

# NOTE DE SYNTHÈSE

---

## MISE EN PLACE ET COMPARAISON DE DEUX OUTILS DE SUPERVISION RESEAU



## **RESEAU AQUITAIN DES UTILISATEURS DES MILIEUX UNIVERSITAIRES ET DE LA RECHERCHE**

# SOMMAIRE

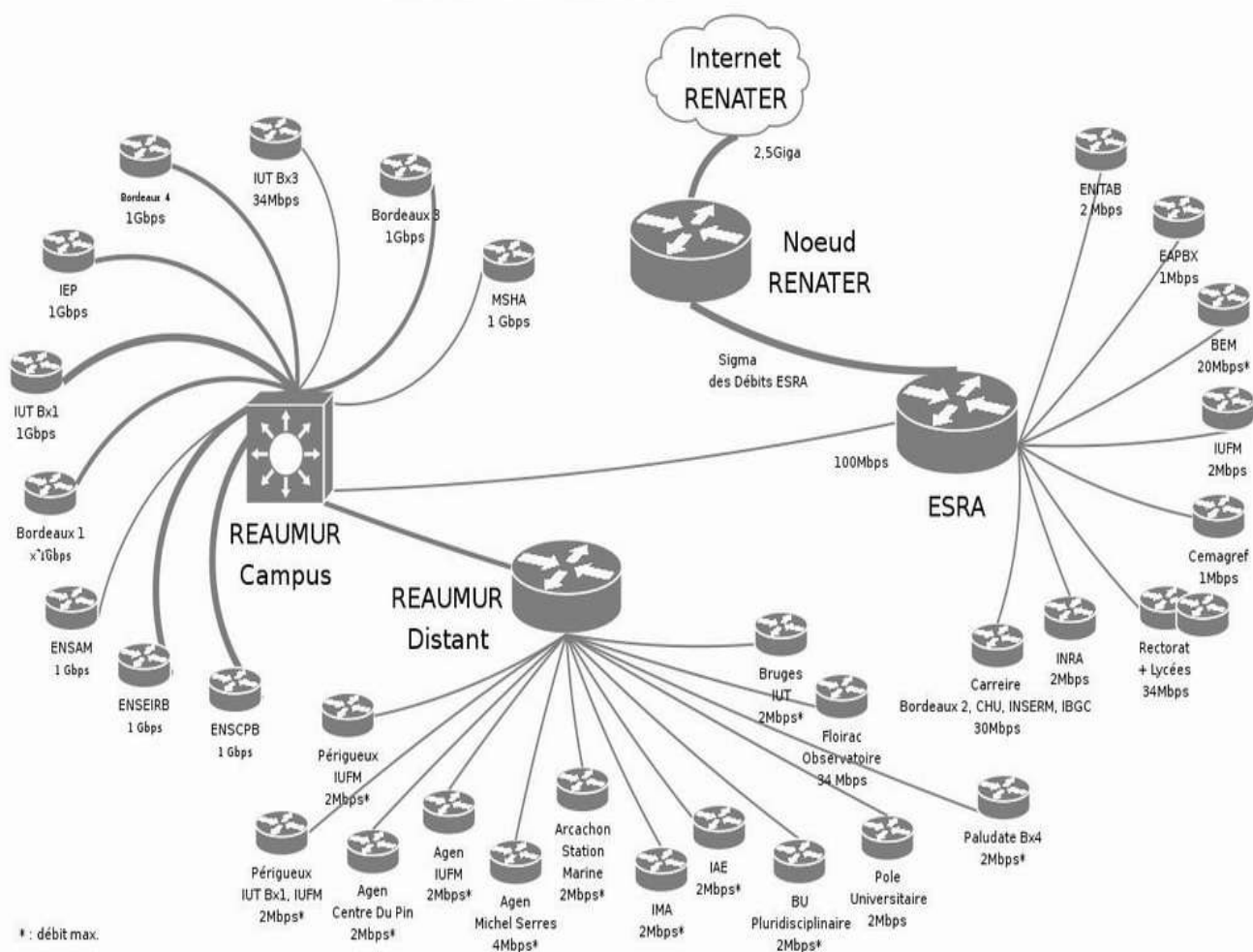
<b><u>1) INTRODUCTION</u></b> .....	<b>3</b>
1.1) PRESENTATION DU RESEAU REAUMUR.....	3
1.2) L'ORGANISATION DE REAUMUR.....	4
1.3) LES MISSIONS DE REAUMUR.....	4
1.4) LA SECURITE AU SEIN DE REAUMUR.....	5
<b><u>2) CONTEXTE DU PROJET</u></b> .....	<b>5</b>
2.1) PRESENTATION DU PROJET.....	5
2.2) LES PHASES DU PROJET.....	6
2.3) INTEGRATION DES VLANS.....	6
2.4) CONFIGURATION DE LA MAQUETTE.....	7
2.4.1) CONFIGURATION DU COMMUTATEUR.....	7
2.4.2) CONFIGURATION DU ROUTEUR.....	9
<b><u>3) MISE EN PLACE DES OUTILS DE SUPERVISION : JFFNMS ET CACTI</u></b> .....	<b>10</b>
3.1) PRE REQUIS.....	10
3.1.1) APACHE : LE SERVEUR WEB.....	10
3.1.2) LE PROTOCOLE SNMP.....	11
3.2) INSTALLATION ET PRESENTATION DE JFFNMS .....	12
3.3) INSTALLATION ET PRESENTATION DE CACTI.....	13
<b><u>4) COMPARAISON DES POSSIBILITES DE JFFNMS ET CACTI</u></b> .....	<b>14</b>
4.1) CHOIX DES OPTIONS ET TESTS.....	14
4.2) TESTS EFFECTUES.....	15
4.3) BILAN COMPARATIF.....	21
<b><u>5) CONCLUSION</u></b> .....	<b>22</b>

# 1) INTRODUCTION

## 1.1) Présentation du réseau REAUMUR

Version 2.2 - 05/11/04 LF

### Réseau REAUMUR



## 1.2) L'organisation de REAUMUR

L'unité réseau REAUMUR fonctionne sous la responsabilité d'un conseil d'administration qui nomme un directeur.

Les partenaires du campus sont les suivants :

- Université Bordeaux 1 Sciences et Technologies
- Université Victor Ségalen Bordeaux 2, pour le compte des facultés des sciences du sport, d'oenologie, et des services inter universitaires rattachés (SIUAPS, SIUMPPS)
- Université Michel de Montaigne Bordeaux 3
- Université Montesquieu Bordeaux IV, y compris pour le compte du SICOD
- CNRS (Délégation régionale)
- ENSEIRB
- ENSCPB
- IEP
- ENSAM
- Maison des Sciences de l'Homme d'Aquitaine

-

## 1.3) Les missions de REAUMUR

### **Missions pour les partenaires du campus de Talence-Pessac-Gradignan :**

Réaumur est un service interuniversitaire, dont la mission est d'assurer l'exploitation, la gestion et le développement de moyens et de services réseaux communs, dans le cadre des activités scientifiques, pédagogiques, documentaires ou de gestion des différents centres, laboratoires et services des organismes partenaires.

Réaumur fixe notamment les conditions de sécurité d'utilisation, en accord avec les partenaires.

### **Missions pour les partenaires de la plaque régionale ESRA :**

Cette mission de Réaumur (dénommée service de base), consiste à mutualiser les services de connexion à RENATER pour les partenaires régionaux.

Réaumur a également une mission élargie au plan régional, puisqu'il est gestionnaire de la Plaque réseau régionale ESRA pour les établissements d'Enseignement Supérieur et de Recherche en Aquitaine.

Cette mission concerne les partenaires déjà cités auxquels s'ajoutent le Rectorat de Bordeaux, le CEMAGREF, l'EAPBx, l'ENITA de Bordeaux, l'INRA Aquitaine, l'IUFM d'Aquitaine, l'Université de Pau et des Pays de l'Adour, Bordeaux Ecole Management. Ses missions sont coordonnées par la Direction des Ressources Informatiques et Multimédia Mutualisées (DRIMM).

## 1.4) La sécurité au sein de REAUMUR

Dès le départ l'aspect sécurité a été pris en compte. La mise en place d'un groupe sécurité du comité technique, lors de la création de REAUMUR l'atteste. Ses conclusions ont entraîné:

- la séparation physique des réseaux de gestion par rapport aux autres réseaux.
- la rédaction d'une charte REAUMUR dont chaque utilisateur d'une machine en réseau doit prendre connaissance, et d'un engagement de sécurité signé par ces mêmes utilisateurs.

REAUMUR mène donc des actions de sensibilisation auprès des responsables d'organismes. Ainsi, le traitement d'un incident se fait en concertation avec le correspondant sécurité du service, du directeur de ce service et du responsable de l'établissement, en fonction de la gravité de l'incident.

## **2) CONTEXTE DU PROJET**

### 2.1) Présentation du projet

REAUMUR mène une politique visant à n'utiliser spécifiquement que des logiciels libres. Un logiciel libre n'est pas seulement un logiciel gratuit mais aussi un logiciel dont on peut modifier les sources librement à son gré afin d'en améliorer les performances.

Toutes les machines, au sein du réseau REAUMUR servant à assurer les services de base du réseau, sont dotées du système d'exploitation Linux.

REAUMUR dessert de nombreux pôles universitaires et de recherche en s'occupant de l'interconnexion de ces différents réseaux. Il faut donc expressément que leurs méthodes soient correctes afin de fournir des services de qualité à leurs partenaires.

Il faut aussi répondre à ce besoin de qualité de services fournis, en aménageant des outils de supervision réseau, pouvant aider à une administration plus facile et optimisée du réseau.

REAUMUR dispose déjà d'un outil de supervision réseau : NAGIOS. Cependant les utilisateurs de ce logiciel veulent mettre en place une application extérieure qui sera capable, par le biais de requêtes, d'extraire les données fournies par l'outil de supervision réseau.

De plus, suite à un désir de veille technologique ils sont en constante recherche de nouveaux produits et veulent effectuer des essais.

Les utilisateurs du logiciel cherchent donc à savoir et à tester quelles sont les autres possibilités existant sur le marché pouvant éventuellement palier à certains manques. Il m'a donc été suggéré de tester deux outils de supervision réseau : JFFNMS et CACTI.

Le logiciel retenu devra avoir la faculté d'être facilement exploitable. Ceci entend que la base de données devra être accessible de n'importe quelle autre application pour pouvoir en extraire les données. Par exemple, les graphes générés par ces outils de supervision réseau doivent être facilement récupérables par une URL explicite par exemple.

Ces logiciels sont libres, leur installation et leur configuration ont été effectuées après la mise en place d'une maquette réseau.

Les tests effectués devront servir par la suite au possible futur choix d'un outil de supervision pouvant aboutir à ces nouveaux objectifs.

## 2.2) Les phases du projet

Tout d'abord, mise en place de la maquette réseau est nécessaire.

Ensuite, la tâche à effectuer est l'installation et la configuration des outils JFFNMS et CACTI.

Enfin, la dernière procédure est de mettre en place des tests pouvant aider à la comparaison de ces deux outils de supervision.

Un routeur CISCO 2620, un commutateur CISCO Catalyst 2950 ainsi qu'un poste de travail (Linux) et un portable (Windows) m'ont donc été confiés.

Sur le poste de travail, l'installation de Linux a dû être effectuée. La version de l'entreprise est Debian Sarge Testing.

### 2.3) L'intégration des VLANS

Le réseau REAUMUR est essentiellement constitué de Vlan (Virtual Local Area Network) afin d'améliorer la sécurité en limitant la circulation des trames, et les performances en limitant l'étendue des diffusions au réseau virtuel d'appartenance. Les broadcast (trames destinées à toutes les machines du réseau) diminuant les performances au sein des réseaux.

Il m'a donc semblé pertinent de mettre en place sur cette maquette des VLANS (Virtual Local Area Network) afin de rendre compte, du mieux possible, de l'organisation du réseau REAUMUR.

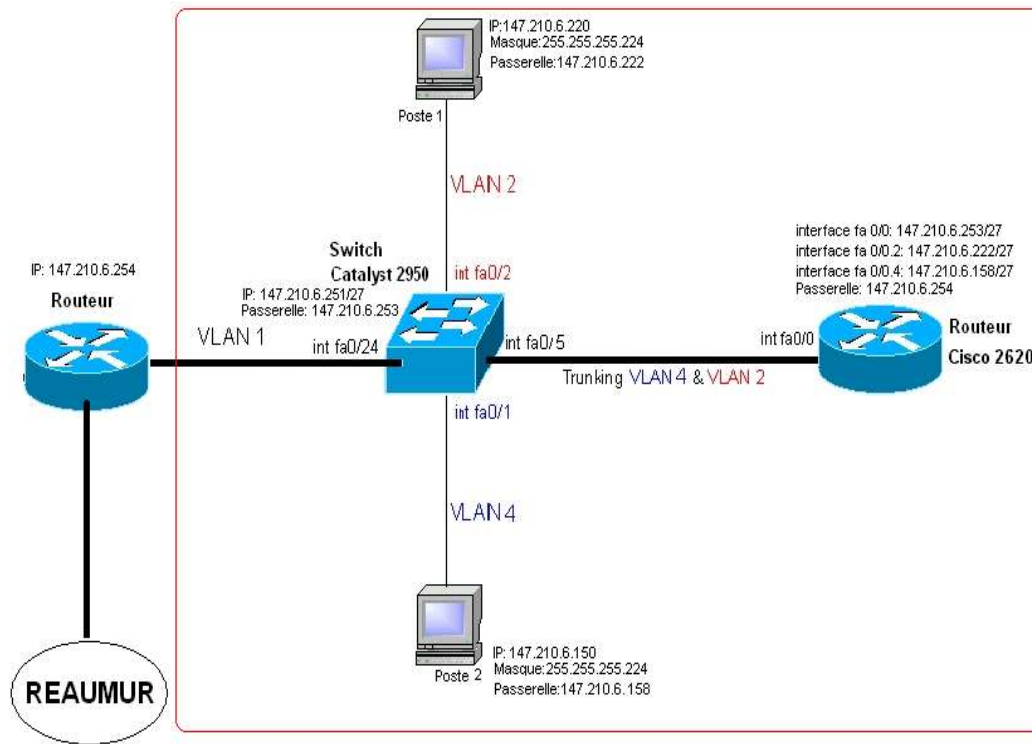
Chaque Vlan peut être considéré comme un réseau de niveau 2 (Liaison) construit à partir d'une technologie permettant de cloisonner des réseaux par usage de filtres de sécurité.

Cette technologie balise le domaine de broadcast (diffusion) auquel ces machines appartiennent, de telle sorte que le trafic intra domaine ne puisse pas être vu par des tiers n'appartenant pas à ce domaine de diffusion.

Cela permet d'isoler certains ports du commutateur et de créer ainsi des réseaux indépendants. La sécurité est accrue puisque les trames ne circulent pas entre les différents Vlans.

### 2.4) Configuration de la maquette

Les équipements réseaux m'ont permis d'effectuer la maquette suivante :



Maquette réalisée

On peut remarquer la présence de plusieurs Vlans sur le commutateur.

Pour communiquer entre deux Vlans, il est nécessaire de réaliser un routage de niveau réseau. C'est ce à quoi sert le routeur cisco 2620 dans le schéma ci-dessus.

En effet, suite à la mise en place des Vlans, les postes de travail ne pouvaient plus communiquer entre eux (car ils appartiennent à des Vlans différents).

### 2.4.1) CONFIGURATION DU COMMUNICATEUR

La configuration du commutateur s'est faite de la manière suivante grâce à l'émulateur de terminal minicom lancé en mode console (c'est-à-dire sans interface graphique):



```

switch#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
switch(config)#int vlan 1
switch(config-if)#ip address 147.210.6.251
255.255.255.224
switch(config-if)#exit
switch(config)#ip default-gateway 147.210.6.253
switch(config)#end
switch#vlan database
switch(vlan)#vtp transparent
switch(vlan)#vlan 2
VLAN 2 added:
Name: VLAN0002
switch(vlan)#vlan 4
VLAN 4 added:
Name: VLAN0004
switch(vlan)#exit
APPLY completed.
Exiting...
switch#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
switch(config)#int fastEthernet 0/5
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan all
switch(config-if)#exit
switch(config)#int fastEthernet 0/2
switch(config-if)#switchport access vlan 2
switch(config-if)#spanning-tree portfast
switch(config-if)#exit
switch(config)#int fastEthernet 0/1
switch(config-if)#switchport access vlan 4
switch(config-if)#spanning-tree portfast
switch(config-if)#exit
switch#write memory

```

```

// On entre dans le mode configuration
// On configure le vlan1 qui est le vlan par défaut
// On donne l'adresse du routeur comme passerelle
par défaut
// On entre dans la base données des Vlans
// On ne configure pas le VTP:Vlan Trunking Protocol
// On crée le Vlan 2
//On crée le Vlan 4
// On configure l'interface 0/5
// Le mode trunk est défini pour cet interface
// Tous les Vlans peuvent transiter à travers le
port trunk
// On configure l'interface 0/2
// On affecte le vlan 2 à cet interface
// le dispositif portfast est affecté à l'interface
// On configure l'interface 0/1
// On affecte le Vlan 4 à cet interface
// Le dispositif portfast est affecté à cet
interface
// On enregistre la configuration

```

### - LE « VLAN-TRUNKING »

L'interface 0/5 du commutateur est en mode « trunk » car c'est sur cette interface que le routeur est relié. En effet, pour assurer le routage entre les deux Vlans, on doit définir un « trunk » qui permettra de transporter des informations de plusieurs Vlans.

Ce mécanisme d'encapsulation de trames Ethernet est appelé « *VLAN-Trunking* » et fonctionne de la manière suivante :

-Lorsqu'une trame Ethernet est reçue sur l'un des ports du commutateur, celui-ci la retransmet telle quelle sur tous les ports en mode « *access* » affectés au même Vlan, et la retransmet également en l'encapsulant au préalable dans une trame spéciale (trame 802.1Q) sur le trunk.

-Lorsqu'une trame spéciale encapsulant une trame Ethernet est reçue sur un port configuré en mode « *trunk* », le commutateur retransmet la trame décapsulée sur tous les ports

en mode « *access* » affectés au même Vlan et retransmet la trame spéciale telle quelle sur les autres ports en mode « *trunk* ».

## 2.4.2) CONFIGURATION DU ROUTEUR

La configuration du routeur n'a pas pu être effectuée de suite car l'IOS (Internetwork Operating System), c'est-à-dire le système d'exploitation du routeur, n'était pas présent. Le téléchargement de cet IOS a donc dû être effectué par une suite de commandes passées grâce à minicom .Il était indispensable de télécharger l'IOS par l'intermédiaire d'un serveur TFTP.

### *-LE PROTOCOLE TFTP*

Le TFTP (Trivial File Transfert Protocole) utilise le protocole UDP. C'est une version du protocole FTP destinée à l'échange de fichiers. Le protocole TFTP ne permet pas l'utilisation d'un répertoire utilisateur, ni celle d'un mot de passe garantissant une certaine protection. On utilise le protocole TFTP notamment pour amorcer des stations de travail sans disque dur.

Pour recevoir le fichier image du serveur TFTP, il faut au préalable le télécharger sur le site de cisco et l'enregistrer sur le serveur TFTP. Une fois ceci réalisé, on peut passer les commandes suivantes :

```
rommon 1 > IP_ADDRESS=147.210.6.253 // Adresse du routeur qui va recevoir l'IOS
rommon 2 > IP_SUBNET_MASK=255.255.255.224 // Masque de sous-réseau du routeur
rommon 3 > DEFAULT_GATEWAY=147.210.6.254 // Passerelle par défaut
rommon 4 > TFTP_SERVER=147.210.x.y // Adresse du serveur TFTP
rommon 5 > TFTP_FILE=julien/c2600-is-mz.121-26.bin // Nom du fichier à télécharger à partir du serveur
rommon 6 > tftpdnld // Commande d'exécution du téléchargement

!-- Voici ce qui apparaît à l'écran :
IP_ADDRESS: 147.210.6.253
IP_SUBNET_MASK: 255.255.255.224
DEFAULT_GATEWAY: 147.210.6.254
TFTP_SERVER: 147.210.x.y
TFTP_FILE: julien/c2600-is-mz.121-26.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on
flash will be lost!
Do you wish to continue? y/n: [n]: y
Receiving julien/c2600-is-mz.121-26.bin from
147.210.x.y!!!!!!
File reception completed.
Copying file c2600-is-mz.121-26.bin to flash.
Erasing flash at 0x607c0000
program flash location 0x60440000
```

## -LA CONFIGURATION DU ROUTEUR

La configuration du routeur s'est effectuée de la manière suivante (toujours grâce à minicom) :

```
routeur#configure terminal // On entre dans le mode configuration
Enter configuration commands, one per line. End with
CNTRL/Z. // On définit la passerelle par défaut
routeur(config)#ip default-gateway 147.210.6.254
routeur(config)#ip route 0.0.0.0 0.0.0.0
147.210.6.254 // On configure l'interface 0/0
routeur(config)#int fastEthernet 0/0 // Désactive l'arrêt de l'interface
routeur(config-if)#no shut // Adresse IP et masque de sous-réseau de
routeur(config-if)#ip address 147.210.6.253 l'interface 0/0
255.255.255.224 // On configure l'interface virtuelle 0/0.2
routeur(config-if)#exit // On choisit le mode d'encapsulation des trames
routeur(config)#int fastEthernet 0/0.2 // Adresse IP et masque de sous-réseau de
routeur(config-subif)#encapsulation dot1Q 2 l'interface 0/0.2
routeur(config-subif)#ip address 147.210.6.222
255.255.255.224 // On configure l'interface virtuelle 0/0.4
routeur(config-subif)#ip broadcast-address 0.0.0.0 // On choisit le mode d'encapsulation des trames
routeur(config-subif)#exit // Adresse IP et masque de sous-réseau de
routeur(config)#int fastEthernet 0/0.4 l'interface 0/0.4
routeur(config-subif)#encapsulation dot1Q 4
routeur(config-subif)#ip address 147.210.6.158
255.255.255.224 // Enregistrement de la configuration
routeur(config-subif)#ip broadcast-address 0.0.0.0
routeur(config-subif)#exit
routeur#write memory
```

## 3) MISE EN PLACE DES OUTILS DE SUPERVISION RESEAU : JFFNMS ET CACTI

### 3.1) Pré requis

Un outil de supervision réseau est une plateforme d'administration des systèmes et des applications, qui est un ensemble de programmes gérés par un logiciel dont le rôle est de :

- dialoguer avec les équipements réseaux,
- recevoir et de traiter les évènements en provenance des équipements réseaux,
- centraliser les évènements SNMP ou non SNMP,
- générer des rapports graphiques.

L'objectif d'un outil de supervision réseau est triple : prévenir les incidents par extrapolation des données fournies, agir rapidement dès qu'un système est noté en erreur, permettre l'analyse "post mortem" d'un problème grâce aux informations collectées.

La contrainte principale d'un outil de supervision est la consommation des ressources. Les administrateurs doivent souvent réduire le nombre de paramètres surveillés afin qu'il n'y ait pas d'impacts sur les applications.

### 3.1.1) Apache : le serveur WEB

Ces deux outils de supervision réseau nécessitent une interface web pour pouvoir être utilisés. Il faut donc installer un serveur web, c'est-à-dire un logiciel permettant à des clients d'accéder à des pages web, à partir d'un navigateur installé sur un ordinateur distant. Le serveur le plus répandu étant APACHE.

De plus, un utilisateur de Apache doit être mis en place. Cet utilisateur pourra utiliser Apache. Dans ce cas-ci, il s'agit de l'utilisateur : www-data qui est mis en place, cependant on peut tout à fait en changer le nom.

### 3.1.2) Le protocole SNMP

Des informations bien spécifiques peuvent être obtenues (occupation des disques, utilisation de la bande passante,...) au moyen du protocole SNMP décrit ci-dessous.

SNMP (Simple Network Management System) est un protocole d'administration de machines supportant TCP/IP. Il a été développé pour permettre à l'administrateur du réseau d'interroger les éléments de son réseau sans avoir à se déplacer. Il permet de répondre à un grand nombre de besoins :

- Disposer d'une cartographie du réseau
- Fournir un inventaire précis de chaque machine
- Mesurer la consommation système d'une application
- Signaler les dysfonctionnements

Une administration SNMP est composée de trois types d'éléments :

**Un agent :** chaque équipement que l'on voudra manager à distance devra disposer d'un agent SNMP. Cet agent est un serveur, c'est-à-dire qu'il reste à l'écoute d'un port particulier: **le port UDP 161**.

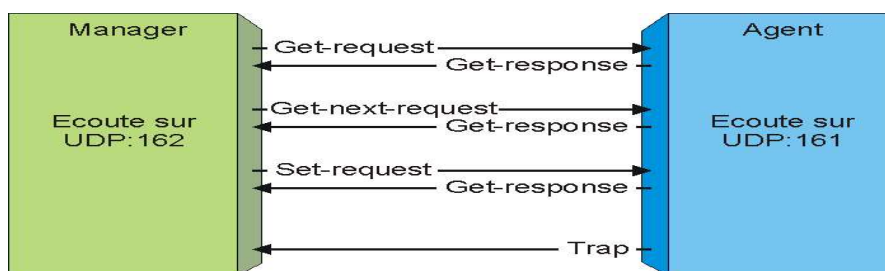
La principale fonction de cet agent est de rester à l'écoute des éventuelles requêtes que l'administrateur lui enverra. Il répondra si la requête est émise par une entité autorisée.

L'agent devra également éventuellement agir sur l'environnement local, si l'administrateur souhaite modifier un paramètre.

Par ailleurs, l'agent SNMP pourra éventuellement émettre des alertes de sa propre initiative. Il peut y avoir une multitude d'alertes possibles suivant la complexité de l'agent : température du processeur, taux d'occupation des disques durs, taux d'occupation CPU...

**Un manager :** c'est avant tout un client, dans la mesure où c'est lui qui envoient des requêtes aux divers agents SNMP du réseau. Il doit aussi disposer d'une fonction serveur car il doit rester à l'écoute sur **le port UDP 162** des alertes ou « traps » que les divers équipements sont susceptibles d'émettre à tout moment.

**Une MIB :** (Management Information Base) décrivant les informations gérées. Elle se présente comme une base de données normalisée qui permet de lire et d'écrire sur les équipements distants et est organisée hiérarchiquement.



Un agent SNMP est plus ou moins finement paramétrable, suivant le système. Il est possible, par exemple de créer des groupes de sécurité qui auront accès en lecture seule, d'autres en lecture/écriture, d'autres encore en lecture seule, mais sur certaines branches seulement.

Chaque groupe devra disposer d'une sorte de mot de passe, appelé "community". En général, la communauté "public" est celle qui a le droit de lecture sur les informations non sensibles.

Les communautés doivent tout aussi bien être configurées sur JFFNMS et CACTI que sur les équipements réseaux où l'agent SNMP est installé.

## 3.2) Installation et présentation de JFFNMS

JFFNMS (« Just For Fun Network Management System ») est un outil de supervision. Il permet d'être informé sur des éléments d'un réseau (routeurs, commutateurs, serveurs, ...) en temps réel, ainsi que d'avoir une vision globale sur de plus longues périodes (jours, semaines, mois, années).

La version de Linux utilisée est Debian, celle de jffnms est la 0.7.9. Suivant les versions de linux et de jffnms, la configuration diffère notamment sur l'emplacement des scripts de configuration et les commandes à affecter à ces scripts.

JFFNMS fonctionne grâce à une base de données qui peut être soit MySQL, soit PostgreSQL. La version choisie est MySQL car c'est la plus utilisée. Cette base de données est configurée et rendue accessible grâce à un utilisateur et un mot de passe.

Un groupe d'utilisateurs doit aussi être créé pour les « cron jobs ». Les « cron jobs » désignent l'ensemble des tâches à réaliser. Sans cela aucune statistique ne pourrait être collectée et aucun état ne pourrait être mis à jour. Un utilisateur doit être affecté à ce groupe. En effet, il est nécessaire dans JFFNMS de renseigner cet utilisateur. Cet utilisateur doit être un utilisateur de Apache (www-data comme défini précédemment).

Quant au répertoire où est installé JFFNMS, il faut lui affecter des droits de lecture/écriture. En effet, ceci permet à l'utilisateur de pouvoir collecter des informations de les modifier ou d'en ajouter.

Des alertes peuvent être générées par les équipements réseaux sous surveillance. Ces alertes peuvent être paramétrables, c'est-à-dire que l'on peut définir des conditions sous lesquelles l'alerte sera rapportée ou non.

La collecte d'informations à long terme, ainsi que l'affichage s'effectuent au moyen d'un outil complémentaire ou plugin nommé RRDTOOL : il stocke des informations dans une base de données de manière cyclique et génère les graphiques à l'aide de celle-ci.

Cet outil est composé des bibliothèques php et mysql. Le stockage des informations au sein de RRDTOOL s'effectue donc grâce au téléchargement des bibliothèques php et mysql ainsi que celles qui y sont rattachées.

Le téléchargement de JFFNMS nous fournit uniquement le programme source. Il n'y a pas de fichiers exécutables mais seulement des fichiers à configurer puis à compiler.

Il est possible de définir dans la configuration de JFFNMS des utilisateurs ayant des droits bien spécifiques. Ces droits donnant la possibilité ou non pour certains utilisateurs d'afficher certaines informations sur les équipements réseaux.

JFFNMS utilise un vocabulaire bien spécifique. Il faut donc tout d'abord comprendre la logique des notions afin de bien comprendre son fonctionnement.

En effet, nous pouvons configurer ce que le logiciel nomme « hosts », « interfaces », « zones », « users », « customers ».

Les « hosts » ou hôtes désignent les équipements eux-mêmes, par exemple un routeur. C'est essentiellement ce qui possède une adresse IP. Un hôte possède au moins une interface.

Les interfaces ne désignent quant à eux pas seulement des interfaces physiques qui connectent un hôte au réseau. Ils incluent aussi des services et/ou démons assignés à un numéro de port ou encore à des paramètres SNMP.

Les zones regroupent les hôtes et désignent donc un lieu géographique dans la majeure partie des cas.

On distingue trois niveaux d'accès à JFFNMS.

Les administrateurs sont, tout d'abord, capable d'ajouter des « users » ou utilisateurs, de modifier des interfaces, etc. Pour être administrateur, il suffit d'être un utilisateur ayant tous les droits.

Les utilisateurs ont la possibilité d'utiliser cet outil de supervision et non pas de modifier la configuration. Ce sont eux ayant le moins de droits pour utiliser le logiciel.

Les « customers » ou clients sont des personnes possédant ou utilisant un service (ce qui est appelé interfaces pour JFFNMS). Il est indispensable de créer au moins un client pour que les autres objets aient une appartenance.

### 3.3) Installation et présentation de CACTI

Tout comme JFFNMS, CACTI doit être configuré puis compilé pour qu'il puisse fonctionner.

Il est aussi nécessaire de créer la base de données MySQL avec un utilisateur et un mot de passe pour cette base.

De plus, certains dossiers se doivent aussi d'avoir des autorisations d'accès spéciales pour l'utilisateur de la base. C'est notamment le cas pour les dossiers /var et /log qui concernent respectivement les graphes et les logs.

CACTI s'appuie lui aussi sur RRDTOOL afin de stocker les informations nécessaires pour créer des graphiques et pour leur affecter des données dans une base de données MySQL.

CACTI exploite alors les données en plusieurs phases par l'intermédiaire de modèles que l'on peut appliquer aux données, aux graphes ou aux hôtes. Ceux-ci permettent de rassembler les objets (serveurs, données, graphiques) présentant des caractéristiques communes afin de les gérer de manière centralisée. Ce système de gestion va permettre de remanier facilement les graphiques créés afin d'y faire apparaître les informations les plus pertinentes.

Lors de la première utilisation de CACTI, il est nécessaire de créer ce qui est appelé ici un serveur (cela peut être n'importe quel équipement réseau) afin de pouvoir par la suite créer les graphes souhaités grâce aux données récupérées. Il existe déjà des modèles pré configurés pour la surveillance de serveurs spécifiques (routeur Cisco, Windows 2000, Linux).

Cependant, il est aussi possible de créer ses propres modèles que ça soit pour les serveurs, les graphes et les données à récupérer.

Ainsi, il est possible de visualiser des graphismes RRDTOOLS selon des critères de périodicité, et des critères d'origine des données.

De plus, l'utilisateur peut définir des requêtes de données par le biais d'un script personnalisé ou d'une méthode implémentée dans les agents SNMP.

CACTI propose aussi une gestion par utilisateur. Ainsi, on peut créer des utilisateurs et leurs donner des droits d'accès à certains secteurs de CACTI. Par exemple, un utilisateur peut avoir la possibilité de changer les paramètres d'un graphique alors qu'un autre aura seulement la possibilité de le visualiser.

#### **4) COMPARAISON DES POSSIBILITES DE JFFNMS ET CACTI**



## 4.1) Choix des options et tests

Pour effectuer une comparaison entre ces deux outils, il paraît nécessaire au préalable de faire un inventaire des critères de comparaison, qui vont permettre de mettre en évidence les avantages et les inconvénients de chacun des outils.

Les critères pour JFFNMS sont donc les suivants :

- Ergonomie (Interface graphique conviviale, visibilité des éléments à superviser)
- Facilité du paramétrage, de la prise en main
- Les différents objets observés (Interfaces, processus, CPU,...)
- Prise en compte de nouveaux équipements sur le réseau
- Alertes (L'utilisateur est-il alerté ? Comment est-il alerté ?)
- Configuration d'un seuil d'alerte
- Possibilité de filtres
- Evolutivité
- Gestion des logs (fichier journal)
- Possibilité de « looking glass » (Peut-on ajouter une API/ WEB pouvant extraire les données de la base de données du logiciel ?)

Les critères choisis pour CACTI sont les suivants :

- Ergonomie (Interface graphique conviviale, visibilité des éléments à superviser)
- Facilité du paramétrage, de la prise en main
- Les différents objets observés (Interfaces, processus, CPU,...)
- Prise en compte de nouveaux équipements sur le réseau
- Possibilité de filtres
- Modèles
- Possibilité de « looking glass » (Peut-on ajouter une API/ WEB pouvant extraire les données de la base de données du logiciel ?)

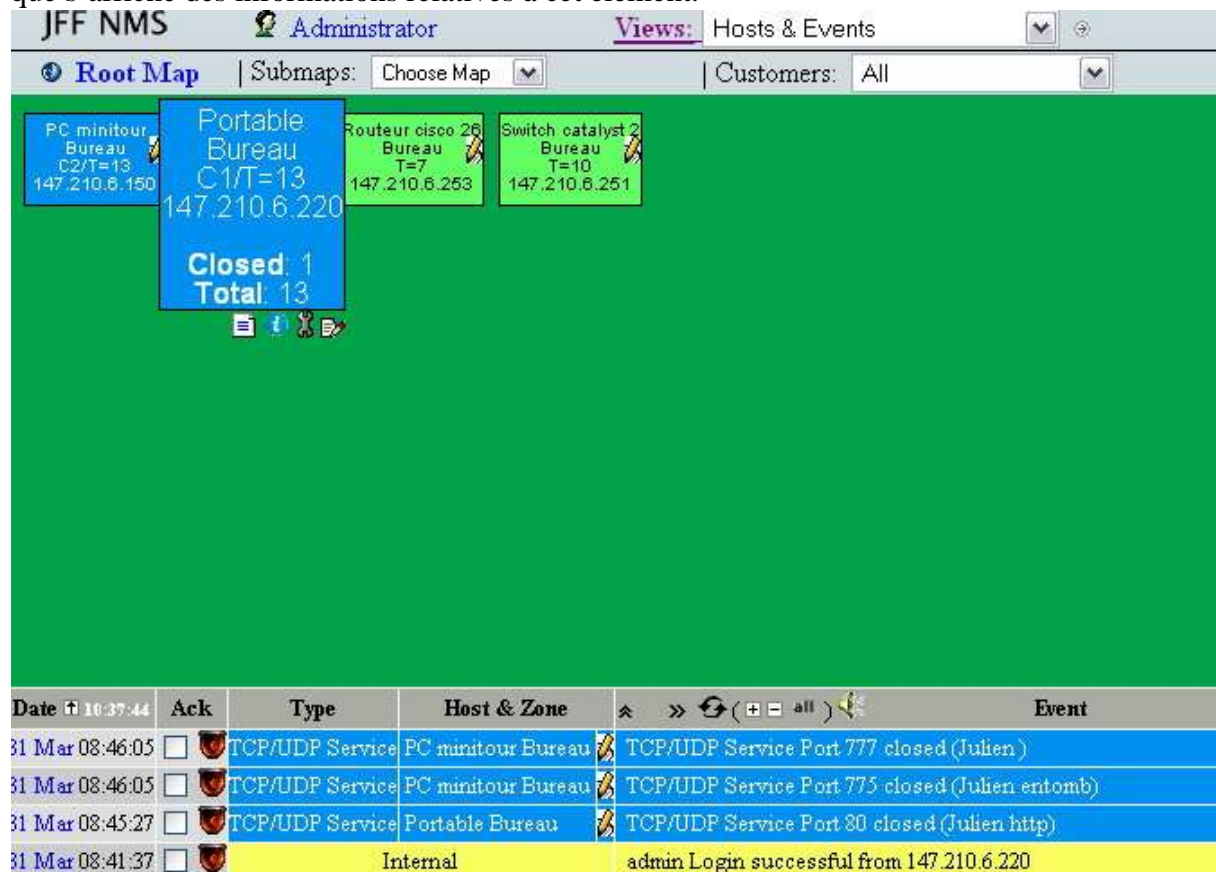
## 4.2) Tests effectués

### **JFFNMS :**

#### -Ergonomie

L'administration globale est simplifiée grâce à l'interface graphique conviviale qui donne une bonne perception de l'état des hôtes ou interfaces que l'on veut observer. Des couleurs mettent bien en évidence les évènements importants. De plus, un système de pop-up permet de voir rapidement les informations souhaitées sur tel ou tel équipement.

Le système de pop-up signifie que l'on a juste besoin de passer la souris sur un élément pour que s'affiche des informations relatives à cet élément.



The screenshot displays the JFF NMS interface. At the top, it shows the user 'Administrator' and the current view 'Hosts & Events'. Below this, there's a 'Root Map' section with a 'Submaps' dropdown set to 'Choose Map' and a 'Customers' dropdown set to 'All'. The main area is a green network map with several nodes: 'PC minitour Bureau C2/T=13' (IP 147.210.6.150), 'Portable Bureau C1/T=13' (IP 147.210.6.220), 'Routeur cisco 26 Bureau T=7' (IP 147.210.6.253), and 'Switch catalyst 2 Bureau T=10' (IP 147.210.6.251). A pop-up window for the 'Portable Bureau' node shows 'Closed: 1' and 'Total: 13'. At the bottom, there's an event log table.

Date	Ack	Type	Host & Zone	Event
31 Mar 08:46:05	<input type="checkbox"/>	TCP/UDP Service	PC minitour Bureau	TCP/UDP Service Port 777 closed (Julien)
31 Mar 08:46:05	<input type="checkbox"/>	TCP/UDP Service	PC minitour Bureau	TCP/UDP Service Port 775 closed (Julien entomb)
31 Mar 08:45:27	<input type="checkbox"/>	TCP/UDP Service	Portable Bureau	TCP/UDP Service Port 80 closed (Julien http)
31 Mar 08:41:37	<input type="checkbox"/>		Internal	admin Login successful from 147.210.6.220

#### -Facilité du paramétrage, prise en main

Le paramétrage est plus ou moins facile selon ce que l'on cherche à faire. Les rubriques de paramétrages ne sont pas très explicites. On ne sait donc pas facilement à quel endroit on paramètre telle ou telle chose. Ceci est le cas en ce qui concerne les seuils d'alertes.

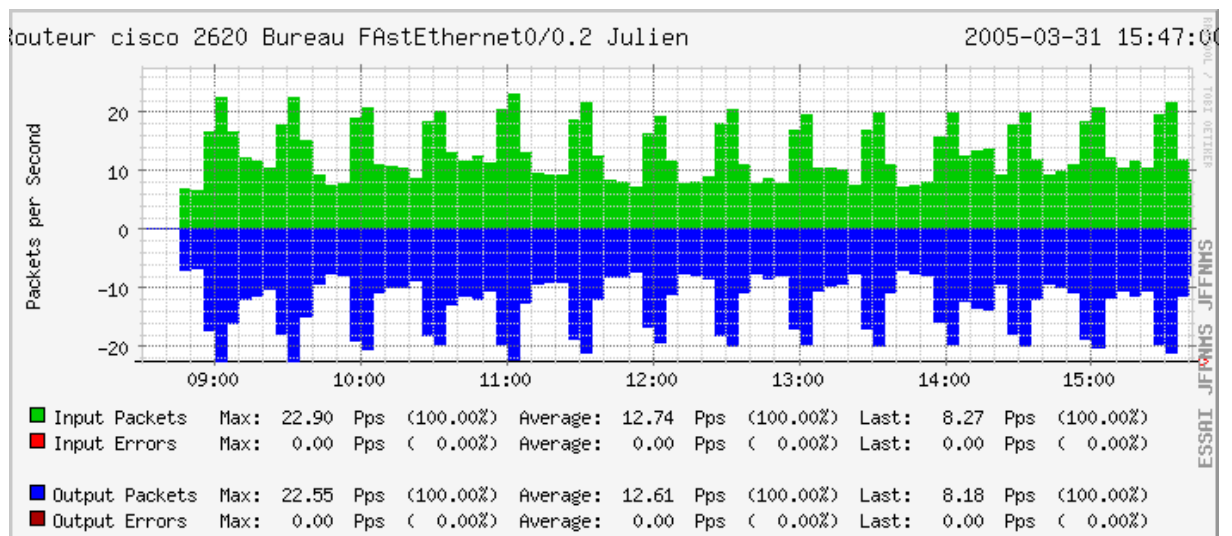
Les seuils d'alertes sont visibles dans plusieurs menus de JFFNMS mais seulement paramétrables depuis un seul menu. Il faut donc effectuer de nombreux essais avant de comprendre où se situe le paramétrage de telle ou telle information.

### - Les différents objets observés

La charge CPU(Central Process Unit), le nombre de processus, l'espace disque, la mémoire, certains processus, la version du système d'exploitation, le trafic en entrée/sortie et les différents ports sont observables sur des postes de travail.

La température du processeur, la charge CPU, la mémoire, la version de l'IOS et le trafic en entrée/sortie sur toutes les interfaces présentes sont observables sur un routeur ou un commutateur.

Il est évidemment aussi possible d'observer le nombre de paquets erronés, perdus, envoyés ou reçus :



### -Surveillance des processus systèmes

Grâce à JFFNMS, on peut surveiller n'importe quel processus système et vérifier qu'il est bien en exécution à un instant t. On peut aussi voir le nombre de processus actifs sur une machine. Ceci permet de voir par exemple, sur un serveur, si certains services sont en fonctionnement. Des pannes peuvent subvenir sur des bases de données. On peut donc vérifier la présence des processus nécessaires à l'accès à la base de données.

### -Prise en compte de nouveaux équipements

Pour qu'un nouvel équipement sur le réseau puisse être observé, il est nécessaire de configurer son adresse IP dans le menu Administration. D'autres informations sont nécessaires, telles que la communauté auquel ce nouvel équipement appartient, ou encore l'adresse du serveur TFTP. Ensuite, il est nécessaire de sélectionner les interfaces que l'on veut surveiller. Ceci peut se faire de manière automatique ou bien manuelle.

### -Seuil d'alerte dépassé

Il est possible de définir un seuil d'alerte quand par exemple l'espace disque occupé dépasse un certain pourcentage de l'espace disque total. L'alerte est visible avec un degré de sévérité que l'on peut affecté selon des critères personnels. L'administrateur peut être alerté via SMS ou par mail selon certaines conditions.

### -Ports ouverts ou fermés

La détection des ports ouverts ou fermés se fait de manière automatique du moment que l'on choisit de les surveiller. De plus, ceci permet de savoir notamment si des utilisateurs du réseau parviennent à se connecter sur un équipement, tel qu'un routeur, par telnet par exemple. On peut en effet voir le nombre de connections établies sur ce port, et donc en déduire facilement que quelqu'un a peut être essayer de modifier la configuration d'un équipement.

### -Filtres

Chaque utilisateur du logiciel est doté de droits bien spécifiques qui lui permettront de ne voir seulement les informations qui lui sont nécessaires. Le fait de restreindre l'accès à toutes les informations évite que des données importantes puissent être lues par n'importe qui.

### -Evolutivité

L'évolutivité dépend de la possibilité que l'on puisse intégrer ou non de nouvelles données au logiciel au fil du temps ; ce qui permettra au logiciel d'être totalement façonnable en fonction de l'avancée du réseau.

Il est possible dans JFFNMS de rajouter par exemple des interfaces à observer qui n'étaient pas intégrées à l'origine .La condition est de bien connaître la MIB(Management Information Base) comme le montre l'exemple ci-dessous :

MIB  
↓

ID	Description	Name (Match RRD Struct DS)	Poller Command (file)	Parameters
122	Apache Status	tac,tkb,cplo,up,bpr,bw,iw	apache	
31	BGP Inbound Updates	bgpin	snmp_counter	.1.3.6.1.2.1.15.3.1.10.<remote
32	BGP Outbound Updates	bgpout	snmp_counter	.1.3.6.1.2.1.15.3.1.11.<remote
38	BGP Peer Status	bgp_peer_status	bgp_peer_status	<remote>
33	BGP Uptime	bgpuptime	snmp_counter	.1.3.6.1.2.1.15.3.1.16.<remote
30	Cisco 2500 Series CPU Utilizat	cpu	snmp_counter	.1.3.6.1.4.1.9.2.1.56.0
58	Cisco Accounting	acct_bytes,acct_packets	cisco_accounting	
16	Cisco CPU Utilization	cpu	snmp_counter	.1.3.6.1.4.1.9.9.109.1.1.1.5
25	Cisco Free Memory	mem_free	snmp_counter	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
67	Cisco MAC Accounting Input Byt	input	snmp_counter	.1.3.6.1.4.1.9.9.84.1.2.1.1.4.
65	Cisco MAC Accounting Input Pac	inputpackets	snmp_counter	.1.3.6.1.4.1.9.9.84.1.2.1.1.3.
68	Cisco MAC Accounting Output By	output	snmp_counter	.1.3.6.1.4.1.9.9.84.1.2.1.1.4.
66	Cisco MAC Accounting Output Pa	outputpackets	snmp_counter	.1.3.6.1.4.1.9.9.84.1.2.1.1.3.

### -Gestion des logs

Les logs peuvent être enregistrés dans la base de données. Les logs sont enregistrés à l'intérieur d'un fichier texte et sont organisés de façon correcte. Lorsqu'on édite le fichier journal contenant les événements, il est possible de distinguer facilement quels événements sont intervenus ainsi que la date et l'heure des événements. Cela apporte donc une facilité dans la consultation des fichiers logs.

### -Possibilité de « looking-glass »

Les graphes générés par JFFNMS paraissent peu exploitables du fait que rien n'indique un moyen apparent de les récupérer. En effet, lorsque l'on veut visualiser un graphique, il n'y a pas d'URL chargé qui permettrait de connaître le lien afin de pouvoir effectuer cette recherche en utilisant cette URL par exemple.

### **CACTI :**

#### - Ergonomie

Les menus proposés sont explicites et permettent de bien appréhender le logiciel. Le menu se trouve sur la gauche de la page comme en témoigne la capture d'écran ci-dessous :



### -Facilité du paramétrage, prise en main

Le paramétrage du logiciel est assez simplifié. En effet, dès que l'on s'est connecté, l'écran propose une gestion simplifiée afin de configurer de suite les équipements que l'on veut surveiller, ainsi que les informations à faire figurer sur les graphes.

### -Les différents objets observés

La capture d'écran ci-dessus donne un aperçu du type d'éléments que l'on peut observer. Il est ainsi possible de surveiller l'espace disque, la mémoire physique et virtuelle, la CPU et le trafic sur les différentes interfaces.

On peut noter aussi que l'on peut observer le nombre d'utilisateurs connectés et le nombre de processus. Cependant, il n'est pas possible d'observer un processus spécifique. De plus, les températures du châssis et du processeur des éléments d'interconnexion ne sont pas disponibles.

### -Prise en compte des nouveaux équipements

La prise en compte de nouveaux équipements s'effectue grâce à des modèles à sélectionner. Ceci influera ensuite sur le type de données qui peuvent être recueillies. En effet, on ne pourra pas avoir sur un serveur des informations relatives à un routeur Cisco par exemple. Cependant, si le modèle n'est pas créé dans Cacti, il est possible de le créer. Ceci est notamment le cas pour les commutateurs Cisco.

## -Modèles

La notion de modèles est très importante car elle permet de faciliter la gestion de ce que l'on modélise. Des modèles de graphes, d'hôtes (équipements réseaux), et de données peuvent être créés.

Les modèles de graphes correspondent à la mise en place d'un certain type de graphes où l'on pourra définir par exemple : la légende, l'ordonnée maximale d'un graphe, la taille ...

Les modèles d'hôtes, quant à eux, permettent de créer comme l'a été précédemment expliqué des types d'équipements réseaux. On pourra renseigner notamment comment les données y sont recueillies (par le protocole SNMP par exemple).

Enfin, les modèles de données représentent comment des données telles que la capacité du disque est recueillie. On peut aussi y définir des valeurs maximales ou minimales.

Les modèles peuvent tout aussi bien être importés ou exportés. L'exportation peut s'effectuer vers le format XML. Les modèles exportés peuvent servir pour la sauvegarde de ces modèles, ceux qui sont importés permettent la reconstitution des modèles.

## -Possibilité de « Looking-glass »

Cacti exploite tout à fait convenablement cette fonctionnalité. Il est possible lors de l'affichage d'un graphe de connaître l'URL définissant le lien. Lors de la demande d'affichage d'un graphe spécifique, une nouvelle page est chargée. On peut donc récupérer facilement le lien de ce graphe afin de pouvoir l'intégrer à une application extérieure.

Cependant, l'URL est du type :

[http://147.210.6.150/cacti-0.8.6c/graph.php?rra\\_id=all&local\\_graph\\_id=21](http://147.210.6.150/cacti-0.8.6c/graph.php?rra_id=all&local_graph_id=21)

On peut voir dans cet exemple que CACTI recherche le « local\_graph\_id=21 » correspondant ici à l'espace disque du disque dur.

Or cette URL n'est pas tout à fait explicite car elle fait appel à des numéros assignés aux graphes. Ces numéros sont assignés de manière aléatoire à chacun des graphes. Si la configuration de CACTI ou du réseau n'est pas changée, cela n'apporte pas d'inconvénients. Cependant, si l'on veut ajouter ou remplacer des équipements sur le réseau, il faudra à nouveau rechercher le nouveau numéro affecté aux graphes de ces équipements.

## 4.3) Bilan comparatif

Au vu de l'ensemble des tests effectués, il semblerait que JFFNMS offre de nombreuses possibilités de configuration contrairement à CACTI. En effet, CACTI est beaucoup plus centré sur la notion de graphiques, malgré la notion de modèles fortement appréciable.

Cependant, JFFNMS ne présente pas une facilité de prise en main. Les menus de CACTI sont beaucoup plus appréciables. De plus, il subsiste des problèmes quant à l'utilisation de JFFNMS. Les utilisations répétées de ce logiciel, ont permis de constater qu'une amélioration dans le domaine de l'enchaînement des écrans, ainsi que dans celui du rafraîchissement des pages était possible.

Enfin, le plus important est que CACTI est plus exploitable que JFFNMS depuis une autre application. Cet aspect là, qui paraissait très intéressant pour l'entreprise a été beaucoup plus apprécié.

## **5) CONCLUSION**

Les tests effectués ont nécessité une documentation importante sur les protocoles utilisés et les logiciels.

Ces tests ont permis au responsable de la sécurité de REAUMUR d'avoir un point de vue sur les deux logiciels. Ceci a été rendu possible grâce aux avantages et inconvénients listés, qui chacun ayant une importance prépondérante sur les autres.



Néanmoins, des problèmes relatifs à l'installation et la configuration, ainsi qu'à la mise en œuvre des tests ont été rencontrés. Des solutions ont été trouvées en évaluant bien la situation. C'est ainsi que ce projet a pu être mené à terme.