Il est intéressant d'étudier comment le service s'organise pour répondre le plus efficacement possible à cette problématique.

Il est actuellement difficile de faire de la prévention, les majeures parties des pannes sont détectées par les utilisateurs.

Lorsque l'utilisateur a un problème, il appel directement l'assistante technique dite « de premier niveau », elle crée alors une fiche (dans une base de donnée Microsoft Access) comprenant :

- L'utilisateur ayant le problème
- Le service auquel l'utilisateur est rattaché
- Le problème ou la demande (nouveau poste téléphonique, vidéo projecteur…)
- Le type d'incident (permettant de faire des statistiques et de trier les demandes)
- Et le suivi de cette demande (par exemple réparé le 26/06/06)

Si l'assistante technique de premier niveau n'arrive pas à résoudre le problème, la fiche est transmise au niveau suivant, c'est-à-dire les techniciens puis aux ingénieurs et cela selon le service concerné : soit projet, soit réseau.

La demande est ensuite traitée puis archivée.

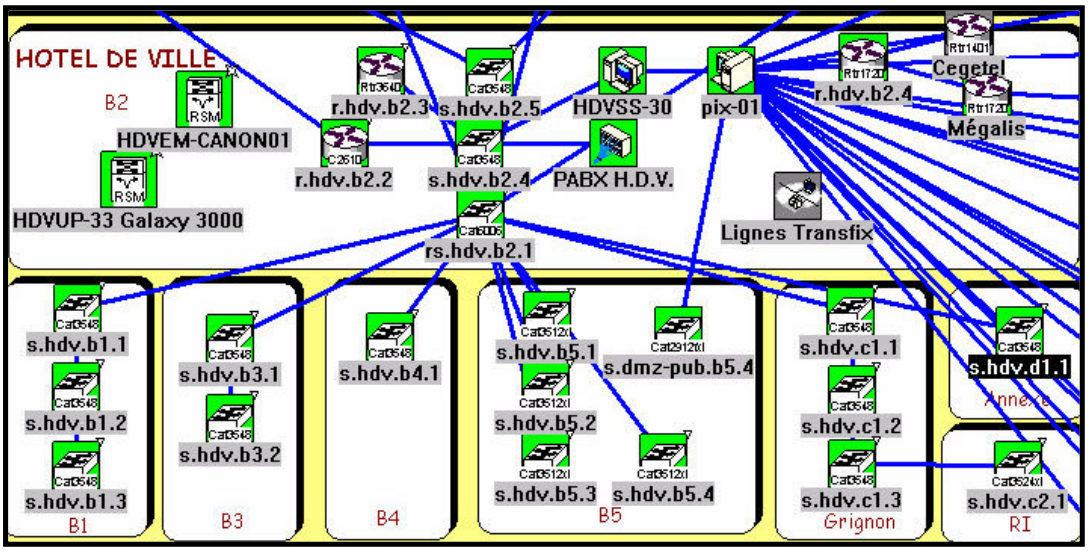
Cette gestion en niveau permet d'utiliser au mieux les compétences des agents. Quand une même demande revient souvent, une fiche de procédure est créée permettant de gagner du temps pour les futures demandes.

Lors d'une demande importante engendrant des frais aux services, cette demande est traitée pour être incluse ou non dans la demande budgétaire du service informatique qui a lieu tous les ans. Cette demande est prise en compte si elle parait nécessaire ou était déjà prévue, mais elle peut aussi être refusée pour différente raisons (renouvellement d'un ordinateur alors que celui date de l'année précédente, mise à jour d'un logiciel alors que celle-ci ne semble pas nécessaire par le service projet…).

2.2.4. La solution de gestion existante

La solution de supervision actuellement en place est le logiciel Whatsup Gold de l'éditeur Ipswitch, installé il y a cinq ans lors de la restructuration, il se présente sous la forme de cartes où apparaissent les éléments du réseau qui auront été préalablement ajoutés manuellement. Pour ajouter un élément, il faut choisir le type d'élément, lui attribuer une adresse IP et définir les services à surveiller. Il est aussi possible de définir les éléments accessibles par le menu contextuel et le type de notification en cas de défaillance : courriel, message système, pop-up…

Pour finir le logiciel publie ce schéma sous forme de pages Web pour une prise de connaissance à distance de l'état des équipements, voici un extrait d'une des pages :



Actuellement cette solution n'est plus suffisante compte tenu de la taille du réseau mais aussi de l'absence d'historique des défaillances, de surveillance de nouveaux services et d'un système de métrologie.

3. La gestion du Système d'information

Au vu de l'augmentation significative de la taille des réseaux, l'ISO (International Standard Organisation) a proposé dans les années 80 deux normes pour définir une architecture d'un protocole d'administration. Voyons le concept qui est défini sur 5 axes:

- The fault management : c'est la gestion des anomalies pour obtenir une qualité de service optimale en étant capable de localiser très rapidement une anomalie.
- The configuration management : la gestion de la configuration des équipements constituants le réseau a pour but de mettre en place un système d'identification unique de chaque équipement, compteur…
- The performance management : la gestion des performances implique d'être en mesure de pouvoir contrôler le trafic du réseau pour savoir s'il est bien dimensionné.
- The security management : aspect sécurité en contrôlant l'accès au réseau mais aussi l'intégrité, l'authentification et la confidentialité des données qui transitent.
- The accounting management : pouvoir gérer la consommation du réseau par un utilisateur en vue d'établir une facture.

Mon projet n'est pas de trouver une solution remplissant ces 5 caractéristiques, mais au moins ces deux points : the performance, the fault management.

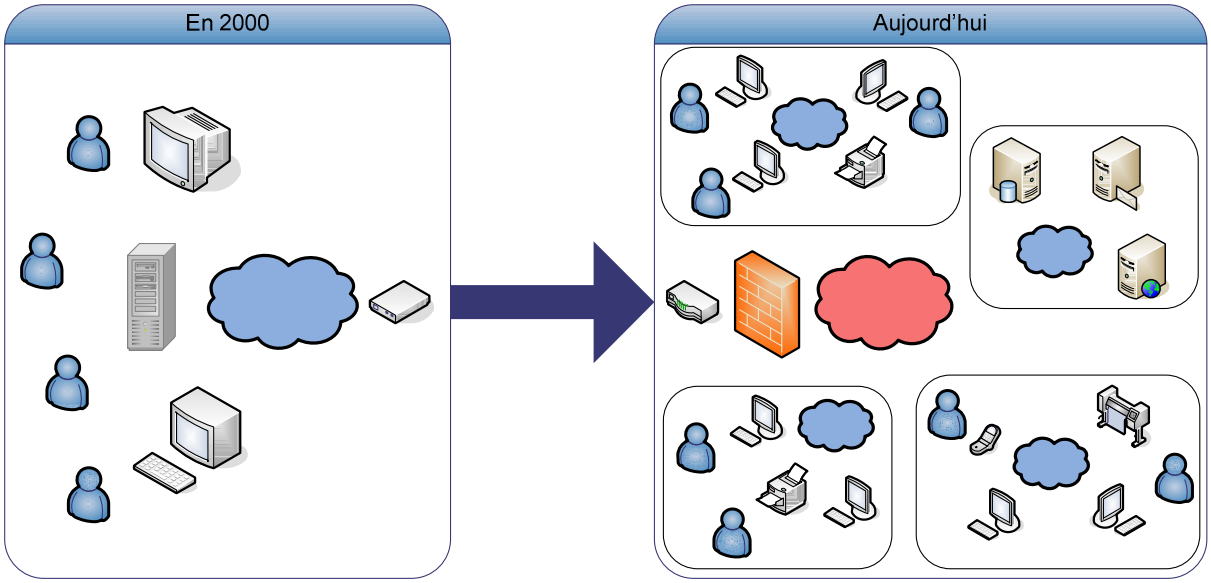
Voici plus en détails les 2 axes abordés dans ce sujet :

- L'audit de performance (The performance management) permet d'évaluer la performance du Système d'information. Il faut donc collecter des informations, stocker ces informations dans une base de données puis les analyser sous une forme facilement exploitable (un graphique par exemple).
- La gestion des pannes (The fault management) : une panne est la conséquence d'un problème interne ou externe, il faut la détecter le plus rapidement possible.
  - Les problèmes internes sont souvent dus à un élément en panne.
  - Les problèmes externes sont eux difficilement détectables.

  Le traitement d'une panne se fait en quatre étapes :
  - ✓ Détection,
  - ✓ Localisation,
  - ✓ Réparation,
  - ✓ Confirmation du retour au bon fonctionnement.

Seul le premier correspond à une solution de métrologie, le second est du ressort d'une solution de supervision. Sans rentrer tout de suite dans les détails, il n'est pas souhaitable que ces deux solutions soient séparées. Les solutions de « network management » actuelles font au moins de la supervision et de la métrologie car les deux se complètent, par exemple : on doit pouvoir tester le bon fonctionnement d'un service fourni par un serveur (supervision) mais aussi savoir combien d'utilisateurs utilisent ce service (métrologie). Il est alors nécessaire de comprendre l'utilité de chacun avant de vouloir déterminer les fonctionnalités que devra posséder la future solution.

Le Système d'information de la ville s'est de plus en plus développé, il offre maintenant de nombreuse fonctionnalités et services ce qui a entraîné l'augmentation du nombre de serveurs, d'équipements et d'applications :



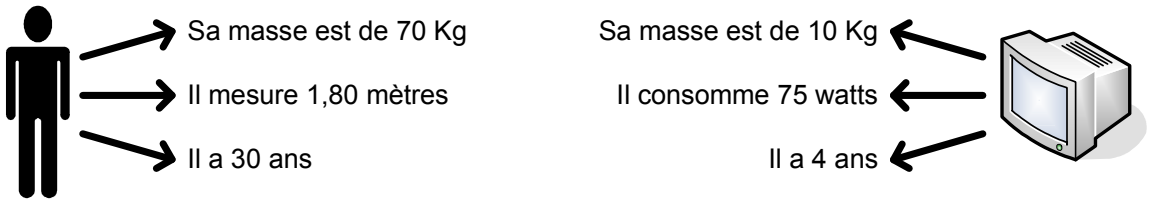
Ce développement du Système d'informations complexifie la gestion de l'infrastructure puisqu'il est devenu difficile d'avoir une vision globale de celle-ci. Il est donc difficile de déterminer la cause d'un dysfonctionnement ou d'une perturbation sans outils dédiés.

La mise en place d'une solution de gestion permettant une vision globale de la performance et l'état de l'infrastructure est devenue indispensable pour le service des systèmes et réseaux de la ville.

3.1. La métrologie

3.1.1. Définition générale

D'après l'encyclopédie libre Wikipédia : La mesure est l'opération qui consiste à donner une valeur numérique à une grandeur. Par exemple, la mesure des dimensions d'un objet va donner les valeurs chiffrées de sa longueur, sa largeur...
La notion de mesure est omniprésente :



3.1.2. Dans le domaine des télécommunications

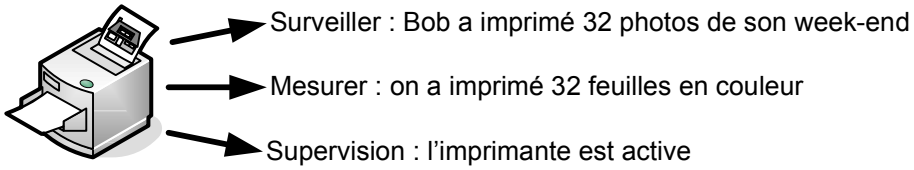
Dans mon cas, c'est bien sûr la métrologie appliquée aux réseaux informatiques voir téléphoniques. La métrologie revient à faire des relevés de valeurs comme relever la bande passante utilisée sur un lien, la répartition des protocoles et des services… Il doit être aussi possible de relever des informations précises sur un équipement constituant le réseau comme la charge du processeur, de la mémoire…

En résumé un système de métrologie efficace permet :

- de détecter d'éventuels engorgements du réseau, des trafics suspects, une machine piratée…
- de pouvoir redimensionner des liens sous dimensionnés ou surdimensionnés
- de détecter un besoin de redémarrage de certains équipements ou d'augmenter leur mémoire.

Attention la métrologie consiste à ne remonter que des informations quantitatives comme le nombre d'utilisateurs connecté sur un serveur Web et non pas quelle page Web Bob regarde ! Il va donc être nécessaire de définir de manière précise ce que l'on va mesurer.

Exemple



3.2. La supervision

3.2.1. Qu'est ce que cela veut dire ?

Le terme superviser désigne l'action de regarder au dessus de l'information, contrairement à celui de surveiller qui signifie veiller sur. En clair la supervision consiste à vérifier le bon fonctionnement d'un service, d'un lien, d'une application…

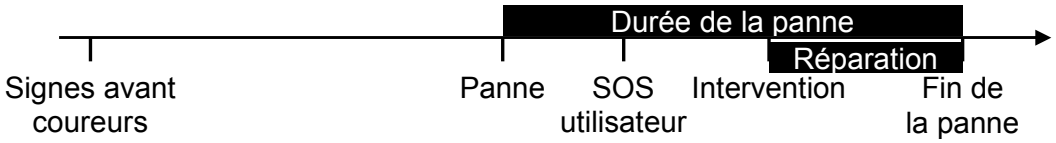
3.2.2. Pourquoi ?

Si le réseau ne possède pas de système de supervision :

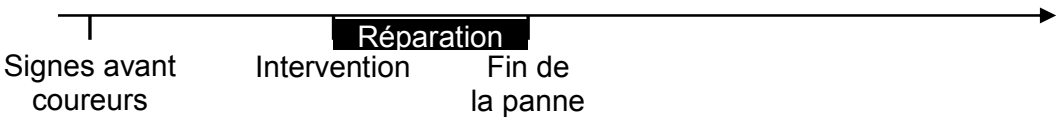
- Il peut être piraté sans que les administrateurs s'en rendent compte (détection d'un nouveau service).
- Lors d'une panne, ce sont les utilisateurs qui informent les administrateurs.

Donc pour que les administrateurs soient crédibles et aient une bonne image, il faut un système de supervision efficace, complet et adapté. En outre un bon système de supervision permet d'anticiper les pannes et donc de gagner du temps :

- Sans supervision :



- Avec supervision :



3.2.3. Maintenance préventive

On vient de le voir, la supervision permet de prévenir d'éventuelles défaillances et donc de pouvoir préparer des opérations de maintenance. Cependant la maintenance préventive peut être très vite considérée comme du gaspillage et comme inutile puisqu'il n'y a pas encore eu de panne ! C'est pour cela que l'opération de maintenance doit être organisée pour ne pas perturber l'usager et mesurer les coûts de cette éventuelle opération.

- Trop de maintenance préventive = gaspillage = peu de panne
- Pas de maintenance préventive = trop de panne = mauvaise image vis-à-vis du public

Il faut donc trouver le juste milieu.

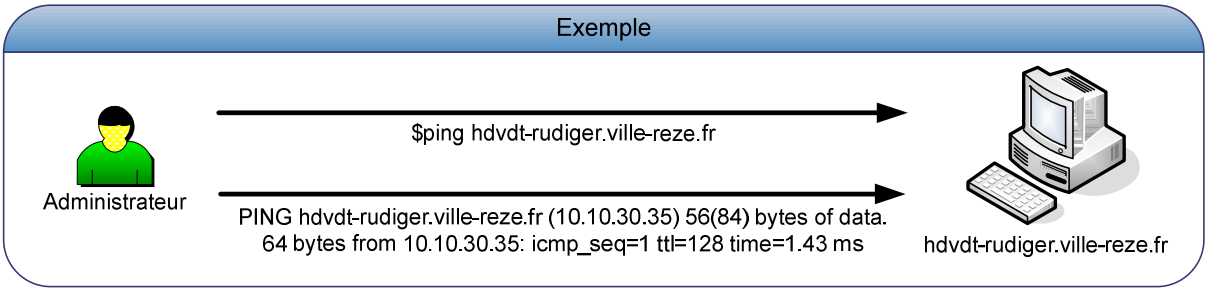
3.3. Les méthodes

Beaucoup de méthodes sont à notre disposition pour superviser un réseau, ces différentes méthodes peuvent être regroupées en deux grandes catégories :

3.3.1. Les méthodes actives

Cette méthode consiste à exécuter un logiciel afin de relever une caractéristique précise à un moment précis et non pas une observation globale du réseau. Connexion (exécution d'une commande par SSH), Ping et Traceroute sur un équipement font partie de cette méthode. C'est donc soit l'utilisation du protocole ICMP soit l'envoi de commandes par SSH pour faire des relevés de l'état du système.

Exemple de l'utilisation de l'application ping, se basant sur le protocole ICMP, par un administrateur voulant tester si ma machine est active :

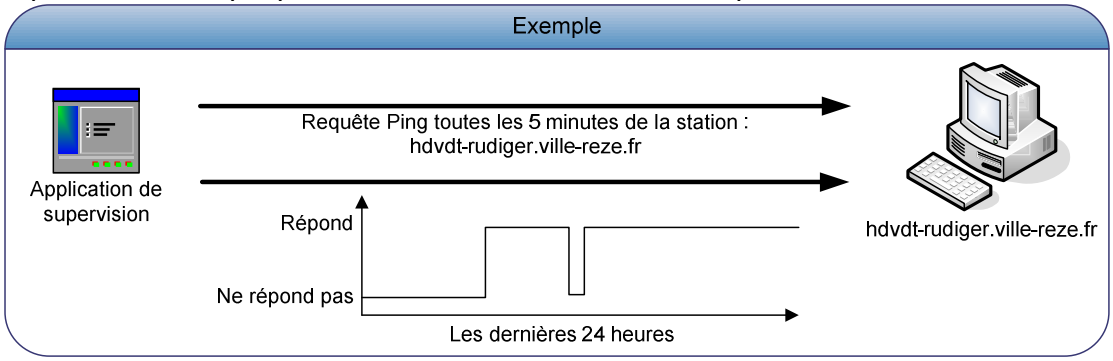


Ce qu'il faut retenir : une méthode active permet de tester à un instant t quelque chose mais ne permet pas de connaitre le résultat de ce test il y a deux heures.

3.3.2. Les méthodes passives

Ces méthodes ne consistent plus à lancer un logiciel de façon ponctuel pour connaître l'état d'un équipement, mais de le mettre en tant que service système pour qu'il puisse fonctionner en continu. L'administrateur peut ainsi accéder aux relevés par le biais d'une interface graphique ouverte en permanence ou par une interface web. Grâce à cette méthode, on peut mettre en place un système de graphique (flux, temps de réponse, occupation de la mémoire…) permettant de mieux voir l'évolution d'un paramètre. La surveillance du réseau se fait en continue, elle met en œuvre des sondes, utilise un protocole de management (SNMP) ou utilise des agents à placer sur les équipements.

Reprenons l'exemple précédent mais avec une méthode passive :



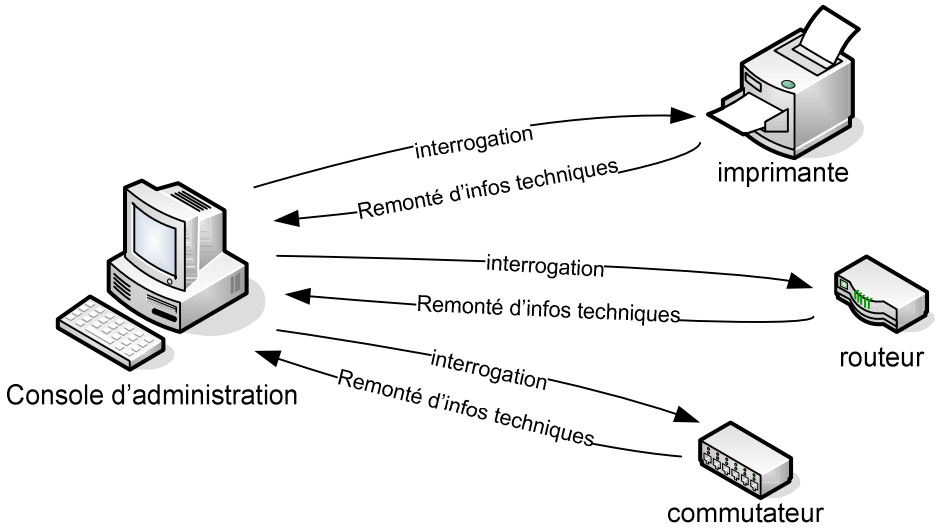
Ce qu'il faut retenir : la supervision passive permet de revenir dans le temps pour mieux comprendre un phénomène de pannes en cascades (services qui « tombent » les un après les autres) par exemple. Mais cette méthode nous oblige à laisser fonctionner constamment une application qui génère une utilisation du réseau et des équipements qu'il ne faut pas négliger surtout pour un grand réseau.

4. Les outils disponibles

4.1. Le protocole SNMP et sa MIB

4.1.1. A quoi ça sert ?

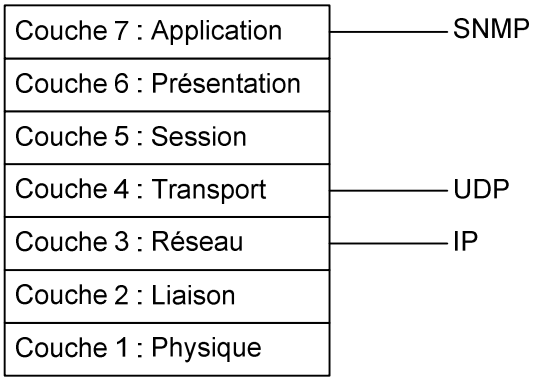
Imaginez un moyen qui permettrait d'administrer tous les équipements d'un réseau et de connaître les informations internes d'un switch, d'une imprimante, d'un routeur, d'un serveur…



Plusieurs moyens existent, l'un d'eux est le protocole SNMP, sa première version a été normalisée en 1988 par l'IETF (RFC 1157). SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau), les équipements supportant ce protocole sont cher mais la quasi-totalité des équipements administrables (par telnet, interface web ou encore par le port console) le supporte. Si ce n'est pas le cas il est possible de pouvoir installer un agent SNMP sur un système d'exploitation mais pas sur un équipement fermé que l'on ne peut mettre à jour, comme un simple commutateur non administrable. Avec ce protocole on peut par exemple sur un équipement :

- Connaître son état : nombre de trames passées, charge du processeur…
- Configurer certains paramètres (on peut ainsi imaginer un système d'équilibrage des charges)
- Etre alerté par l'équipement d'un disfonctionnement interne (surchauffe, permet d'alimentation…)

Bâti au dessus de TCP/IP, voici SNMP dans le modèle OSI :



SNMP utilise le protocole UDP pour sa simplicité et son poids : 8 octets (20 octets pour TCP). Ce protocole permet à SNMP d'être rapide mais ça a l'inconvénient d'être un protocole en mode non connecté et non fiable, il est donc possible qu'un message SNMP n'arrive jamais, ce qui est embêtant si c'est une alarme…

4.1.2. Le protocole

L'utilité d'avoir un protocole standardisé pour administrer un réseau :

- Les règles d'interrogations ne change pas d'un routeur CISCO à un routeur 3COM.
- Il est utilisable sur des plates formes hétérogènes (Linux, IOS, Windows…)
- Les éléments rapportés ne ralentissent pas le réseau.
- Le temps de réponse est très court.

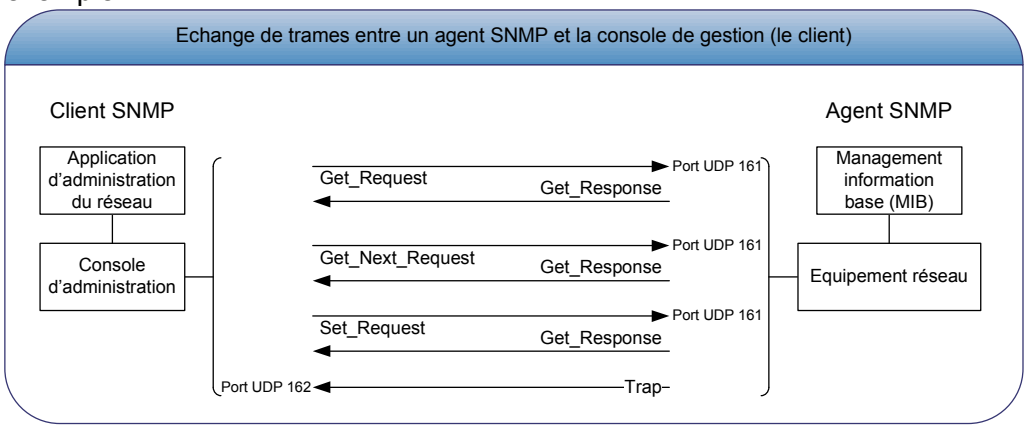
3 versions du protocole SNMP existent, la première en 1990 suivie de la version 2 dite classique (V2c) en 1993, cette version a évolué jusqu'en 2002. La troisième version développa l'aspect sécurité.

La version 1 comprend 5 commandes :

- Get_Request : demande l'envoi de la ou les valeurs d'un objet.
- Get_Next_Request : demande l'envoi de la valeur de l'objet suivant.
- Set_Request : modification de la valeur d'un objet.
- Get_Response : permet de récupérer la réponse obtenue par l'une des trois dernières commandes.
- Trap : permet à l'équipement d'envoyer une alerte au système d'administration du réseau en cas de défaillance d'un lien par exemple.

Dans la version 2, deux nouvelles commandes sont ajoutées :

- Inform request : permet une communication entre les systèmes d'administrations.
- Get_Bulk_Request : requête de plusieurs get_next successifs pour lire une table par exemple.



4.1.3. La M.I.B.

La Management Information Base, qui peut se traduire par : la base d'information de gestion, elle est spécifique à chaque équipement mais aussi à chaque constructeur car c'est lui qui définie les informations consultables, les paramètres modifiables et les alertes à envoyer (Les traps). La MIB est une structure arborescente où chaque feuille correspond à une information sur l'équipement. La MIB permet donc de définir les données à envoyer dans la trame d'interrogation pour récupérer les données voulues. Le nom de chaque nœud est normalisé mais un équipement compatible SNMP n'est exploitable qu'avec sa MIB car il est impossible de deviner les objets disponibles dans chacune des branches et comprendre leurs significations ainsi que leurs valeurs.

4.1.4. La S.M.I.

La Structure of Management Information définie les règles de description et d'identification pour chaque objet de la MIB. Un objet est défini en langage ASN.1 (langage de représentation des données (Abstract Syntax Notation 1) défini par l'ISO 8824), voici quelques types utilisés :

- IPAddress : pour l'adresse IP.
- PhysAddress : pour l'adresse matérielle (MAC).
- TimeTicks : pour un compteur de temps en 1/100 de seconde.
- OCTET STRING : pour une chaîne de caractères.

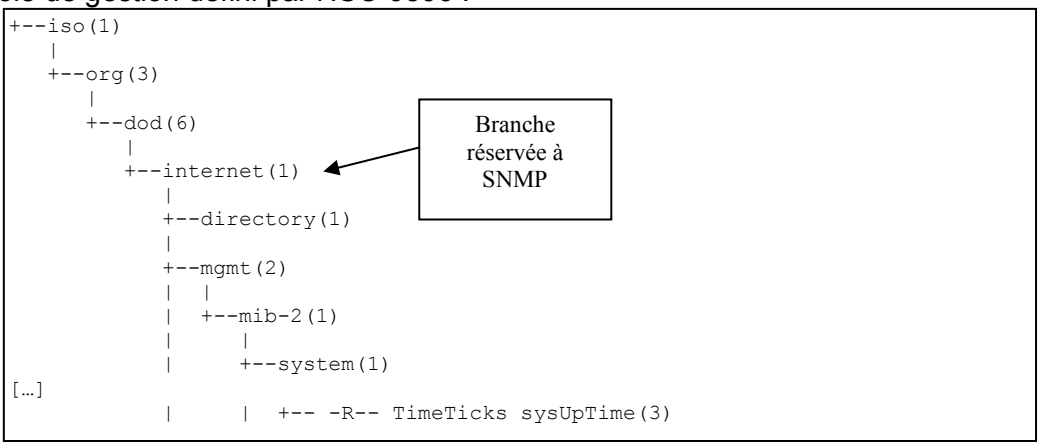
4.1.5. Fonctionnement

Pour mieux comprendre le fonctionnement j'ai voulu savoir comment récupérer l'uptime (temps écoulé depuis le démarrage du système d'explotation) d'un routeur faisant le lien entre l'hôtel de ville et un site distant par un lien loué à France Télécom. Dans un premier temps il a fallu aller chercher sur le site du constructeur (ici Cisco) le MIB de ce routeur pour savoir où se situe cette donnée.

Voici un extrait, plus particulièrement une feuille, de la MIB d'un équipement Cisco :

```
system   OBJECT IDENTIFIER ::= { mib-2 1 }
[…]
sysUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time (in hundredths of a second) since the network
            management portion of the system was last re-initialized."
    ::= { system 3 }
[…]
```

Chaque branche est repérée par un numéro, SNMP utilise cette façon de faire pour accéder à un paramètre : de la racine jusqu'au paramètre d'un objet. Dans l'encadré ci-dessous on voit que la branche system(1) fait partie de la branche mib-2(1) qui fait à son tour partie d'une autre branche… C'est l'espace de nommage qui reprend une grande partie du protocole de gestion défini par l'ISO 9596 :



Donc pour accéder au paramètre de la feuille étudiée, il faut passer par les nœuds .1.3.6.1.2.1.1.3 (c'est l'OID de l'objet : Object Identifier) et rajouter 0 pour obtenir la valeur de l'objet 'sysUpTime'.

Essai avec le chemin complet grâce à l'outil snmpget :

```
# snmpget -v 2c -c public 10.10.100.1 .1.3.6.1.2.1.1.3.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (3683053517) 426 days, 6:42:15.17
```

Comme la suite des nœuds .1.3.6.1.2.1 est très souvent utilisée, il est possible d'utiliser un chemin relatif en omettant le point de début, on obtient donc la suite : 1.3.0, cela donne :

```
# snmpget -v 2c -c public 10.10.100.1 1.3.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (3683342256) 426 days, 7:30:22.56
```

Il est aussi possible de mettre directement le nom de chaque nœud :

```
# snmpget -v 2c -c public 10.10.100.1 system.sysUpTime.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (3683349087) 426 days, 7:31:30.87
```

Dans la ligne de commande on peut voir que plusieurs paramètres sont entrés pour snmpget :

- **-v 2c** pour désigner la version du protocole SNMP installé sur l'hôte
- **-c public** pour définir le nom de la communauté à utiliser
- **10.10.100.1** qui correspond à l'adresse IP de l'équipement à interroger

Il faut savoir que les objets présents dans la branche mib-2 (nœuds .1.3.6.1.2.1) respects un standard, une autre branche est utilisée par les constructeurs qui ajoutent des objets, cette branche se situe aux nœuds .1.3.6.1.4.1.x, x étant un numéro attribué au constructeur. Une autre branche est destinée à la version 3 du protocole SNMP.

On vient de le voir, SNMP a choisi l'espace de nommage de l'ISO, le langage utilisé pour définir les objets est ASN.1 (Abstract Syntax Notation Number 1), les primitives de ces objets sont définies dans la SMI (Structure of Management Information).

Malgré le fait que la MIB contienne énormément d'informations techniques, SNMP ne permet pas de remonter des informations capitales pour la supervision comme l'état d'un service (Web, base de données…).

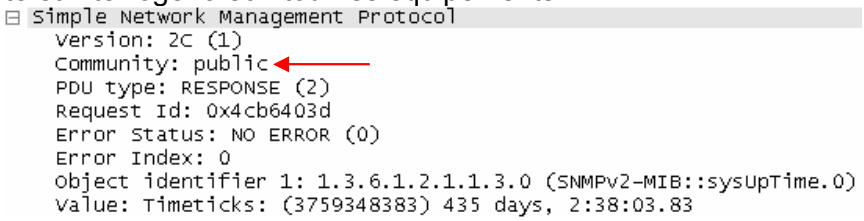
4.1.6. La sécurité

L'aspect sécurité doit être pris en compte dans le choix d'une solution d'administration du réseau puisque si la solution utilise le protocole SNMP, celui-ci devra être implanté et/ou activé sur les serveurs, les routeurs, les pare-feux…Il est donc nécessaire de voir si l'utilisation du protocole SNMP ne crée pas de failles importantes.

En revanche l'utilisation de SNMP implique l'ouverture d'un service (sur le port 161), voyons l'impact :

- Du point de vu d'Internet, la sécurité n'est pas modifiée puisqu'un pare-feu filtre tout et que seul quelques protocoles (FTP, HTTP, HTTPS et Z3950 : communication du catalogue du fond bibliographique) fournis par 2 serveurs sont disponibles ; il ne sera donc pas possible d'interroger un agent SNMP.
- En interne ça se complique car toutes les stations de travail peuvent accéder aux serveurs et aux équipements du réseau, il faut voir comment le protocole SNMP est sécurisé puisque l'on a vu que l'agent SNMP nous permet d'accéder à un grand nombre d'informations.

La première version du protocole base la sécurité sur la connaissance d'une chaîne de caractères (c'est la communauté) pour pouvoir accéder à la MIB. Cette chaîne de caractères est donc présente dans toutes les requêtes faites par le logiciel d'administration du réseau à l'agent SNMP, le problème c'est que la chaîne de caractères n'est pas cryptée et donc si quelqu'un intercepte une trame de requête il pourra sans aucune difficulté obtenir le nom de la communauté et interroger à son tour les équipements.



Partie d'une trame de réponse SNMP, la communauté apparaît bien en clair.

La seconde version avait pour but de corriger les limitations imposées par la SMI (par exemple la taille des compteurs limitée à 32 bits) mais aussi l'aspect sécurité quasiment absent dans la première. La mise à jour de la SMI a bien été réalisée (nouvelle version : SMIv2) mais pas l'aspect sécurité. Les bénéfices apportés par la nouvelle SMI seront utilisés dans la version SNMPv2c avec c pour community puisque le mécanisme de sécurité reste celui de la première version.

La version 3 achevée en 1999 met enfin en place une stratégie de sécurité consultable sur la RFC2574 (User-based Security Model for version 3 of SNMP), voici les 4 axes principaux :

- L'estampillage du temps pour empêcher la réutilisation d'un paquet (anti-rejeu).
- L'encryption pour ne plus pouvoir lire les informations de gestions contenues dans un message.
- L'authentification pour empêcher la modification du message par quelqu'un.
- La localisation des mots de passe permet de ne pas compromettre la sécurité du domaine même si l'un des agents est compromis.

3 niveaux de sécurité sont ainsi offerts :

- **noAuthNoPriv** : authentification par l'échange d'une chaîne de caractères : community (v1 et v2c) ou username pour la version 3.
- **authNoPriv** : authentification par la technique de cryptographie à clé symétrique HMAC-MD5 ou HMAC-SHA, l'authentification en passe plus en clair sur le réseau.
- **authPriv** : reprend le système d'authentification à clé symétrique mais ajoute un chiffrement des informations sensibles (les réponses demandées et l'identifiant de contexte : le port du routeur par exemple) contenus dans les trames SNMP pour les rendre illisibles sur le réseau, chiffrement par l'algorithme DES en 56 bits.

La version 3 remplace la notion de communauté par celle d'utilisateur, chaque utilisateur appartient à un groupe et chaque groupe a des droits d'accès bien définis à la MIB (objets consultables, droit d'écriture, de lecture…) mais aussi un niveau de sécurité à respecter. On peut ainsi mettre en place un groupe administrateur, chacun des utilisateurs devra obligatoirement se connecter en auhtPriv et pourra consulter et modifier tous les objets de la MIB.

En conclusion, il serait donc judicieux d'utiliser la version numéro 3 de SNMP qui assure l'authenticité et la confidentialité des échanges entre la console d'administration et les agents, mais quelle version est utilisée sur les équipements de la ville de Rezé ?

4.1.7. Le matériel est il compatible ?

La majeur partie des équipements d'interconnections du réseau (commutateurs, routeurs…) de l'hôtel de ville sont de la marque Cisco, le système d'exploitation de Cisco gère les 3 versions du protocole SNMP. On peut ainsi superviser ces équipements de façon sécurisée sans difficulté mais il faut que la console d'administration soit aussi compatible avec SNMPv3…

Voyons maintenant ce que la Direction des Systèmes d'Informations de la ville a besoin.

4.2. Définition des besoins

Avant de comparer les solutions de métrologie et de supervision disponible, il est nécessaire de définir clairement les besoins auxquels la solution devra répondre.

4.2.1. Domaine couvert, type de licence et langue

Il ne faut pas multiplier les outils car l'administration deviendra vite trop lourde, l'on souhaite donc avoir une solution complète qui sache faire de la métrologie, de la supervision, des alertes...

Il n'y a pas de restriction au niveau du type de licence, cela peut être une licence libre de type Licence publique générale GNU ou une licence commerciale. Voici les avantages et inconvénients :

La solution libre :

☺ Coût nul de licence
☺ Facilité de personnalisation (le code est modifiable)
☺ Mise à jour gratuite (à condition que le projet soit suivi)
☺ Respect des standards pour une meilleure interopérabilité
☹ Assistance humaine pour l'installation, la maintenance difficile à trouver

La solution commerciale :

☺ Livrable clé en main : installation, configuration faite par un intervenant
☺ Contrat d'assistance possible avec l'éditeur de la solution
☺ Garantie de stabilité
☹ Mise à jour généralement payante
☹ Aucune personnalisation n'est possible
☹ Cout d'achat et de mise en œuvre important

Il faut retenir que la solution libre permet une adaptation parfaite avec l'environnement du réseau (possibilité de développer un système de vérification pour une application développer en interne par exemple) mais il faut pour cela que les administrateurs sachent modifier le code de la solution. La solution commerciale ne pose pas ce problème puisqu'il n'est généralement pas possible d'ajouter des fonctionnalités spécifiques ; il faut donc qu'elle soit le plus complète possible afin de couvrir les évolutions futures du réseau (nouveau service, nouveau matériel…).

La langue utilisée sera de préférence française puisque les administrateurs du réseau ne seront pas les seuls à utiliser la solution, par exemple les assistants techniques de premier niveau seront amenés à l'utiliser. Une solution en anglais est tout de même envisageable puisqu'elle sera utilisée par des personnes ayant un minimum de connaissance des réseaux et sera donc capable de comprendre la signification des mots en anglais technique.

4.2.2. L'interface homme machine

Que la solution soit sous la forme d'une 'appliance' (désigne un équipement livré prêt à l'emploi) ou d'un logiciel d'administration à installer, l'interface entre la solution et l'utilisateur doit répondre à de nombreux critères.

4.2.2.1. L'interface elle même

L'interface locale (disponible sur la machine où est installée la solution) peut être du type fenêtré ou par une interface web.

L'interface distante (accessible aux utilisateurs depuis leur poste) peut être sous la forme d'une application JAVA ou d'un serveur http, elle est donc accessible par un navigateur

Internet.
La gestion de profils utilisateur permettant à chaque utilisateur de personnaliser l'interface distante serait un plus.

Il est par contre nécessaire que la solution permette de créer différents groupes d'utilisateurs avec différents droits possibles :

- Droit de modification des paramètres (ajout d'un équipement, modification des cartes…)
- Droit d'affichage du statut du réseau (pour les assistants informatiques de premier niveau)
- Droit d'ajouter, modifier et supprimer des utilisateurs et des groupes
- …

4.2.2.2. Organisation des entités surveillées

Une organisation des entités sous forme d'un arbre hiérarchique constitué de nœuds pères et fils est indispensable, un nœud peut être un bâtiment, un service municipal, un routeur, un hôte…

Un hôte ou un host définit une entité physique connectée sur le réseau comme une station de travail, un routeur, un commutateur… Chaque hôte possède ses propres propriétés :

- Le nom (DNS ou NetBIOS)
- Son adresse IP
- Son icône (pour une meilleure compréhension de la carte du réseau)
- Sa communauté SNMP en lecture et/ou en lecture et écriture
- Son père
- Pour un routeur et un commutateur :
- Interfaces à analyser
- Lien vers l'administration en http, https ou telnet

4.2.2.3. La surveillance

La solution doit au moins être en mesure de surveiller les serveurs (sous Windows 2000 server), les routeurs (matériel Cisco en majorité), les commutateurs (Cisco ou 3Com), les imprimantes et certains postes de travail.

Voici les différents types de surveillance qui seront utilisés si l'équipement surveillé le permet :

4.2.2.3.a. Surveillance de la disponibilité

Contrôle de la disponibilité des équipements en effectuant une interrogation SNMP ou ICMP (ping) à intervalle régulier, au minimum toutes les 5 minutes, cet intervalle doit être personnalisable par équipement.

La couleur de chacune des entités (sur la carte) doit représenter leur état :

- Rouge lorsque l'équipement ne répond pas
- Orange si l'équipement ne répond pas plusieurs fois de suite (seuil réglable)
- Vert quand l'équipement répond
- Gris si la présence de l'équipement n'est pas testée

4.2.2.3.b. Surveillance des niveaux

Surveillance par SNMP des équipements compatibles de leur état et du taux d'utilisation :

- Charge processeur
- Utilisation de la mémoire
- Nombre de requêtes SNMP traitées

- Pour une imprimante :
  - Niveau des cartouches d'impression
  - Nombre de documents en fil d'attente
  - Nombre de pages imprimées
- Pour un serveur ou une station de travail :
  - Espace disque utilisé et restant
  - Nombre de processus en cours
- Pour un routeur et un commutateur :
  - Nombre de paquets par seconde par interface
  - Nombre de ko par seconde par interface

4.2.2.3.c. Surveillance des services réseaux

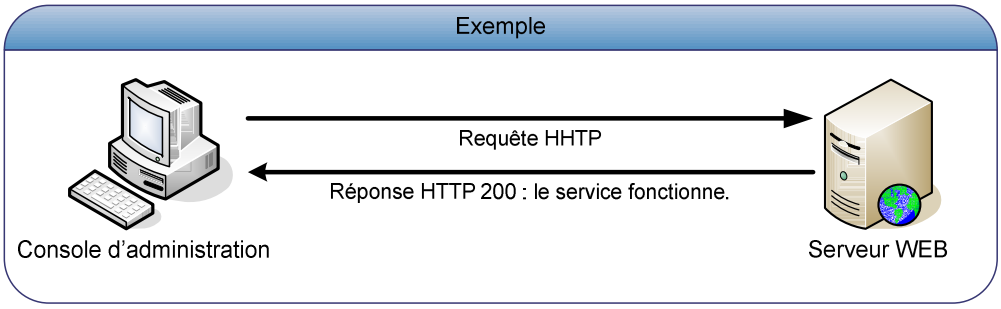
Contrôle par SNMP ou par agent sur les serveurs de la ville pour vérifier la présence de certains processus système.

Contrôle du bon fonctionnement des services par une tentative de connexion, en particulier pour les services suivants :

- Web : requête http et/ou HTTPS
- FTP : tentative de connexion
- DNS : résolution d'un nom de domaine
- POP et/ou SMTP : test de connexion à la messagerie
- Partage de fichiers : test NetBIOS
- LDAP : test de consultation de l'annuaire.

Pour les services non pris en charge, une des deux possibilités doit être présente :

- Effectuer un test de connexion TCP sur un port particulier
- Exécuter un script de test développé par un administrateur



4.2.2.4. Les graphiques

Nous souhaitons pouvoir générer différents graphiques pour toutes les ressources systèmes et réseaux que l'on souhaite et cela sur différentes échelles pour les graphiques en fonction du temps : les 5 dernières minutes, la dernière heure, les dernières 24 heures, les 7 derniers jours, les 30 derniers jours et les 365 derniers jours.

Taux d'échantillonnage minimal :

- Pour les dernières 5 minutes et pour la dernière heure : taux correspondant à la fréquence des relevés
- Pour les graphiques journaliers : un échantillon toutes les 5 minutes
- Pour les graphiques hebdomadaires : un échantillon toutes les heures
- Pour les graphiques mensuels : un échantillon toutes les 6 heures
- Pour les graphiques annuels : un échantillon par jour

Optionnellement elle peut offrir :

- La possibilité de pouvoir générer un graphique personnalisé en précisant une période comme de 8h à 20h il y a trois jours.

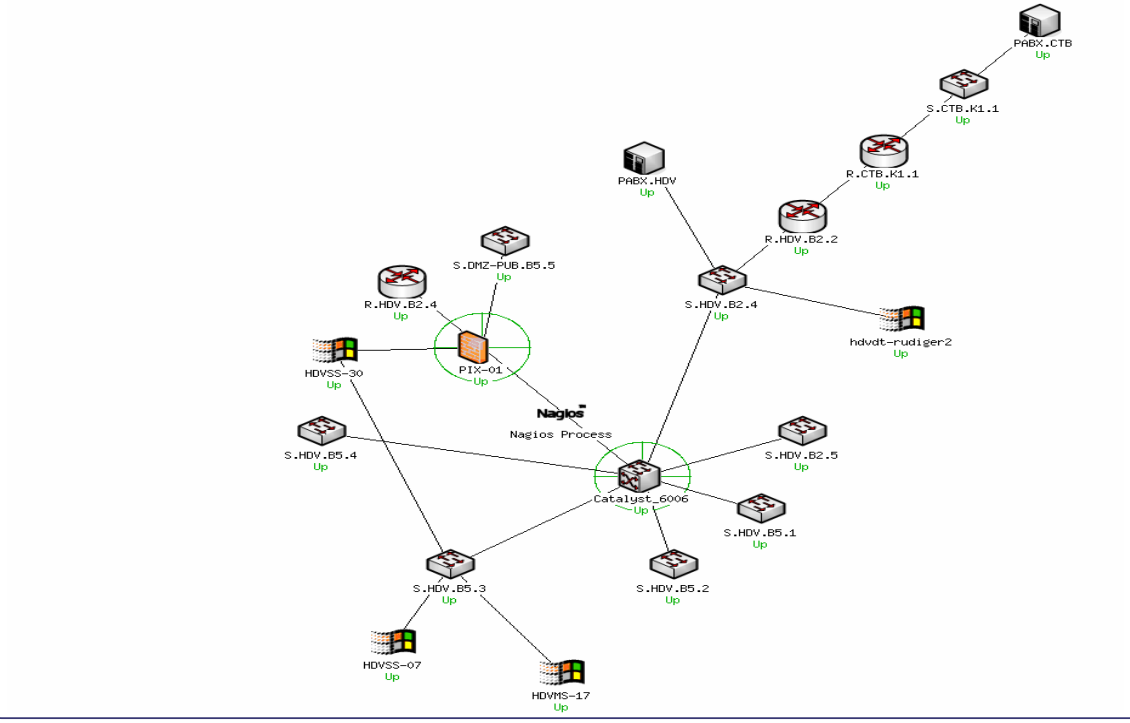
- La possibilité de permettre d'afficher plusieurs graphiques en même temps pour par exemple étudier la charge processeur d'un routeur et le flux d'une de ses interfaces réseau : affichage en un graphique regroupant plusieurs paramètres ou sur plusieurs graphiques
- La possibilité d'une exportation vers Excel ou en données bruts des valeurs.
- L'affichage du maximum
- La configuration des échelles utilisées (Axe x et y)
- La personnalisation des couleurs, du titre, des légendes
- Des graphiques de type Vumètre pour une visualisation instantanée : utilisation du processeur…

4.2.2.5. La cartographie

Un système de cartographie complet est nécessaire pour permettre aux utilisateurs d'avoir une vue globale de tous les équipements du réseau et de voir rapidement par exemple l'impact qu'aurait la coupure d'un lien. Le système doit être complet mais synthétique pour trouver efficacement d'où vient le problème, le regroupage logique des équipements est donc nécessaire : regroupage par sites, par service…

Un système d'auto découverte fiable serait un point positif mais dans tous les cas la solution doit offrir la possibilité de gérer la cartographie du réseau manuellement pour faire la différence entre la topologie logique (comprise par un système d'auto découverte) et la topologie physique du réseau. De plus, la gestion manuelle de la cartographie permet une meilleure hiérarchisation des éléments ce qui rend plus compréhensive les cartes.

Cartographie par le logiciel Nagios du réseau de l'hôtel de ville.



Une visualisation active permettant de visualiser graphiquement la structure (par site, étage, service…) est nécessaire compte tenu de la taille du réseau. Une carte inter réseau permettant de voir les liens entre les routeurs serait pratique.

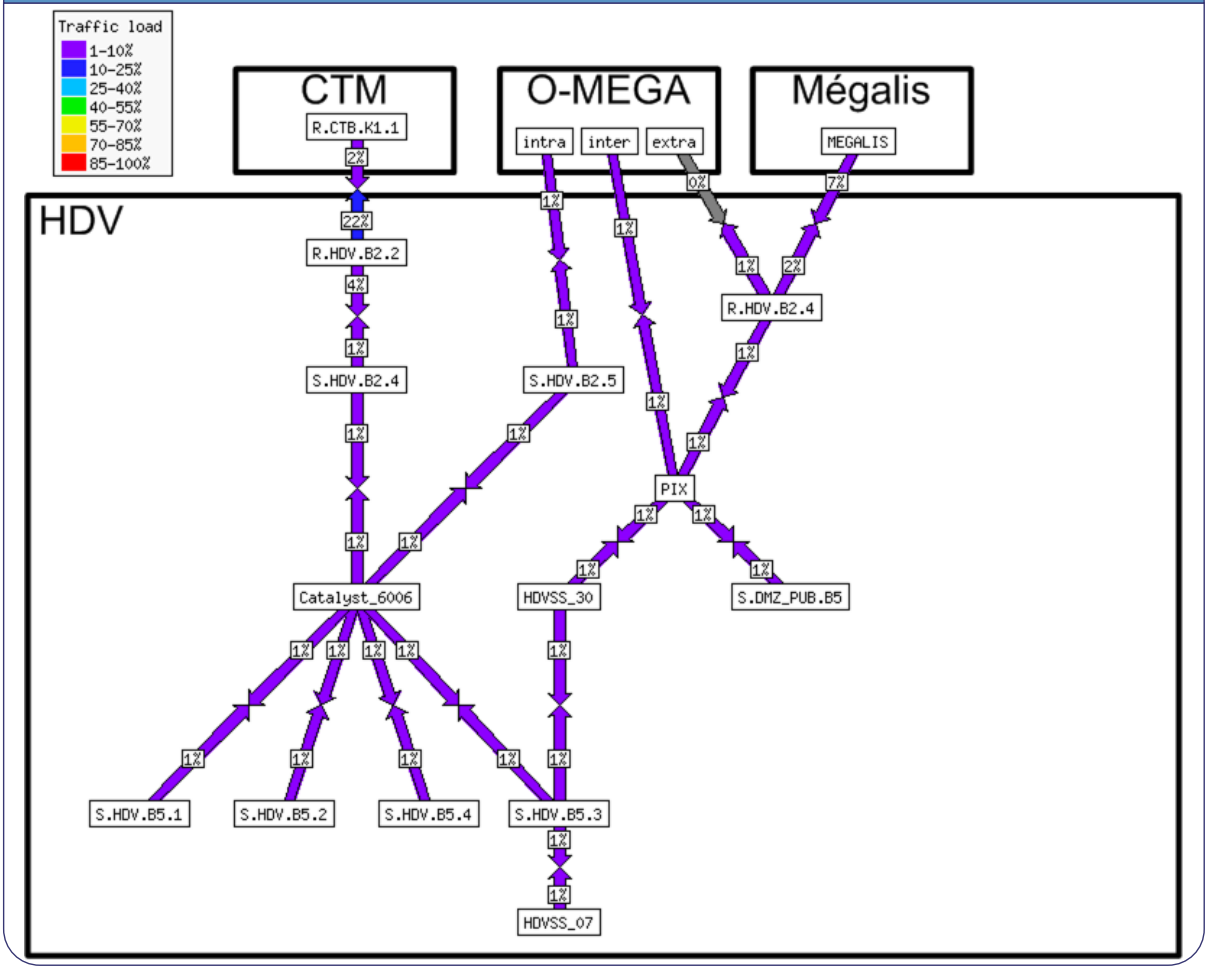
La couleur d'un objet est définit selon le résultat du test de disponibilité.

Chaque objet doit proposer un menu avec différentes options selon le type d'objet comme :

- Afficher une MIB SNMP
- Connexion Telnet, http, HTTPS
- Requête Ping par le protocole ICMP
- Accéder au statut de disponibilité de l'équipement
- Afficher un objet SNMP (uptime, charge processeur, bande passante utilisé…)
- Afficher un graphique de l'un élément qui est surveillé (Utilisation de la mémoire par exemple)
- …

Une carte permettant de voir l'utilisation de la bande passante (en pourcentage) entre certains équipements constituant le réseau permettrait de voir rapidement les éventuels goulots d'étranglement et donc les évolutions à prévoir en termes de bandes passantes nécessaires. Ce type de carte serait un point fort pour la solution.

Exemple avec la carte des flux des principaux liens de l'hôtel de ville avec le logiciel Nagios.



4.2.2.6. Gestion des événements

Un événement, c'est un changement d'état d'un équipement (Non réponse d'un routeur) ou d'une valeur.

La gestion des événements est donc importante, la solution ne doit pas se contenter de rapporter une quantité importante de données, elle doit savoir analyser ces données et détecter une anomalie, une surcharge, une dégradation de la qualité d'un service…cela avant que ce soit un utilisateur qui prévienne les administrateurs du problème.

4.2.2.6.a. La notification

Une notification intervient lorsqu'un événement a lieu et si cet événement doit engendrer une notification. Elle a pour but d'informer le plus rapidement possible les personnes souhaitées. Bien sûr tous les événements ne doivent pas provoquer une notification, il doit être possible définir les événements à notifier, le seuil de notification et les utilisateurs et/ou les groupes à notifier lorsque ce seuil est atteint.

On doit pouvoir modifier la fréquence de ces notifications (une notification toute les 5 minutes et cela trois fois) et cela par moyen utilisé : courriel, pager (petit équipement portatif destiné à recevoir de court message), mini message… Par exemple, il est important de limiter le nombre maximal de mini message à envoyer car cela coûte cher.

Le système de notification doit gérer l'organisation logique du réseau : si un lien vers un site distant ne fonctionne plus, il est inutile d'envoyer 40 notifications signalant que les 40 postes informatiques présents sur ce site sont injoignables.

4.2.2.6.b. Liste des événements

Sur l'interface, on doit pouvoir visualiser la liste de tous les événements qui ont eu lieu. Un système de filtre permettant de ne visualiser que les événements concernant un seul équipement par exemple ainsi qu'un système de comptage des événements sont souhaitables.

Les événements doivent être conservés au moins 1 an dans la limite de 20 événements par jour pour permettre aux administrateurs d'analyser une panne ou un ralentissement répétitif d'un équipement par exemple.

4.2.2.6.c. Création d'un événement

D'après les points cités ci-dessus, la création d'un événement implique l'utilisation des champs suivants :

- Un nom d'événement
- Les équipements concernés par cet événement
- L'élément déclencheur de l'événement :
- Un seuil dépassé (charge du processeur, espace disque…)
- Un changement d'état : l'hôte ou un service ne répond plus
- Un problème de sécurité : un nouveau service a été installé, un port a été ouvert…
- Intervalle de contrôle de disponibilité, si contrôlé
- Evénement sur réception d'un Trap SNMP
- Sélection de l'équipement envoyant ce Trap
- Type de Trap : LinkUp, LinkDown…
- Ajout de l'événement dans la liste des événements (pour éviter de « poluer » la liste)
  - La ou les actions à réaliser :
  - Notifier:
    - ✓ Les utilisateurs et/ou groupes à notifier
    - ✓ La fréquence de notification par moyens
    - ✓ Le message à envoyer (gravité, équipement…)
  - Agir :
    - ✓ Exécution d'un script
    - ✓ Modification de la configuration d'un équipement (avec la commande SET de SNMP par exemple)
    - ✓ Enregistrement automatique des fichiers log de l'équipement…

4.2.3. Fonctionnement

4.2.3.1. La base de donnée

Une base de données sera nécessaire pour enregistrer par exemple : les valeurs collectées, les événements, les éléments réseaux… L'espace utilisé par cette base ne devra pas dépasser une certaine valeur, ce sera à la solution de consolider sa base, en particulier pour les valeurs relevées.

4.2.3.2. Matériel nécessaire

Dans le cas d'une solution sous forme d'une 'appliance', seule une connexion au réseau de l'hôtel de ville est nécessaire.

Dans l'autre il s'agira de l'installation d'un logiciel, l'utilisation d'une machine dédiée est envisageable c'est le cas de la solution actuelle. Le système d'exploitation actuellement en place est Microsoft Windows 2000 qui est d'ailleurs le seul système d'exploitation utilisé sur tous les micro-ordinateurs de la ville, il sera possible de changer ce système d'exploitation pour faire fonctionner une solution libre par exemple.

4.2.3.3. La configuration

L'installation et la configuration de la solution ne doit pas demander de compétences particulières et donc être intuitive. La majorité de la configuration : définition des utilisateurs, des équipements à surveiller… doit pouvoir se faire à distance via une interface web ou une application cliente.

4.2.3.4. Les protocoles

Le protocole de supervision et de métrologie utilisera le protocole SNMP de la première version à la version 2c puisque tous les équipements ne sont pas compatibles avec la version 3.

L'installation d'agents sur les serveurs est possible, ces agents doivent être compatibles avec Windows 2000 et les versions ultérieures (notamment XP et 2003). L'installation doit être simplifiée et les agents ne doivent pas rendre instable le système d'exploitation. Windows 2000 intègre un agent SNMP qui est désactivé par défaut, il sera possible d'activer celui-ci.

4.2.3.5. Adaptation au réseau

C'est à la solution de s'adapter au réseau de la ville, qui je le rappelle est répartie sur plusieurs sites et notamment par des liaisons du type VPN (Virtual Private Network). Les sites VPN distants sont cloisonnés par un Firewall et doivent être surveillés. La solution doit donc définir les modifications à faire au niveau du Firewall mais aussi des routeurs pour qu'elle puisse les superviser.

4.2.3.6. La sécurité

L'accès à l'interface distante utilisera un système d'authentification par nom d'utilisateur et mot de passe ou en utilisant l'annuaire active directory (protocole LAPD).

La sécurité au niveau de la récupération des données dépendra du protocole utilisé, il n'y a pas de niveau de sécurité à respecter puisque les attaques internes sont considérées comme nulles mais une solution n'utilisant pas les options de sécurité offertes par le protocole qu'elle utilise ne sera pas retenue puisque certaines interrogations passeront sur le réseau Internet.

La sécurité de ‘l’appliance’ ou de l’application doit être un minimum présente mais la aussi les attaques internes sont peu probables et il ne sera pas possible d’accéder à la machine par Internet.

4.2.3.7. La maintenance

Il ne doit pas y’en avoir ou alors très peu puisque la solution doit être autonome au maximum.

La mise à jour de la solution peut être payante ou gratuite, sauf en ce qui concerne les mises à jour visant à combler une faille de sécurité qui doit être gratuite.

4.2.3.8. La tolérance aux pannes

En cas de plantage du système d’exploitation, et donc d’un redémarrage par coupure électrique ou d’une coupure électrique de la machine, la solution doit être capable de se relancer seule sans erreur.

5. La solution mise en place

Le sujet de mon stage ne consistait pas à mettre en place une solution mais à analyser les méthodes de métrologies et supervisions existantes pour déterminer ce qu'une solution fasse, ce qui est inutile…pour guider mon service dans l'acquisition future d'une solution.

J'ai néanmoins essayé une solution très connue dans le monde des logiciels libres mais aussi dans le monde de la supervision et la métrologie : c'est Nagios.

La communauté open source à dans un premier temps créée des solutions permettant de répondre aux aspects les plus simple de la gestion d'un réseau. Ces solutions s'étant de plus en plus développées, elles offrent maintenant une alternative crédible face aux solutions propriétaires.

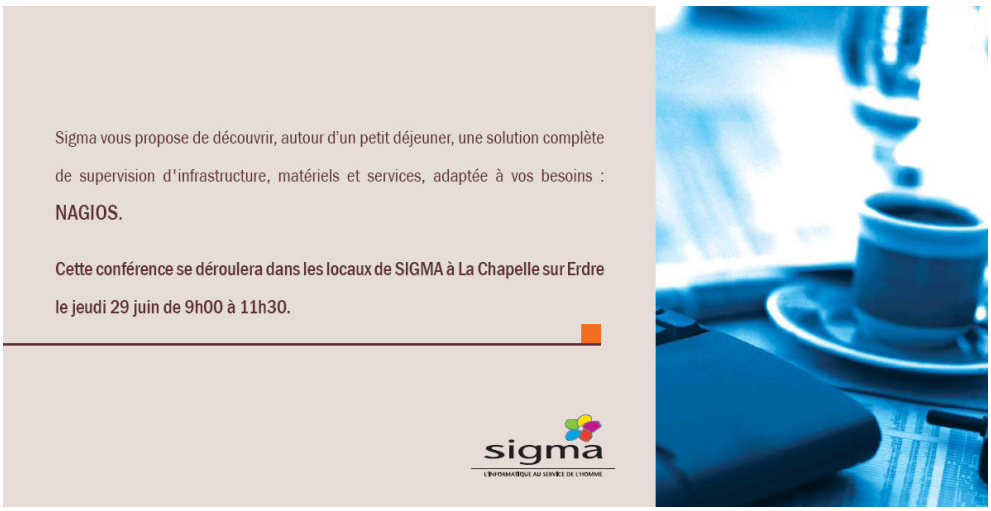
5.1. Historique et caractéristiques

Nagios anciennement appelé Netsaint jusqu'en 2003 est qualifié comme un logiciel capable de superviser un Système d'information complet. Il est disponible sous la licence GPL (General Public License) permettant de jouir des libertés suivantes :

- Libre droit d'exécution pour n'importe quel usage,
- Libre droit d'étude du logiciel et de modification,
- Libre droit d'amélioration et de rendre publique vos modifications,
- Libre droit de le redistribuer.

La licence ne pose donc aucune contrainte.

La communauté de développement est importante, le cœur de Nagios est écrit par Ethan Galstad. Le projet est très suivi, la dernière version stable date du 31 mais 2006. Il est possible de trouver un support technique en France, plus de 25 sociétés de services sont référencées avec des tarifs allant de 25 à 500€ de l'heure (source : www.findopensourcesupport.com). La mairie à d'ailleur récemment reçu (le 7 juin) de la par d'une Société de Services en Ingéniérie Informatique (SSII) de la région Nantaise, une invitation à découvrir « Une solution complète de supervision » :



Un support par internet est aussi possible avec différents forums francophone et anglais permettant d'exposer ses problèmes et d'obtenir une réponse rapide (dans la journée généralement). Ces forums créent une base de données imposante permettant de trouver rapidement des réponses sans attendre.

La communauté de développement est imposante mais celle écrivant les documentations l'est aussi puisqu'il est possible de trouver rapidement les instructions d'installation, de configuration, de résolution des problèmes… dans plus de 10 langues.

Il fonctionne sur les systèmes d'exploitation suivants : Linux, BSD (Berkley Software Distribution), Unix et Os X. Il est déjà présent sur la plupart des distributions Linux.

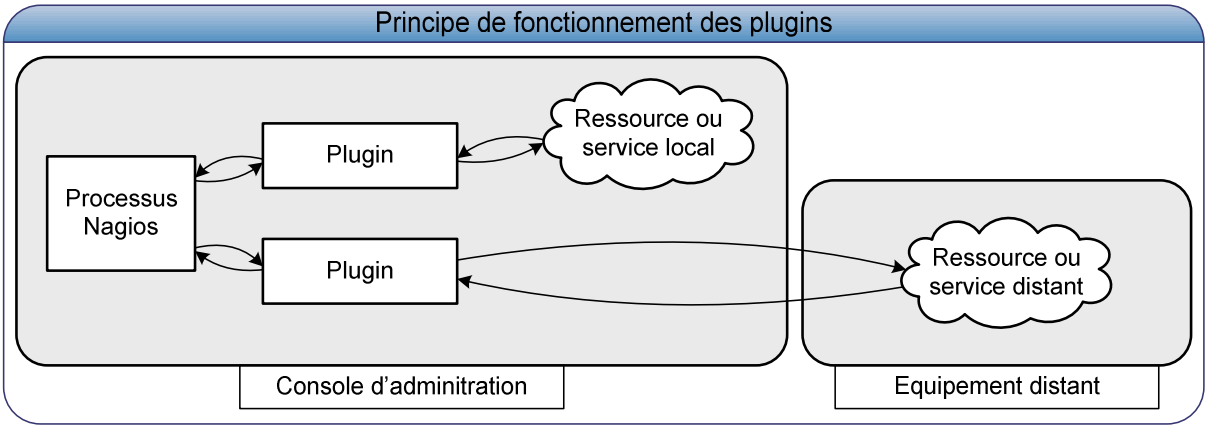
5.2. Fonctionnement

Comme beaucoup de logiciels libres, Nagios est modulaire, il se décompose en trois parties :

- L'Ordonnanceur (le moteur de l'application) qui organise et traite l'exécution des vérifications, il détermine ensuite en fonction des réponses les actions à entreprendre : mise à jour de l'affichage de l'interface, notification, génération d'un événement…
- L'interface web qui permet une vue d'ensemble du système d'information et des éventuelles disfonctionnements.
- Les plugins sont des petits programmes qui réalisent les opérations de vérification des équipements, services et applications. Ces plugins permettent de s'adapter à des besoins spécifiques d'un système d'information. Il en existe une multitude, il est facilement possible de les modifier ou d'en créer de nouveaux (langage de programmation Perl, Bash, C++, PHP, Python…).

Principe des plugins :

En standard, Nagios intègre certains plugins dont un permettant d'interroger les équipements par SNMP, il est donc possible de base de surveiller un grand nombre d'équipements.



Il existe aussi des agents qu'il faut installer sur l'équipement. Il s'agit en fait d'un plugin comme les autres mais qui est capable d'exécuter un autre plugin sur l'équipement : c'est l'agent NRPE (Nagios Remote Plugin Executor). Un autre agent permet de faire des vérifications de type passives, la vérification n'est donc plus faite à l'initiative de Nagios. C'est l'agent qui réalise les vérifications et qui envoie les résultats à Nagios au travers du plugin NSCA (Nagios Service Check Acceptor) qui est en fait un daemon (processus s'exécutant en arrière plan). Ce plugin permet une adaptation aux environnements cloisonnés.

5.3. Possibilités

Voici une liste non exhaustive des possibilités de gestion offertes :

- ✓ Supervision des services réseaux : SNMP, POP, HTTP, LDAP…
- ✓ Supervision des ressources serveurs : processeur, mémoire, disque...
- ✓ Vérification en parallèle ou non des services.
- ✓ Hiérarchisation des équipements pour différencier un serveur en panne d'un serveur injoignable.
- ✓ Notification paramétrable par les plugins : courriel, SMS…
- ✓ Chaque vérification renvoi l'un de ces quatre états :
- ✓ OK (pas de seuil dépassée, tout va bien)
- ✓ WARNING (le seuil de cet état est dépassé)
- ✓ CRITICAL (le seuil de cet état est atteint)
- ✓ UNKNOWN (l'état est inconnu ou l'équipement est injoignable)

5.4. La couche Oreon

Le projet Oreon a été lancé il y a maintenant plus de trois ans, il a pour but d'offrir une nouvelle interface à Nagios et d'offrir de nouvelles fonctionnalités.

L'interface est plus personnalisable, et intuitive ; elle facilite la configuration de Nagios, des équipements mais aussi des services à surveiller. En effet la configuration de Nagios est laborieuse, rien n'est possible par l'interface web d'origine il faut directement aller modifier les fichiers de configuration et relancer le processus pour que les modifications soient prises en comptes.

Voici à quoi ressemble la définition d'un équipement avec un simple test par ping :

```
# 'hdvdt-rudiger2' host definition 0
#
define host{
    use                     HTemplate_Défaut_test_ping
    host_name                       hdvdt-rudiger2
    alias                   Client : RUDIGER R
    address                         hdvdt-rudiger2
    parents                         S.HDV.B2.4
    check_command                   check_host_alive
    max_check_attempts              3
    checks_enabled                  1
    low_flap_threshold              0
    high_flap_threshold     0
    notification_interval   15
    notification_period     24x7
    notification_options    d
    notifications_enabled   1
```

La simplification de la configuration n'est donc pas un élément négligeable, Oreon présente cette configuration sous la forme d'un formulaire et permet l'utilisation de Template (définition par défauts) très pratique lors de taches répétitives comme l'ajout de 15 serveurs avec par défaut un test par ping.

Par ailleur l'interface étant entièrement franchisée, il n'est pas difficile de comprendre l'utilisation de celle-ci.

Oreon offre aussi un système de carte météo du réseau, ce système se base sur les sondes qui relèvent le trafic des interfaces des routeurs, commutateurs et les serveurs. Ce système est classé en développement puisque les développeurs migrent vers un plugin PHP intitulé php-weathermap en remplacement du langage perl.

Le projet est lui aussi très bien suivi, la dernière version BETA disponible date du premier juin 2006. Il est également publié sous la licence GPL. Oreon étant une interface de Nagios, il faut bien entendu installer Nagios en premier.

5.5. Installation

Nagios fonctionnant sous Linux et ayant de bonnes connaissances de la distribution Debian, j'ai choisi d'installer celle-ci.

N'ayant qu'une machine et n'étant qu'un essai d'une solution, j'ai utilisé le logiciel Microsoft Virtual PC pour lancer une machine virtuelle sous Windows sur laquelle j'ai installé Debian. Cela présente plusieurs avantages dont la portabilité de la solution de supervision quelque soit l'architecture matériel ne demande aucune modification de la configuration, en cas de plantage il n'y a que la machine virtuelle de touchée…

5.5.1. Le système d'exploitation

L'installation de Debian n'a posé aucun problème, installation à partir d'internet puisque très peut de paquets sont nécessaires : pas d'interface graphique, pas de logiciel de bureautique…

A la fin de l'installation environs 600 Mo sont utilisés. A ce stade le système n'offre aucun service sauf un accès à distance SSH. J'ai fait ce choix pour n'installer que le strict minimum mais aussi pour choisir les bonnes versions des logiciels dont Nagios et Oreon se servent.

5.5.2. Les dépendances

Les pré requis de Nagios sont peut nombreux, il faut que le protocole TCP/IP soit bien configuré puisque l'on souhaite surveiller les équipements sur le réseau. Il faut également un compilateur de langage C. Ces deux éléments sont déjà présent puisque l'installation se fait par le réseau le protocole TCP/IP fonctionne et le compilateur était lui nécessaire à l'installation des paquets de base.

Un serveur web à du être installé, j'ai utilisé apache (version 2) car c'est celui que je connais le mieux. Pour la génération des images incluse dans les scripts CGI (En anglais : Common Gateway Interface, c'est un procédé consistant à ne pas afficher le contenue d'un fichier mais à exécuter un programme pour en afficher le résultat), Nagios a besoin de la librairie GD écrite pas Thomas Boutell's.

Oreon utilise une interface écrite principalement en PHP, cette interface se base sur une base de données de type SQL.

Voici un récapitulatif des logiciels utilisés :

apache2	2.0.54-5	Serveur HTTP
apache2-common	2.0.54-5	fichiers de base du serveur HTTP
apache2-mpm-pr	2.0.54-5	module du serveur HTTP
apache2-utils	2.0.54-5	utilitaire de configuration et de débug
libapache2-mod	4.3.10-16	Librairie d'exécution des scripts HTTP
libdbd-mysql-p	2.9006-1	Interface entre les scripts perl et la base MySQL
libdbi-perl	1.46-6	Librairie pour les scripts perls
libgd2	2.0.33-1.1	Librairie GD version 2
libgd2-xpm	2.0.33-3	Librairie GD version 2
libgd2-xpm-dev	2.0.33-3	Librairie GD version 2
libgdbm3	1.8.3-2	Librairie GD version 2 (routine d'exécution)
libjpeg62	6b-10	Librairie pour la génération d'images JPEG
libjpeg62-dev	6b-10	Paquet de développement de la librairie JPEG
libsnmp-base	5.1.2-6.2	Librairie pour le client SNMP
libsnmp5	5.1.2-6.2	Librairie pour le client SNMP
mysql-client	4 4.1.11a	Client en ligne de commande de la base MySQL
mysql-common	4 4.1.11a	Base MySQL
php4	4.3.10-16	Gestion du langage PHP pour apache
php4-cgi	4.3.10-16	Exécution de CGI dans les scripts PHP
php4-cli	4.3.10-16	Interpréteur de ligne de commande PHP
php4-common	4.3.10-16	Paquet commun au langage PHP
php4-gd	4.3.10-16	Utilisation de GD au travers des scripts PHP
php4-mysql	4.3.10-16	Gestion de la base Mysql au travers des scripts PHP
php4-snmp	4.3.10-16	Gestion de SNMP au travers des scripts PHP
phpmyadmin	2.6.2-3sarge1	Client MySQL par une interface WEB
postfix	2.1.5-9	Acheminement des mail vers un serveur SMTP
rrdtool	1.0.49-1	Génération des graphiques
snmp	5.1.2-6.2	Paquet pour faire des interrogations SNMP

5.5.3. Installation de Nagios

Une fois les dépendances faites, l'installation ne pose normalement pas de problème, j'ai simplement générer les fichiers de configurations utilisés pour que le compilateur C sache où se trouve les différentes librairies, leurs versions… Il suffit d'exécuter un script en tapant : './Configure'

Il faut ensuite créer l'exécutable d'après les fichiers source et la configuration précédemment générée en effectuant un 'make'.

Maintenant il ne reste plus qu'à installer le programme avec la commande 'make install' qui provoque la lecture du code contenant les instructions d'installation.

Nagios est maintenant installé, il reste à le configurer mais Oreon est ici pour simplifier cette fastidieuse tache.

5.5.4. Installation d'Oreon

Oreon n'étant pas un logiciel mais une interface WEB, c'est un simple script qui demande le répertoire d'installation de Nagios (qui est par défaut /usr/etc/nagios/), le répertoire où Oreon sera installé puis où se trouve 'sudo' qui permet d'exécuter des commandes en tant que super utilisateur (root).

Oreon a ajouté un alias dans la configuration du serveur Apache :

Ainsi lorsque l'on accède à la page WEB avec une adresse du type :
http://127.0.0.1/oroen/
le serveur affichera la page d'accueil présente dans le dossier : /usr/local/oreon/

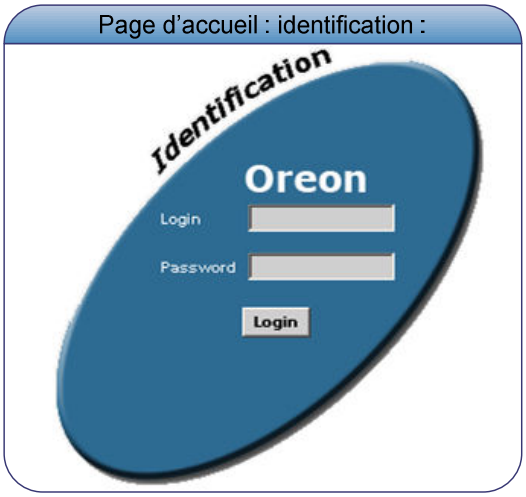
5.5.5. Configuration de base

La configuration se finalise au travers de quelques pages WEB, il faut indiquer l'emplacement du binaire rrd, des plugins Nagios, l'adresse du serveur MySQL…

Les deux dernières pages permettent de créer un compte administrateur et la dernière injecte les tableaux de données dans la base MySQL (une cinquantaine).

Voilà la configuration de base est terminée, Oreon et Nagios sont opérationnels.

Page d'accueil : identification :



5.6. Adaptation au réseau et utilisation

5.6.1. Configuration des Hôtes et des services à surveiller

Il faut dans un premier temps prendre connaissance du fonctionnement des sondes (ou plugins), comment ajouter un équipement, comment lui associer des services de surveillance, savoir gérer les groupes d'équipements, de services…

Je ne détaille pas ces étapes qui n'ont rien de complexes mais sont longues à réaliser vu la taille du parc informatique. Le but n'était pas de mettre en place une solution complète, configurée et donc fonctionnel pour le service Systèmes et Réseaux, c'est pourquoi je n'ai pas ajouté tous les équipements, notamment certains serveurs, routeurs des sites distants…

J'ai ajouté un nombre suffisant d'équipements pour me permettre de voir, tester, critiquer les différentes fonctionnalités.

Au total ce sont 58 équipements supervisés avec 115 services qui leurs sont associés. Cela va de la simple vérification de présence de l'équipement pas un test « ping » à la surveillance de la charge processeur et mémoire du firewall, des routeurs, des serveurs…

Voici un résumé des possibilités de configuration :

- Gestion de Template pour les équipements, les services et les graphiques (titre, légendes, valeurs affichées…). Mise à jour automatique de tous les équipements ou services lorsque l'on modifie un Template. Cette mise à jours n'est malheureusement pas disponible pour les graphiques, ce point faible sera corrigé dans la nouvelle version.
- Système de détection automatique des équipements
- Système de duplication d'un équipement permettant de copier toute la configuration et les services qui lui sont attribués.
- La carte des flux n'est pas générée automatiquement puisque c'est techniquement difficilement réalisable. Néanmoins la configuration est longue, il faut créer un fond de carte sous un logiciel d'imagerie, l'exporter au format PNG en 256 couleurs avec un fond transparents. Puis ajouter les équipements pour lesquelles il existe au moins un service portant le mot « traffic » et attribuer une position sur les axes X et Y au pixel prêt. La configuration ma pris une journée pour 18 équipements, elle est visible page : 46.

- La gestion des sondes est facilement compréhensible, une liste d'arguments est appliquée aux plugins qui réalisent la vérification. L'ajout d'une sonde est possible via l'interface ce qui est pratique pour un utilisateur ayant peut de connaissance de Linux.

5.6.2. Fonctionnalités

Voici un petit descriptif des fonctionnalités offertes par le couple logiciel Nagios/Oreon.
Coté supervision on à :

- Supervision des équipements réalisant l'infrastructure du réseau (bande passante par ports, charge du CPU, de la mémoire…)
- Supervision des serveurs ou stations de travails (charge CPU, charge mémoire, charge des interfaces réseaux, température…)
- Supervision des services offerts (WEB, courriels (SMTP, POP3), bases de données…)
- Certaines de ces supervisions offrent l'utilisation de graphiques : globalement toutes les données numériques (charge, température, bande passante…).

Coté gestion :

- Il est possible de créer une arborescence des équipements constituants le réseau, ce qui permet de respecter la logique du Système d'Information et d'obtenir une cartographie réaliste du réseau.
- Toute défaillance génère un événement et une notification si celle-ci est activée.
- Le système de notification est complet, les notifications sont envoyées par courriels ou SMS à condition de disposer d'une passerelle.
- Il est possible de programmer une maintenance sur un équipement, ce qui désactive les notifications pendant toute la durée de la maintenance.
- L'interface est multi utilisateurs, chaque profil comprend la langue utilisée, les droits de configuration ou non et les ressources visibles.
- Il est possible de générer des graphiques personnalisées (dans la nouvelle version, une fonction permet d'intégrer plusieurs sources dans un même graphique).
- La configuration est bien sûr exportable, la mise à jour de Nagios ou Oreon semble facilement réalisable. Lors de l'ajout ou la modification d'un équipement ou d'un service, il faut générer les fichiers de configurations de Nagios puis redémarrer celui, ces deux opération se réalisent par l'interface WEB en quelques clique. Un système de débogage permet de voir les éventuelles erreurs dans la configuration comme un équipement sans service associé, un nom d'équipement comportant des caractères spéciaux susceptible d'engendrer un mauvais fonctionnement des plugins…

Coté cartographie :

- Une carte du réseau est disponible, elle est générée automatiquement en se basant sur les dépendances entre les équipements, celle-ci fonctionne bien mais lorsqu'il y a trop d'équipement elle devient illisible. Il est possible d'attribuer une représentation graphique pour chaque équipement, ce sont des images 'png', cette attribution se fait très facilement avec une fonction d'upload des images intégrées à l'interface.
- Cette même carte est disponible en 3D, un peut gadget comme fonction…
- Une carte des flux comme promis dans les documents est disponible, elle offre de bons résultats mais le langage utilisé étant en perl, la génération est longue plutôt longue (environs 5 secondes). Cette fonction est en cours de réécriture par les développeurs.

5.7. Conclusion du test

Oreon et Nagios offrent une bonne solution de supervision et de métrologie cependant le périmètre technique couvert par cette solution Open Source ne semble pas aussi étendu qu'une solution propriétaire. La solution couvre à peu près tous les aspects définis dans les besoins du service (Paragraphe 4.2).

Je préconise cette solution au service Systèmes et Réseaux car elle est simple d'utilisation, stable, complète et en constante évolution. Le problème posé par cette solution c'est qu'elle fonctionne sur une plateforme Linux, aujourd'hui aucune personne dans le service n'a de connaissance suffisante pour mettre à jour la solution et le système d'exploitation mais surtout si un disfonctionnement de la plate forme de supervision survient, personne ne sera capable de résoudre le problème. La solution serait de confier l'installation, la configuration et la maintenance à une société de service informatique comme celle qui leur propose de découvrir Nagios.

Mon maître de stage envisage d'utiliser cette solution car elle répond aux besoins exprimés par la Ville de Rezé.

6. Rezé les couleurs

6.1. L'événement

La ville de Rezé n'a pas réellement de centre, puisqu'elle est en réalité composée de plusieurs villages réunis au XVIII^{ème} siècle. C'est donc dans une idée d'impliquer tous les quartiers autour d'une même manifestation que Rezé les couleurs a été créé.

Chaque quartier est invité à hisser l'une des six couleurs (une par quartier) qui lui a été attribuée, c'est l'occasion de mieux connaître des voisins, d'organiser des repas, des animations, des concerts…

6.2. L'implication du service

Pour l'édition 2006 la ville de Rezé a investi dans un projet de Totems interactifs. Un Totems c'est une colonne de 2 mètres dans laquelle sont superposés quatre écrans, munis d'une webcam les habitants de chaque quartier pourront défendre leur couleur en se faisant prendre en photo, photo qui est instantanément affichée sur tous les totems et sur internet. Ainsi trois Totems ont été installés dans la ville.

6.3. L'implication du service et mon rôle

Pour que les photos s'affichent sur tous les totems, ceux-ci doivent pouvoir communiquer, c'est la que mon service intervient.

Sur les trois sites investis par les totems le réseau de la ville est présent, il était donc possible d'utiliser le réseau de la mairie pour permettre la communication des totems mais ceux-ci réclament l'ouverture de ports spécifiques sur le routeur de chaque site, l'ajout de règles dans le pare-feu… Devant cette complexité technique et en prenant en compte que ce n'est que pour trois mois, un partenariat avec France Telecom a été mis en place.

France Telecom a donc mis à notre disposition une ligne ADSL sur chaque site, il ne restait plus qu'à configurer puis installer les trois routeurs pour offrir un accès internet aux Totems.

C'est ici que j'interviens, on m'a chargé de configurer les routeurs, d'ouvrir les ports demandés par le créateur des Totems et d'autoriser un accès à distance à l'interface de configuration des routeurs (interface WEB sécurisée par le protocole HTTPS).

Ce sont des routeurs de la marque Cisco avec un modem ADSL intégré, quatre ports Ethernet et un port console pour la configuration en ligne de commande.

La configuration n'a pas posé de problème, une partie est reportée page 41.

Une fois la configuration du premier routeur testée en essayant la redirection des ports, la configuration du pare-feu et l'accès à la console d'administration, j'ai dupliqué cette configuration aux deux autres routeurs pour n'avoir plus qu'à modifier les identifiants ADSL.

Une fois que France Telecom nous a indiqué que les lignes ADSL étaient en place, nous nous sommes déplacés sur les différents sites pour mettre en place les routeurs. J'ai ainsi pu câbler l'arrivé ADSL sur le routeur, puis brasser le lien Ethernet vers la bonne prise réseau.

Sur l'un des sites il n'y avait pas de prises réseau à proximité du Totem, le passage d'un câble n'étant pas envisageable dans un lieu public nous avons utilisé une transmission par courant porteur en plaçant deux boitiers CPL (Courant Porteur en Ligne) : un dans la baie de brassage, l'autre sur la prise électrique utilisée par le Totem.

6.4. Conclusion

Ce projet m'a donné l'occasion de voir la topologie physique du réseau des sites distants, et m'a donné l'occasion d'exercer le métier d'un technicien réseaux pendant quelques jours.

7. Conclusion

Ce stage est ma première expérience du monde des collectivités locales, j'ai été surpris par la taille du réseau en place, par la modernité des technologies utilisées et par les moyens matériels et humains mi à la disposition des utilisateurs du Système d'Information.

Il m'a été proposé un sujet intéressant puisque beaucoup d'organisation réfléchissent sur une solution leur permettant de connaître l'état de leur réseaux mais aussi d'avoir de précieux indicateurs pour anticiper les évolutions à réaliser et ainsi mieux gérer leurs budgets d'investissement et de fonctionnement.

Ce stage m'a enrichi personnellement et professionnellement car j'ai appris à gérer un projet du début à la fin et à m'intégrer dans une équipe. A cette occasion j'ai pu mettre en pratique mes connaissances théoriques acquises au cours de ma formation sans pour autant avoir des connaissances dans le domaine de la supervision et de la métrologie. Pour compléter mes connaissances je me suis appuyé sur des documents trouvés sur Internet et par le biais d'échanges formels et informels avec mon maître de stage et les membres de l'équipe « Systèmes, Réseaux et Télécommunications ».

7.1. Les Totems interactifs

7.1.1. Un Totem et quelques œuvres

Un des Totems :

Deux œuvres, la première c'est mon maître de stage :

La seconde, l'un des deux techniciens :

7.1.2. La configuration des routeurs

Voici les règles de translation pour autoriser les ports :

- vers l'adresse privée du Totem : 192.168.1.40 :
  - 1501 en tcp
  - 1500 en udp
  - 1194 en udp
  - 22 (SSH) en tcp
  - 80 (HTTP) en tcp
- le port 443 pour accéder à distance à l'interface de configuration mais que de la mairie (sélection par l'adresse IP de la mairie qui est la seule autorisée à utiliser le port 443).

Voici les règles pour la translation statique des ports vers le Totem :

```
ip nat inside source static tcp 192.168.1.40 1501 interface Dialer0 1501
ip nat inside source static udp 192.168.1.40 1500 interface Dialer0 1500
ip nat inside source static udp 192.168.1.40 1194 interface Dialer0 1194
ip nat inside source static tcp 192.168.1.40 22 interface Dialer0 22
ip nat inside source static tcp 192.168.1.40 80 interface Dialer0 80
```

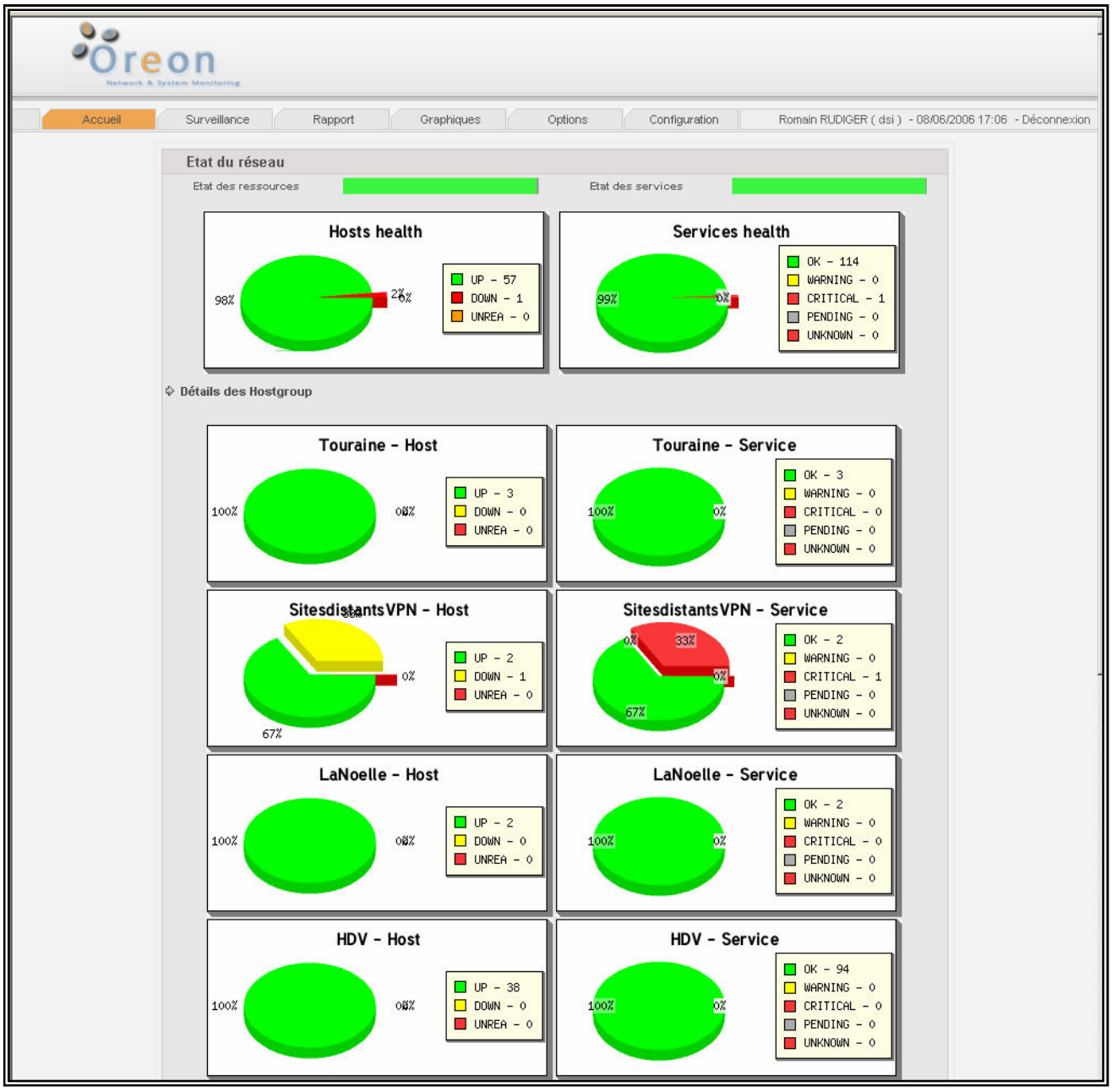
Il n'y a pas besoin de translater le port 443 vers le routeur puisqu'il aura directement une adresse publique.

Maintenant voici les règles du pare-feu autorisant n'importe qu'elle adresse IP à communiquer avec le Totem sur les ports définis ci-dessus et les 3 adresses IP publique de la mairie pour l'administration à distance du routeur :

```
access-list 101 permit tcp any any eq 1501
access-list 101 permit udp any any eq 1500
access-list 101 permit udp any any eq 1194
access-list 101 permit tcp any any eq 22
access-list 101 permit tcp any any eq www
access-list 101 permit tcp host 212.234.243.1 any eq 443
access-list 101 permit tcp host 217.109.172.1 any eq 443
access-list 101 permit tcp host 217.109.172.13 any eq 443
access-list 101 deny   ip any any log
```

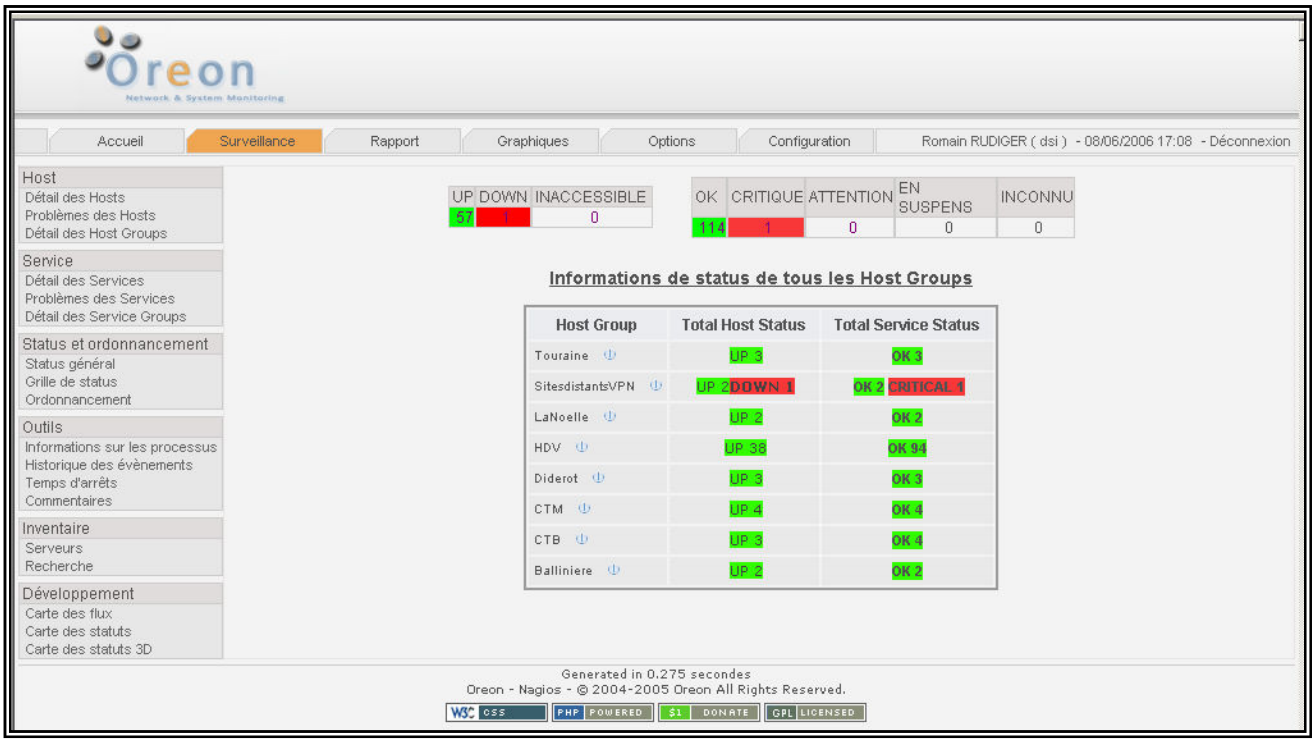
7.2. Oreon en images

7.2.1. La page d'accueil



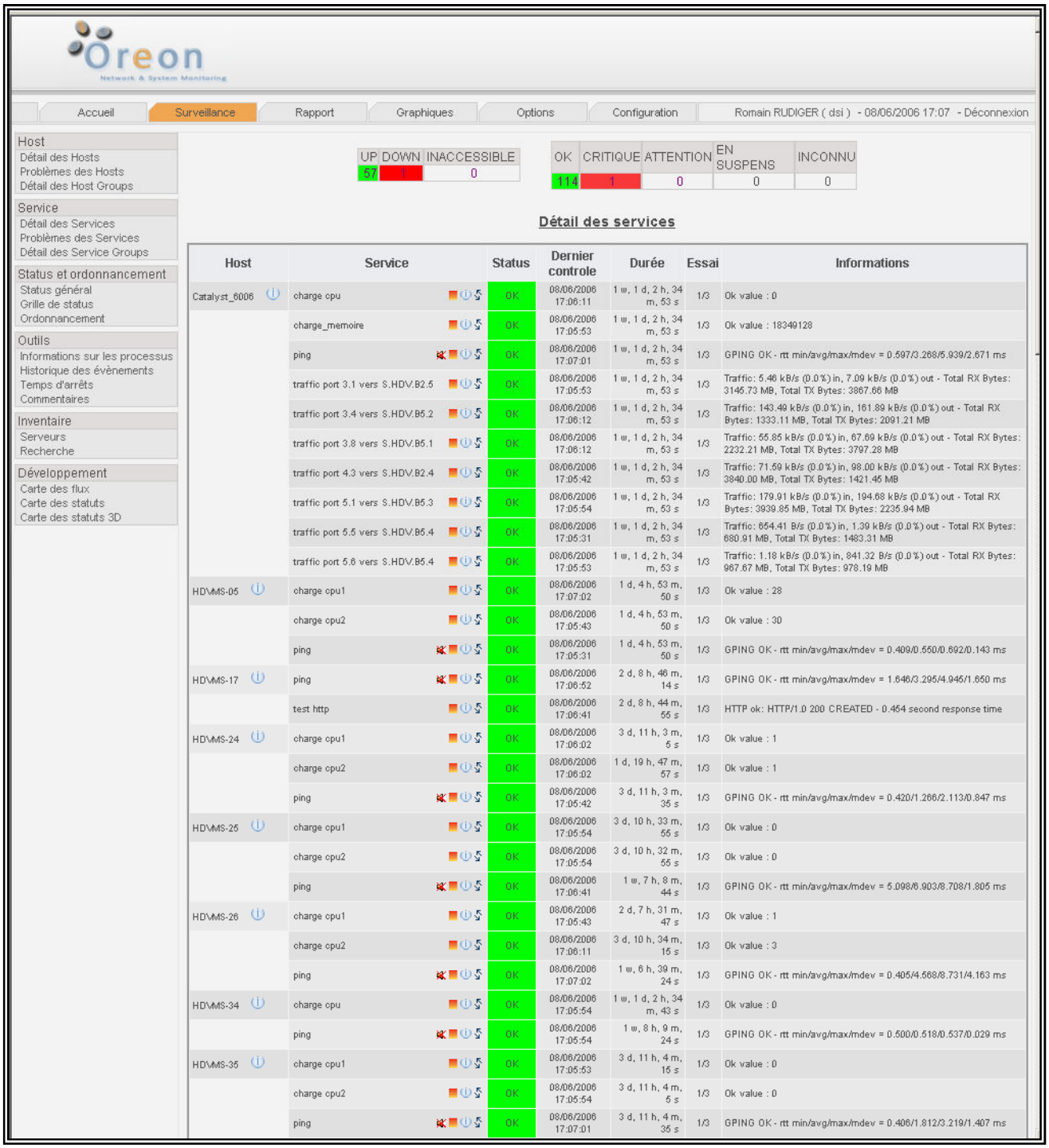
On voit bien ici qu'un site distant relié par une liaison ADSL ne répond plus, un clique sur l'un des graphiques nous enverra sur la page résumant l'état du réseau.

7.2.2. Le résumé des statuts



On retrouve donc sur le résumé de l'état du réseau, l'équipement qui ne répond plus.

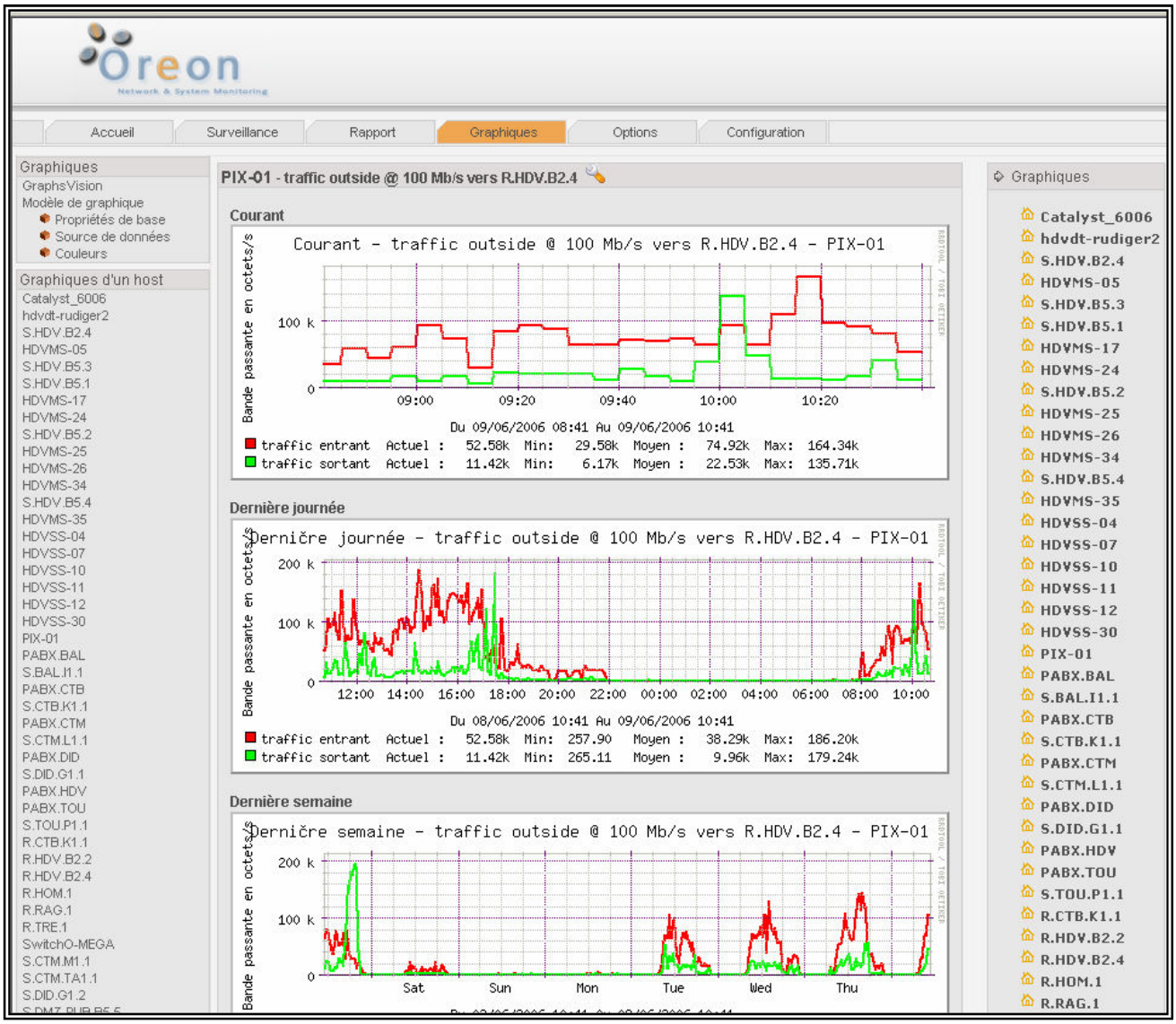
7.2.3. Les détails des services



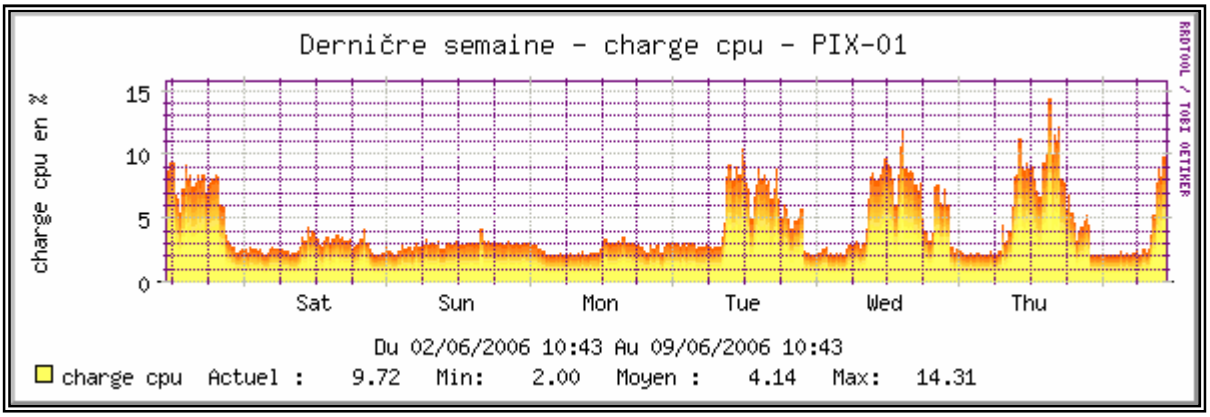
Détail des services, avec : la durée depuis laquelle l'état du service n'a pas changé, la date de la dernière vérification, la réponse du plugin, un accès direct aux graphiques, à la configuration de l'équipement, des services…

7.2.4. Les graphiques

Voici les graphique correspondant au trafic entre le pare feu et le routeur de sortie Internet :

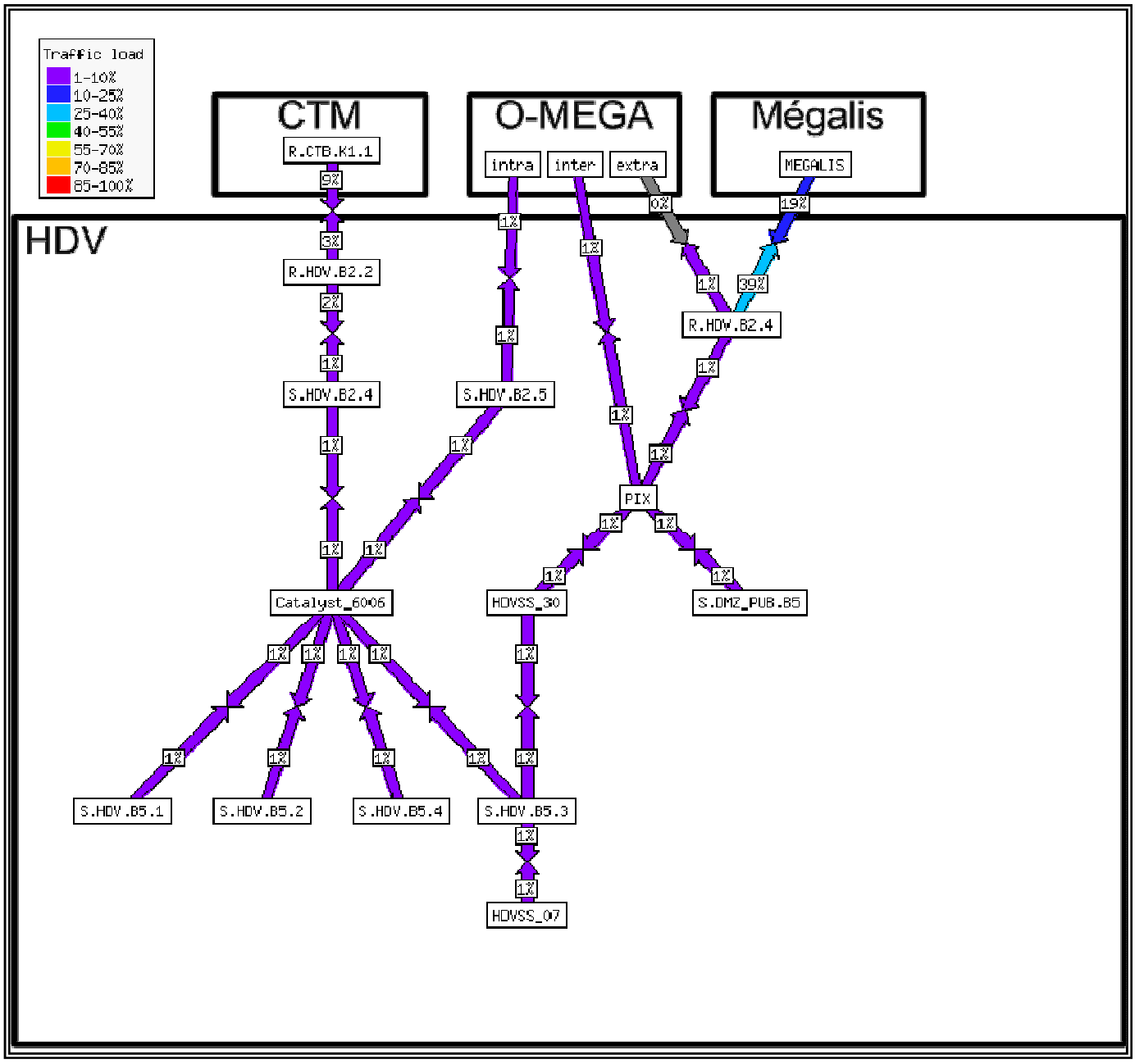


Voici maintenant la charge processeur du pare feu sur les sept derniers jours :



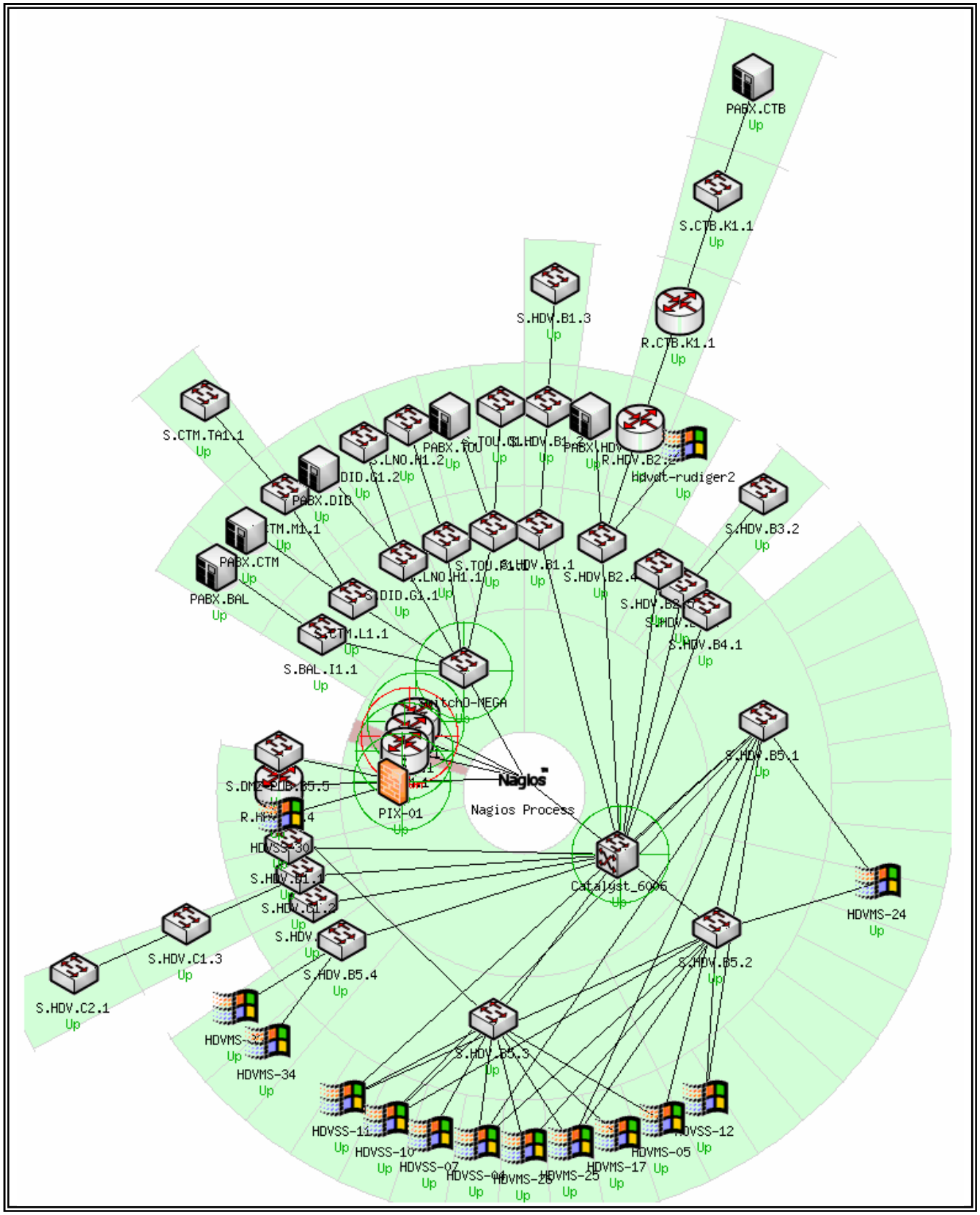
Une relation entre le trafic et la charge processeur est clairement visible, le pare feu semble bien dimensionné.

7.2.5. La carte des flux



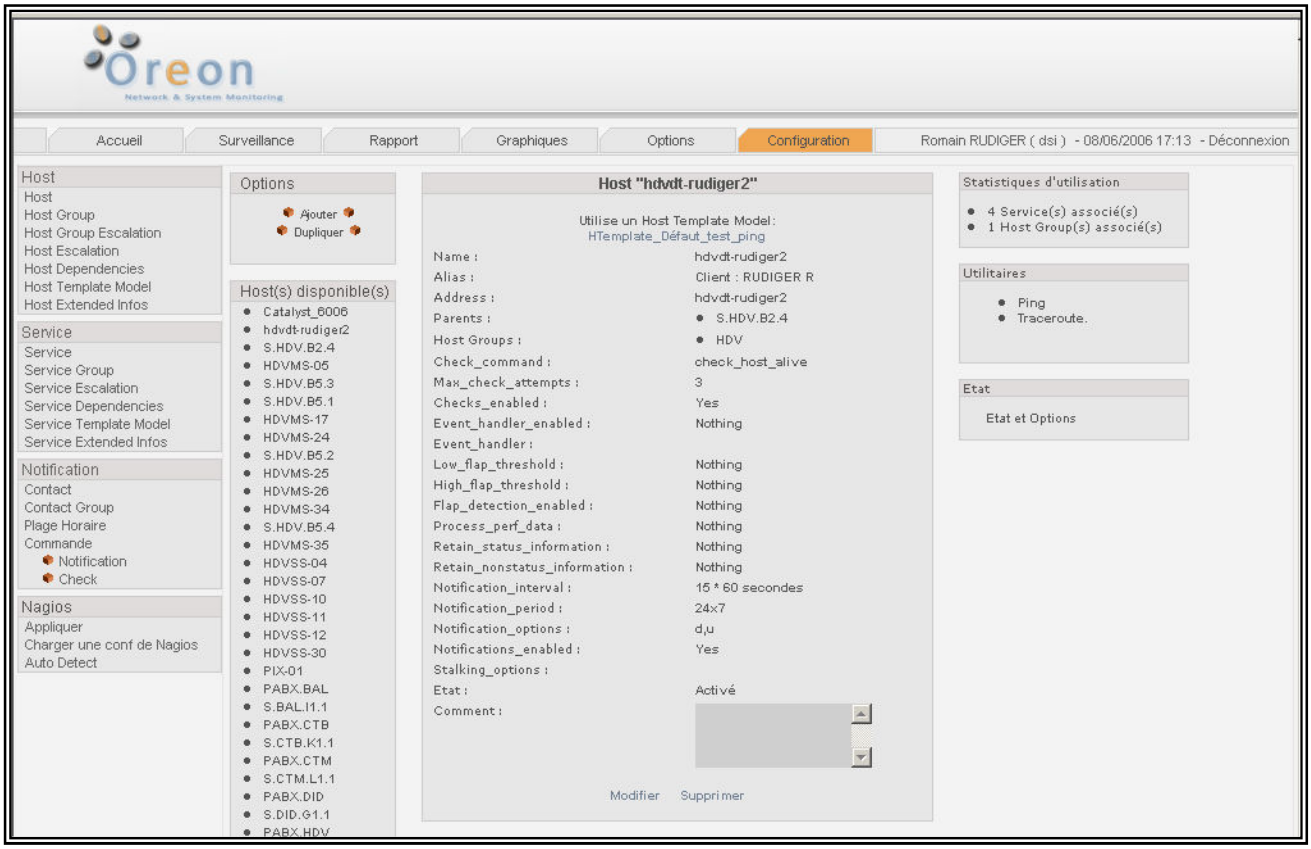
Tous les utilisateurs sont dirigés sur la sortie internet de Mégalis, celle-ci sature à certains moments de la journée.
CTM correspond au site distant relié par une liaison spécialisé France Telecom en 2 Mo.
Tous les autres liens semblent surdimensionnés sauf lors des sauvegardes puisque les interfaces réseaux des serveurs et du NAS ont un débit de 100 Mbits/s et forment donc un goulot d'étranglement.

7.2.6. La carte des statuts



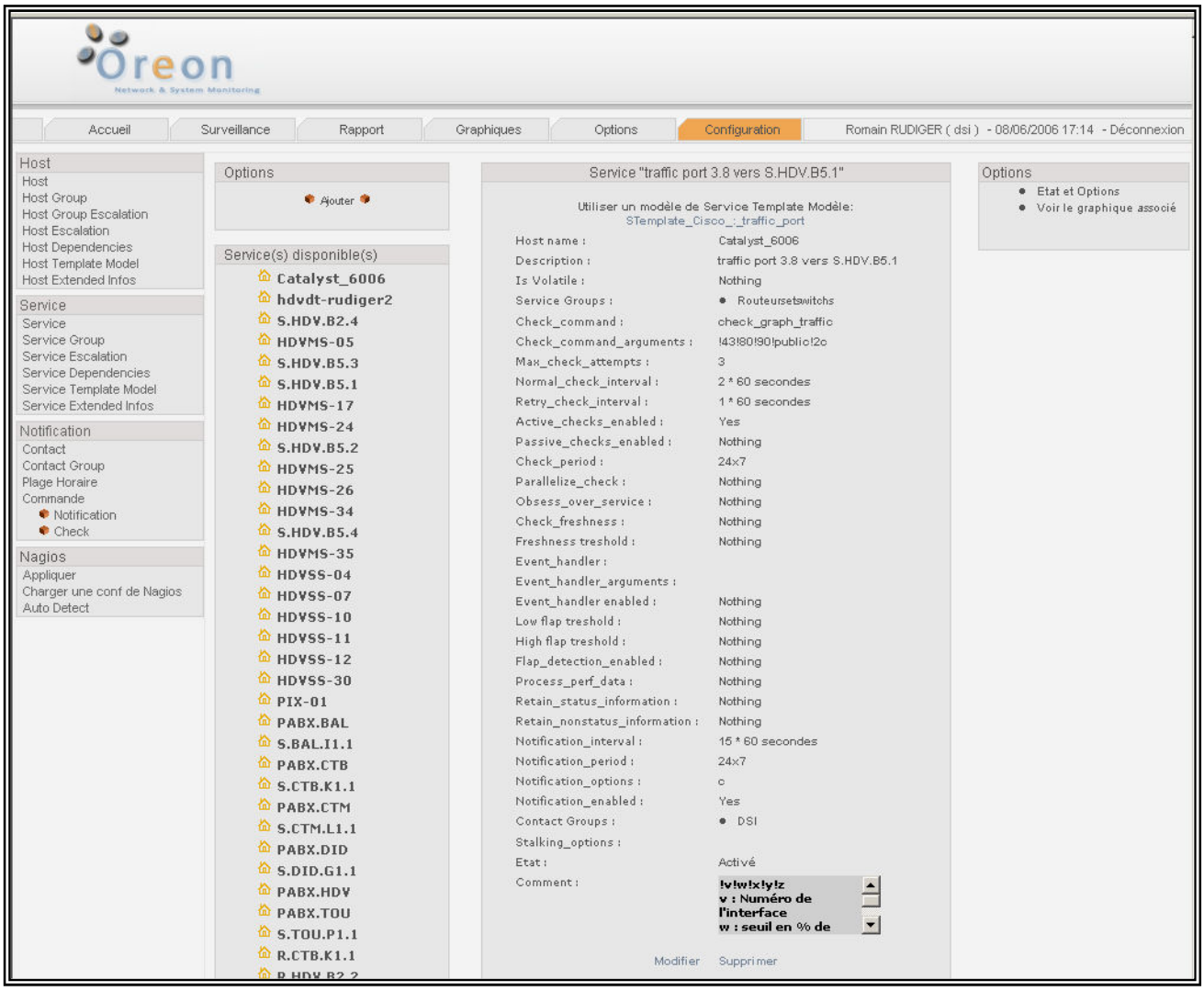
On retrouve le routeur ADSL du site distant qui ne répond plus.

7.2.7. La configuration d'un équipement



Ici la configuration de mon poste de travail, je n'ai pas mis l'adresse IP mais le nom net bios, on peut voir que cette équipement est configuré par un model : le Template Défaut_test_ping. Une vérification par ping est faite, si au bout de 3 vérifications, l'équipement ne répond pas, une notification est envoyée 24 heures sur 24 et 7jours sur 7.

7.2.8. La configuration d'un service



Voici la configuration d'un service, ce service est attribué au commutateur/routeur en fibre optique qui est le cœur du réseau. Ici aussi un Template a été utilisé, il s'agit d'un relevé du trafic sur le port 43 (quatrième carte 4 et troisième port).

Le plugin utilisé est : check_graph_traffic, il s'appuit sur le protocole SNMP, voici les arguments envoyé au plugin lors d'une vérification :

!43!80!90!public!2c

Les arguments sont séparés par un point d'exclamation, le premier correspond au numéro de port, le second au seuil de déclenchement de l'état Warning (attention) à 80 % d'utilisation de la bande passante, le suivant au seuil Critique à 90%, la communauté SNMP et la version utilisée par le client.

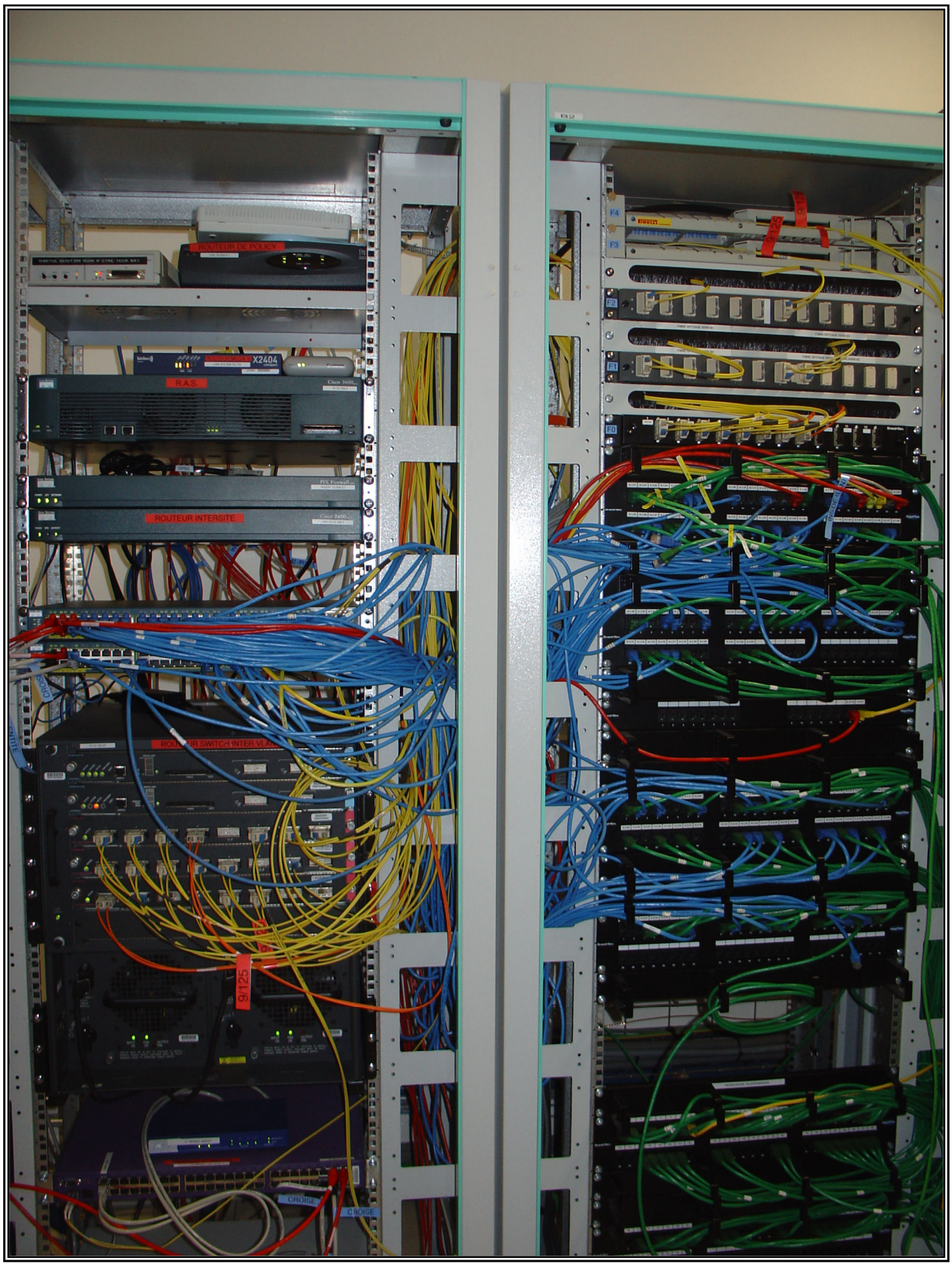
Le nom du service porte le mot « trafic » pour pouvoir utiliser les valeurs dans la carte des flux.

7.3. Les serveurs de l'hôtel de ville

Voici les trois baies de serveurs présents sur l'hôtel de ville :

7.4. Le cœur du réseau

A gauche les éléments actifs et a droite la baie de brassage avec quatre tiroirs optique.



7.5. La carte du réseau de la Ville de Rezé