HAL
open science

# Administration routeurs et surveillance des différents accès réseaux Infomil

Gauthier Jauneau

## To cite this version:

Gauthier Jauneau. Administration routeurs et surveillance des différents accès réseaux Infomil. Systèmes et contrôle [cs.SY]. 2013. dumas-01147600

**HAL Id: dumas-01147600**

**https://dumas.ccsd.cnrs.fr/dumas-01147600v1**

Submitted on 30 Apr 2015

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**CONSERVATOIRE NATIONAL DES ARTS ET METIERS**

**CENTRE REGIONAL ASSOCIE DE**

***Toulouse***

**MEMOIRE**

**présenté en vue d'obtenir**

**le DIPLOME d'INGENIEUR CNAM**

**SPECIALITE : INFORMATIQUE**

**OPTION : RESEAU SYSTEME ET MULTIMEDIA**

**par**

**JAUNEAU Gauthier**

---

# Administration routeurs et surveillance des différents accès réseaux Infomil

**Soutenu le 26 juin 2013**

---

**JURY**

**PRESIDENT :**

**MEMBRES :**

**Remerciements**

Je tiens tout d'abord à remercier tout particulièrement les acteurs qui m'ont permis aujourd'hui de réaliser ce projet d'envergure au sein de mon entreprise.

Christophe Labarre, chef de service support client et maintenance, tuteur du projet, qui a fait le nécessaire pour que ce projet voie le jour et arrive à terme.

Christophe Belaubre, responsable support solutions Front Office au support Infomil, qui m'a alloué le temps nécessaire à la réalisation de ce projet et à la rédaction de ce mémoire.

Florian Cristina, ingénieur réseau, qui m'a assisté et formé sur la console Osuri, me présentant les différentes fonctionnalités et possibilités de cette console.

Guillaume Larrieu, ingénieur support, qui m'a assisté et aidé dans l'élaboration des scripts vb de récupération de données sur les équipements en place.

L'accès aux outils de développement au sein du support Infomil étant assez restreint, je tiens à remercier tous ceux qui m'ont fourni des explications, des conseils et de la documentation diverse et variée.

Ces outils de surveillance et la rédaction de ce mémoire ont vu le jour grâce à eux.

**ABREVIATIONS /GLOSSAIRE**

Evolutel : logiciel de front-office

Abaco : logiciel de back-office

Galec : groupement des Adhérents E.LECLERC

Osuri : console de supervision de serveurs et d'équipements réseaux

Cacti : logiciel de supervision utilisé par la console OSURI

HSRP : Hot Standby Router Protocol

VPN : Virtual Private Network

L2TP : Layer2 Tunneling Protocol

IPSec : Internet Protocol Security

SNMP : Simple Network Management Protocol

TFTP : Trivial File Transfer Protocol

DHCP : Dynamic Host Configuration Protocol

Vbs : vbscript -langage de scripting-

Nagios : outil de monitoring

Rrdtool : Round Robin Database tool

Bgp : Border Gateway protocol

<u>Les types de routeurs et leurs nominations :</u>

Arpv : Ancêtre du RML. Routeur de télémaintenance qui n'est pas secouru, le magasin dispose d'un seul accès (pas de groupe HSRP)

Routeurs l2tp : ponts qui permettent d'assurer un vpn entre un espace déporté (une station essence, un Leclerc express, un drive...) et l'hypermarché via le protocole l2tp (layer2 tunneling protocol)

Pont bridge : Même utilisation que le pont l2tp, à l'exception que celui-ci utilise le mode bridge. Cette utilisation est amenée à disparaître car ce fonctionnement est incompatible avec la version IOS 12.4(24)T7.

RML : Routeur métier Leclerc, routeur de télémaintenance qui dispose d'un secours dynamique via groupe HSRP

Arpvd : Routeurs déployés sur les express drive. Ces routeurs sont également secourus de la même façon que les routeurs RML (un accès SDSL et un accès ADSL).

Ouvren1 : Routeur utilisé comme passerelle 2 LANS : celui info géré par Infomil et celui des réseaux tiers

Ouvredacn1 : Routeur utilisé aux stations essences. Ce routeur est utilisé comme passerelle entre le réseau du pétrolier et le réseau Infomil. Variante de l'ouvren1 dédié aux configurations des stations.

Ouvremab. Routeur utilisé aux manèges à bijoux (MAB). Variante de l'ouvren1 dédié aux configurations du MAB.

Termes opérateurs/ Fai

**ADSL : Asymetrical Digital Subscriber Line**

L'ADSL fait partie des technologies xDSL qui permettent d'améliorer les performances des réseaux d'accès et en particulier de la ligne d'abonné du réseau téléphonique classique, constituée de fils de cuivre.

Grâce à l'utilisation de deux modems, l'un placé chez l'abonné, l'autre sur la ligne d'abonné, devant le répartiteur principal, il permet d'améliorer considérablement le débit du réseau et d'obtenir des transmissions 70 fois plus rapides qu'avec un modem analogique classique.

Le principe de l'ADSL consiste à réserver une partie de la bande passante au transport de la voix, une autre au transport des données circulant en direction du cœur de réseau autrement appelé backbone (données montantes) et une troisième, plus importante au transport des données circulant vers l'abonné (données descendantes).

Pour la restitution correcte de la voix, des filtres situés à chaque extrémité de la ligne éliminent les parties du signal inutiles.

La technologie ADSL est particulièrement bien adaptée aux liaisons de boucle locale puisque le débit qu'elle permet diminue avec la longueur de la ligne. En raison de son faible coût, elle constitue une solution intéressante pour bénéficier d'un accès rapide à Internet.

Ainsi donc, afin d'optimiser le débit disponible pour une utilisation courante, le débit est asymétrique : le débit descendant (download) est plus élevé que le débit montant (aussi nommé upload).

La technologie ADSL2+ :

Successeur de l'ADSL pour le très haut débit. Il permet d'atteindre un débit de 25 Mbps pour les abonnés situés à moins 500 mètres du DSLAM. Pour les autres, c'est un peu moins : 8 Mbps à une distance de 3 km, par exemple.

Il se distingue par l'ajout de la gamme de fréquence entre 1.1 et 2.2 Mhz en plus de la gamme de l'ADSL classique, située entre 0.15 et 1.1 MHz. Ceci permet d'augmenter significativement la bande passante disponible.

La technologie Re-ADSL2 :

Il existe une technologie nommée ***Re-ADLS2*** (Reach extended ADSL2). Cette Technologie étend la portée d'un NRA à plus de 8 km, contre un maximum de 5km pour la technologie ADSL, avec un débit descendant de 512 Kbps et un débit montant de 128 kbps. Elle consiste à amplifier le signal (surtout les hautes fréquences) envoyé par le DSLAM, permettant ainsi à nombre d'abonnés potentiels situés jusqu'alors en zone blanche de profiter du haut débit. Cependant, le revers de la médaille est que cette plus grande portée du signal est accompagnée d'une limitation du débit descendant à 1 Mbps dans le meilleur des cas.

**DSLAM : Digital Subscriber Line Multiplexer**

Situé sur le réseau de l'opérateur local, au niveau du répartiteur, il fait partie des équipements utilisés pour transformer une ligne téléphonique classique en ligne ADSL permettant la transmission des données, et en particulier l'accès à Internet, à haut débit.

La fonction du DSLAM est de regrouper plusieurs lignes ADSL sur un seul support, qui achemine les données en provenance et à destination de ces lignes.

**BAS : BroadBand Access Server**

Il s'agit d'un équipement dont la fonction est de gérer le transport de données en mode ATM (Asynchronous Transfert Mode) dans le cadre des offres d'accès à Internet par ADSL (Asymetrical Digital Subscriber Line).

Sur le réseau de l'opérateur historique, chaque BAS regroupe le trafic ATM issu d'une dizaine de DSLAM (Digital Subscriber Lime Multiplexer).

Un BAS gère donc le trafic de l'ensemble des lignes ADSL situées dans les zones couvertes par les DSLAM qui lui sont connectés.

La zone ainsi couverte par un BAS est appelée "plaque" par France Télécom. Il est établi un circuit ATM "montant" et un circuit ATM "descendant" entre chaque client connecté et le BAS auquel il est raccordé.

**ATM : Asynchronous Transfert Mode**

Protocole de transfert basé sur un mode de transfert asynchrone.

Il utilise la technique de transfert asynchrone pour des communications à haut débit d'informations numérisées, organisées en paquets courts et de longueur fixe.

L'ATM permet une transmission ultrarapide des informations et une utilisation optimale de la capacité des lignes, et se trouve particulièrement adapté aux réseaux multiservices à haut débit.

Ce mode de transmission peut notamment être utilisé pour tirer le meilleur parti d'un backbone (structure mère d'un réseau aussi appelée cœur de réseau).

**NRA : Noeud de Raccordement**

C'est le local technique rassemblant tous les équipements actifs de télécommunications (dont les DSLAM des différents opérateurs).

**Sdsl : Symmetric Digital Subscriber Line**

Le (SDSL, en français *ligne d'abonné numérique à débit symétrique*) permet de transporter des données, comme son nom l'indique, de manière symétrique, contrairement à l'adsl. Cela signifie que, pour un accès à 2Mbps, le client aura aussi bien 2Mbps en upload qu'en download. Le Sdsl a une portée maximum de 2.4km. Le SDSL utilise à minima une paire torsadée. Le débit de la SDSL peut être accru en utilisant plusieurs paires torsadées.

Cette utilisation de plusieurs paires de cuivre est aujourd'hui très fréquente, 4 paires de cuivre sont nécessaires pour atteindre un débit de 8 Mb/s au maximum. L'opérateur va tout simplement regrouper plusieurs paires de cuivre.

L'offre d'accès SDSL est avant tout destinée aux établissements professionnels : elle permet l'échange de données à haut débit entre plusieurs sites distants d'une même entreprise.

Contrairement à l'ADSL, le SDSL utilise également la bande spectrale utilisée communément pour le transport de la voix (de 300 à 3400 Hz). Il n'est alors plus possible d'utiliser le service téléphonique classique, la ligne est donc dédiée aux flux data. De ce fait, il n'est plus nécessaire d'utiliser de filtre.

# Administration routeur RML

INTRODUCTION ..... 9
PRESENTATION DE LA SOCIETE INFOMIL ..... 11
PRESENTATION DU GROUPE E.LECLERC ..... 14
ARCHITECTURE RESEAU EN PLACE. PROBLEMATIQUE ET BESOINS ..... 18
EQUIPEMENTS RESEAUX UTILISES. ETAT DU PARC LORS DU DEBUT DU PROJET 22
OUTILS DE SURVEILLANCE MIS EN PLACE. TRAVAUX EFFECTUES ..... 25
1. Script de maj automatique des versions IOS Cisco 29
2. Console de supervision Osuri 33
2.1. SNMP ..... 34
2.2. Rrdtool ..... 37
2.3. Cacti ..... 39
2.4. Présentation des indicateurs récupérés sur Osuri..... 39
3. Scripts de surveillance 45
3.1. Test de vie d'un équipement local en magasin ..... 45
3.2. Test de latence réseau..... 45
3.3. Récupération bande passante des interfaces d'un routeur ..... 46
RESULTATS..... 48
1. Rédaction de fiches à l'attention des techniciens 48
2. Cas concrets de résolution de problèmes grâce aux scripts développés 66
CONCLUSION ..... 70

# Introduction

Au sein de la société Infomil, société éditrice de solutions logicielles "clé en main" et prestataire informatique des centre commerciaux E.LECLERC, un grand nombre de sites distants sont déployés. Les enseignes E.LECLERC sont informatisées et sont accessibles à distance via des accès réseaux magasin, afin de pouvoir assurer non seulement la télémaintenance du matériel sur site, mais également des flux du réseau métier. Vidéoconférence, flux bancaires, équipements déportés sur datacenter, applications clients-serveurs...

Devant l'accroissement des flux réseaux transitant entre le magasin et "le reste du monde", il a donc fallu trouver des solutions rapides et efficaces pour assurer une continuité et une qualité de service optimale pour nos clients.

Il a donc fallu revoir l'architecture réseau de nos clients, et mettre en place certains outils de surveillance.

C'est par une meilleure anticipation, une réactivité accrue de notre part (actions préventives plutôt que curatives) que nous pouvons garantir une meilleure qualité de service et une meilleure satisfaction client.

Dans ce mémoire, j'aborderai donc la nouvelle architecture réseau mise en place afin de poser clairement le contexte, ainsi que les différents outils de surveillance mise en place pour répondre aux besoins des clients notamment :

- Les scripts de surveillance et de mise à jour des routeurs en vb

- La console Osuri, console graphique construite à partir de Cacti, Nagios et rrdtool

- Les rédactions de procédures à destination des techniciens.

- La formation des techniciens sur ces différents outils

Bien que je n'ai au final pas participé au développement de la console Osuri, je suis obligé d'aborder ce sujet, car les procédures techniques rédigées par mes soins se basent

essentiellement sur cette console graphique. J'ai cependant été amené à former les techniciens sur cette console.

## Présentation de la société Infomil

Infomil est un prestataire informatique des magasins E.LECLERC, et travaille en étroite collaboration avec le GALEC (groupement d'Adhérents E.LECLERC). Sa principale mission est d'équiper les enseignes de systèmes d'encaissement performants et répondant aux contraintes du marché.

Cette société équipe 678 clients sur le territoire Européen et l'outre-mer

La société est née en 1994 et emploie aujourd'hui plus de 250 salariés.

2 agences supplémentaires, en plus de celle de Toulouse, ont vu le jour en 2002 : Nancy et Paris

La société dispose également d'une filiale à l'île Maurice : Infomil Mauritius ltd

Principaux logiciels développés

**Evolutel**, système d'encaissement et de gestion de fidélisation (Front-Office, Middle-Office) permet d'encaisser mais aussi de définir et mettre en place des outils de marketing direct (segmentation, actions de fidélisation, …) via la carte de fidélité.

**Abaco**, système de gestion commerciale et des flux logistiques (Back-Office) permet d'avoir une vue globale des différents circuits et catégories de flux (articles, tarifs fournisseurs, marge...), tout en permettant une gestion fine de l'activité et des données obtenues.

**Leclerc Drive**, logiciel de Middle Office. Le client peut passer commande sur le site internet Leclerc Drive, le magasin est alors prévenu en temps réel. Une fois la commande validée, celle-ci est préparée en entrepôt, le client vient alors retirer directement sa commande sur une piste de retrait.

Les différents corps de métier :

- Développement sur Evolutel, Abaco3, Leclerc Drive...

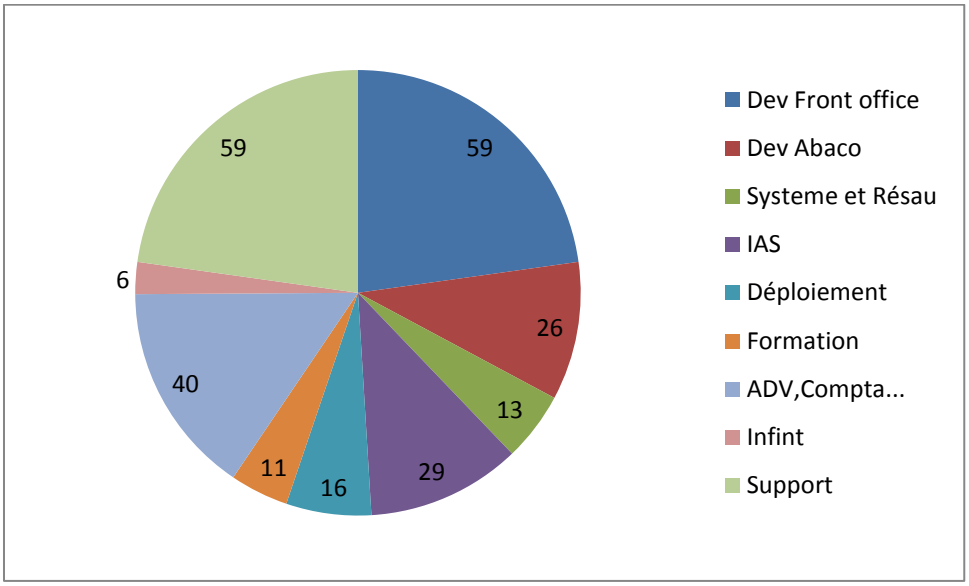
- Ingénierie et conseil,

- Infrastructure système et réseaux,

- Distribution, installation, intégration et formation sur nos différents logiciels et systèmes d'encaissement,

- Assistance téléphonique et maintenance matériel,

Répartition salariale en nombre d'employés à Infomil au 01/05/13 :




Les différents services

IAS : Informatique et Administration Système. Support des applications bureautiques, et diffusion des nouvelles versions des logiciels, après intégration. Intervention sur une partie des contrats d'achat.

Déploiement : lors de l'achat d'un bien ou d'un service, le client est assisté dans sa mise en fonctionnement, son installation et son paramétrage. C'est le service déploiement qui occupe cette fonction

Logistique : Gère toute la partie stock. Acheminement des marchandises, suivi des expéditions/réceptions...

Support Clients : Répond aux différentes sollicitations des clients. Fait le relais entre les équipes de développement et le client en cas de problème matériel ou logiciel.

Développement Abaco : Développement sur le logiciel Abaco, logiciel propriétaire Infomil, qui permet de gérer toute la partie back office d'un magasin. Passage de commande, gestion de stock, inventaire...

Développement Evolutel : Développement sur le logiciel Evolutel, logiciel propriétaire Infomil, qui permet d'effectuer notamment l'encaissement sur le système de caisse, et un logiciel de front office afin de consulter le CA en temps réel, visionner les caisses enregistreuses...

Développement Leclerc Drive : Développement sur le logiciel de middle-office Leclerc Drive, logiciel propriétaire Infomil. Logiciel qui permet de gérer le réapprovisionnement des stocks, les ruptures d'articles, la mise en ligne sur le site internet Leclerc Drive et la maintenance du site Leclerc Drive.

Administration des ventes : Ils répondent aux questions d'ordre administratif et gèrent les relations fournisseurs.

Commercial : Les ingénieurs commerciaux répondent aux besoins des clients.

Informatique interne : Ils gèrent le parc informatique de l'entreprise. Maintenance des postes, maintenance des serveurs, maintenance des logiciels de service.

Formation : Forment les utilisateurs sur les nouveaux logiciels mis à leur disposition. Se rendent en magasin ou procèdent à des formations téléphoniques ou par visio-conférence.

## Présentation du groupe E.Leclerc

Le mouvement E.Leclerc est apparu en 1949, sous l'égide d'Edouard Leclerc avec l'ouverture du premier magasin à Landerneau. Le but premier était de faire baisser les prix des produits de grande consommation dans la France d'après-guerre afin de les rendre accessibles au plus grand nombre.

Chaque magasin sous l'enseigne E.Leclerc fonctionne de manière autonome.

Aujourd'hui, ce groupement dispose de 474 adhérents en France.

Le mouvement Leclerc s'articule autour de trois grands axes :

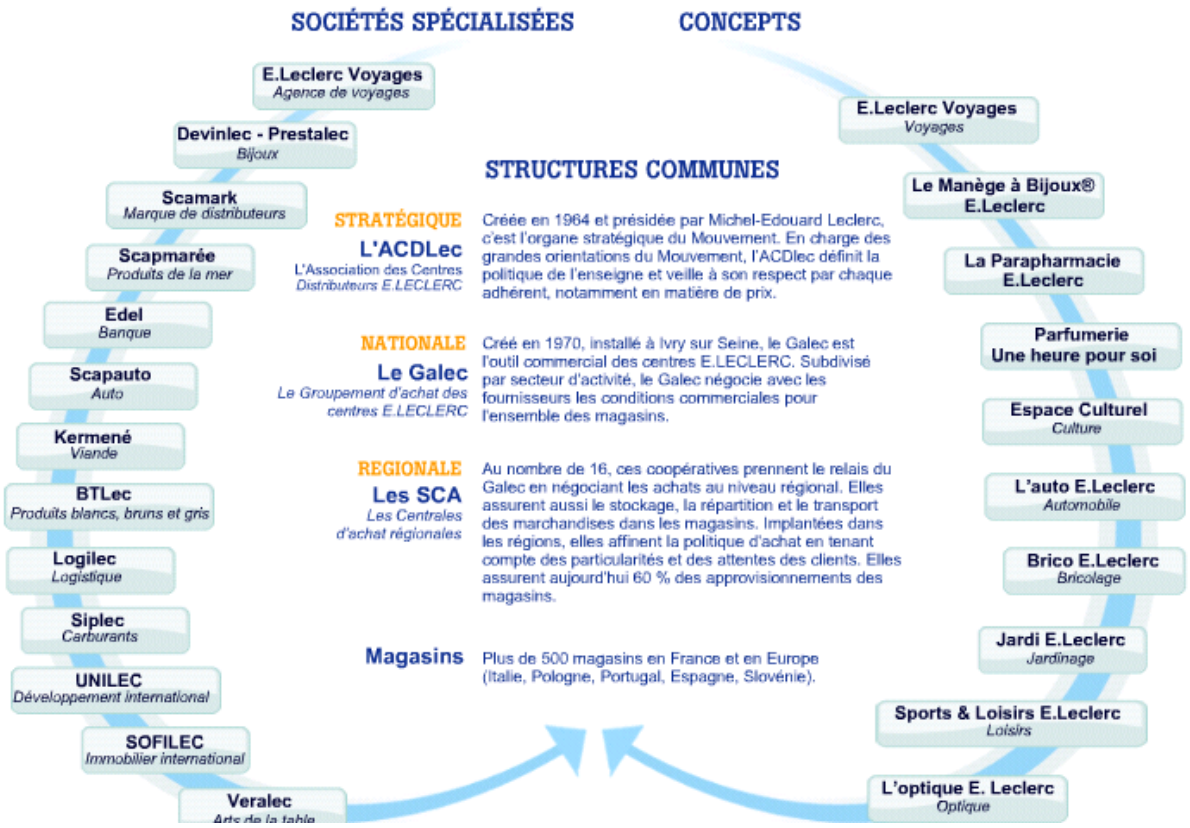
- L'acdlec qui est l'entité du contrôle des règles de fonctionnement du groupement Leclerc.

Elle définit également les orientations stratégiques de l'enseigne et désigne les nouveaux adhérents magasins.

- le Galec coordonne et met en œuvre la politique commerciale de l'enseigne E.LECLERC.

- les centrales qui assurent les liens logistiques entre les magasins et les fournisseurs, négocient également les tarifs/prix avec eux en fonction de la géolocalisation des magasins.

Voici un petit schéma récapitulatif des sociétés et concepts gravitant autour du mouvement Leclerc.




Source : www.mouvement-leclerc.com

Infomil a pour mission de garantir le bon fonctionnement informatique des solutions qu'elle implante dans les magasins Leclerc et leurs concepts . Nous devons également mettre en place et déployer les concepts informatisés que les magasins souhaiteraient obtenir.

Organigramme du support :

- 1 chef de service support client et maintenance

-1 responsable solutions Front Office support Evolutel

-1 responsable solutions Back Office support Abaco

-1 responsable support maintenance

- 1 responsable support cellule matériel

- 6 ingénieurs support Evolutel

- 4 ingénieurs support Abaco

-1 ingénieur firmware/hardware

- 1 responsable d'équipe support Abaco

- 4 responsable d'équipe support Evolutel

- 6 techniciens Abaco

- 26 techniciens support Evolutel

- 3 techniciens support matériel

- 3 techniciens maintenance

Les clients :

678 magasins équipés Evolutel (France, Portugal, Espagne, Slovénie, La Réunion)

282 magasins Abaco au 12/03/13

19 Centrales et Galec,.

Ma position dans l'entreprise : Ingénieur support Evolutel au sein du service support client.

Mon rôle au sein du service support :

- Traiter les problématiques liées à l'activité magasin requérant un niveau d'analyse plus avancé,

- Accompagner en niveau 2 les techniciens dans la résolution de problèmes qui leurs sont soumis par nos clients,

- Assurer la continuité de l'information entre les techniciens support et les équipes de développement,

- Rédiger des documentations et des procédures à destination des techniciens afin de les aider à analyser les différentes problématiques rencontrées,

- Superviser, administrer et traiter des problématiques réseaux afin de s'assurer que tous les flux nécessaires à la télémaintenance et au fonctionnement du magasin soient opérationnels.

## ARCHITECTURE RESEAU EN PLACE. PROBLEMATIQUE ET BESOINS

Devant l'augmentation croissante d'utilisation de bande passante par les magasins, il a fallu convenir d'une modification globale de l'architecture réseau.
Au départ, nos équipements en magasin étaient uniquement constitués d'un routeur qui nous permettait de faire de la télémaintenance. Très peu de flux transitaient par cet accès, une ligne en 512k/1Mo suffisait amplement.

Depuis de nouveaux concepts ont vu le jour.

Serveurs déportés sur datacenter, matériel de visioconférence mis en place, systèmes de télésurveillance, téléphonie ip, accès internet pour les utilisateurs, interconnexions multiples avec des organismes tiers (banque, operateur telecom..)...

L'architecture de base ne suffisait donc plus aux besoins du client.

Il a été nécessaire de revoir l'ensemble de notre architecture réseau.

Et ce en prenant en compte:

- Les problématiques commerciales

- Les problématiques techniques

- Les problématiques de géolocalisation

De là est née l'appellation RML : réseau métier Leclerc.

Le Rml1 est un accès ADSL

Le Rml2 est un accès SDSL

Les deux routeurs forment un groupe HSRP, dont le maître est dans tous les cas le RML2

Le rml2 est maître du groupe. Si l'accès tombe, il dispose d'une route par défaut pour router les flux vers le routeur rml1

Exemple :

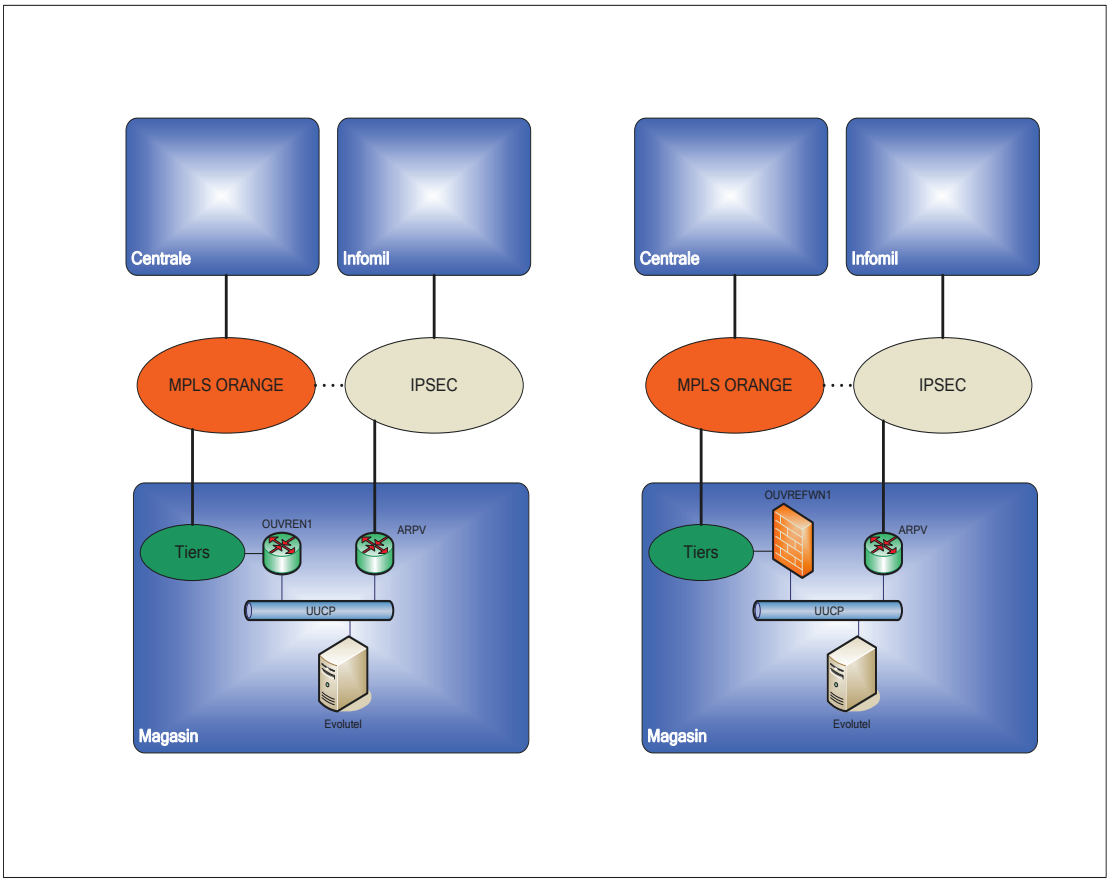
```
S*    0.0.0.0/0 [1/0] via 149.56.26.2
```

Avant :

Les différents flux (Evolutel, Abaco...) transitaient :

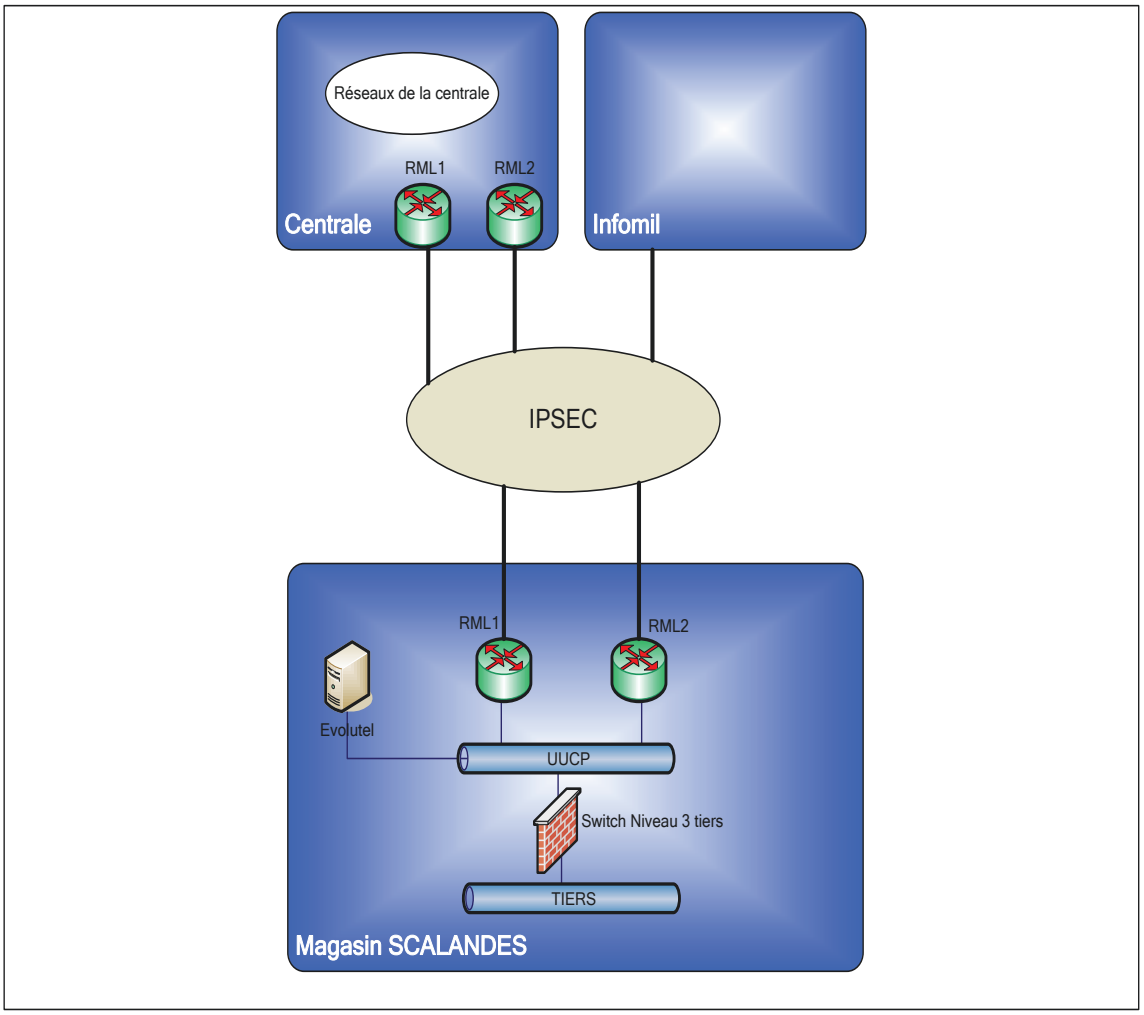
- Soit via l'ARPV magasin (administré par Infomil) : Amex, Payzone, Transax par exemple.

- Soit via le réseau centrale (ou réseau Tiers) : carte fidélité, carte cadeau...



Après :

Les différents flux transitent tous par les routeurs RML1/RML2




Règles de routage des flux :

Les différents flux transitant par les accès RML sont répartis de la façon suivante :

- **Si la bande passante en Upload de l'accès ADSL (RML1) est > 512 kbps**
  **==> Surf Internet sur ADSL (RML1)**
  **==> Tous les autres flux sur SDSL (RML2).**

  La Visio sera priorisée sur la SDSL, c'est à dire qu'on implémente de la qualité de service qui fait que, si l'accès est saturé, on routera en priorité les flux Visio. Le surf Internet sera secouru par l'accès SDSL en cas de perte du lien ADSL.

Les flux SDSL, exceptée la Visio, seront secourus par l'accès ADSL en cas de perte du lien SDSL. En effet, la visio sur des équipements haute définition est très gourmande en bande passante. Si ces flux étaient secourus sur l'accès ADSL RML1, non seulement cela perturberait grandement l'activité magasin, mais en plus la vision ne serait pas pleinement opérationnelle (images dégradées, coupures...)

- **Si la bande passante en Upload de l'accès ADSL (RML1) est < 512 kbps**
  **==> Tous les flux sur SDSL (RML2)**
  **==> L'accès ADSL sert uniquement de secours en cas de pb sur RML2. Tous les flux sont secourus, à l'exception des flux Visio.**

Comme on peut le voir, la redondance des accès avait déjà été prévu auparavant, mais aucun outil de surveillance n'existait pour parer aux éventuelles anomalies.

Le client nous appelait s'il rencontrait une avarie. De plus, cette architecture n'a pas été adoptée par toutes les centrales et tous les magasins. De ce fait, certains centre E.Leclerc sont totalement dépourvus d'accès redondants. En cas de panne sur leur routeur de télémaintenance, appelé ARPV, le magasin fonctionne en mode dégradé, le temps du rétablissement de la situation.

Actuellement, deux nouvelles centrales ont signé pour cette solution : la centrale SCADIF et LECASUD (magasins E.Leclerc de Paris et sa banlieue + région PACA) Leur migration est prévue courant 2013.

Au sein du support, j'ai pour mission, entre autres, de m'assurer qu'il n'y ait pas de problème lors de cette phase de déploiement.

Dans la partie suivante, nous aborderons la partie matérielle mise en place, et aurons une réflexion sur les outils que l'on peut mettre en place pour pallier ou réagir sur les différentes problématiques que peut rencontrer un accès magasin.

## EQUIPEMENTS RESEAUX UTILISES. ETAT DU PARC LORS DU DEBUT DU PROJET

Quel sont les modèles de routeurs déployés ?

Les routeurs déployés sont exclusivement des routeurs Cisco.

Voici un petit récapitulatif des modèles de routeurs déployés et leur version IOS selon leur utilisation :

**TABLEAU RECAPITULATIF DES VERSIONS IOS POUR ROUTEURS CISCO 87X ET 88X**

**Date de création :** 29/08/2012
**Dernière mise à jour :** 29/08/2012

| | ARPV | PONT L2TP | PONT BRIDGE | RML | ARPVD | OUVREN1* | OUVREDACN1* | OUVREMAB* | OUVREN2,3* |
|---|---|---|---|---|---|---|---|---|---|
| **871** | | 12.4(24)T7 | 12.4(4)T1 | 12.4(24)T7 | 12.4(24)T7 | 12.4(4)T1 ou 12.4(24)T7 | 12.4(4)T1 ou 12.4(24)T7 | 12.4(4)T1 ou 12.4(24)T7 | 12.4(4)T1 ou 12.4(24)T7 |
| **877** | 12.4(24)T7 | 12.4(24)T7 | 12.4(4)T1 | 12.4(24)T7 | 12.4(24)T7 | | | | |
| **878** | | 12.4(24)T7 | 12.4(9)T2 | | 12.4(24)T7 | | | | |

*** Le choix de la version se fait en fonction du nombre de VLAN déclarés, car la version 12.4(24)T7 ne permet d'activer que 4 VLAN (VLAN1, étant activé par défaut, inclus), alors que la version 12.4(4)T1 n'a pas cette limitation.**

| | ARPV | PONT L2TP | ARPVHSP (HOTSPOT) | RML | ARPVD | OUVREN1 | OUVREDACN1 | OUVREMAB | OUVREN2,3 |
|---|---|---|---|---|---|---|---|---|---|
| **881** | | 15.2(2)T | | 15.2(2)T | 15.2(2)T | 15.2(2)T | 15.2(2)T | 15.2(2)T | 15.2(2)T |
| **887** | 15.2(2)T | 15.2(2)T | 15.2(2)T | 15.2(2)T | 15.2(2)T | | | | |
| **888** | | 15.2(2)T | | | 15.2(2)T | | | | |

Il a été nécessaire de mettre en place une version IOS unique par type de routeur afin d'avoir un parc homogène. Cela a permis de faciliter la maintenance des accès télécoms en question et la gestion des incidents. La campagne de mise à jour des versions IOS est décrite plus tard dans ce mémoire, puisque j'ai participé à cette campagne.

Actuellement les routeurs de types "ouvre" ne sont pas supervisés via la console Osuri et ce :

- afin de ne pas surcharger la console

- les principaux flux que nous administrons empruntent le réseau RML

- Dans le cas de l'ouvren1 par exemple, nous n'avons pas pour vocation de superviser les flux des mainteneurs tiers.

D'autre part, les routeurs de type pont en mode bridge, sont également amenés à disparaître.

Ce mode de fonctionnement n'est plus supporté par Cisco, qui préconise le mode l2tp. De plus le mode bridge n'est donc, de surcroit, pas compatible avec la dernière version IOS Cisco déployée, la 12.4.24(T7). Au fil de la diffusion de cette version IOS, les ponts sont donc basculés également dans une configuration de type l2tp. J'ai participé à ces mises à jour au sein du support.

Certains routeurs ARPV assuraient une double fonction : un accès de télémaintenance, ainsi qu'une liaison pontée ( vers un Leclerc Express, un espace culturel...)

Ce mode de fonctionnement n'étant plus supporté par Cisco et devant les nombreux problèmes rencontrés sur cette configuration, il a fallu également supprimer les routeurs disposant de cette configuration 'bancale'.

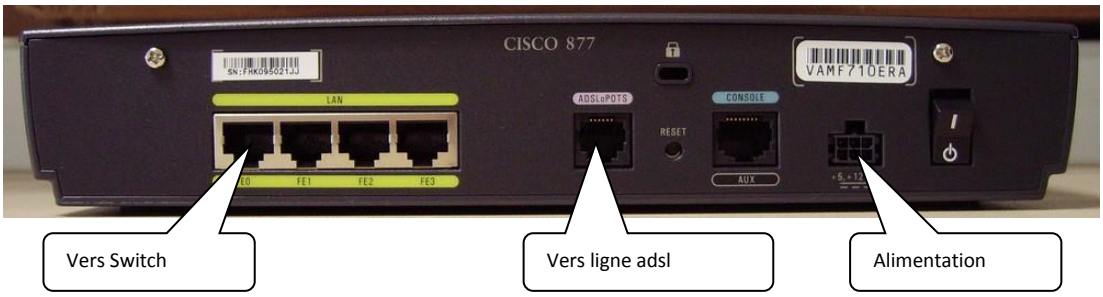
Cette campagne de suppression des arpv-pont présents sur le parc magasin a été suivi par l'équipe des ingénieurs support. Il a donc fallu dans un premier temps :

- alerter le magasin sur les éventuels incidents que peut rencontrer ce type de liaison, et les convaincre des impacts fonctionnels.

- informer le service commercial dans le but de soumettre une proposition au magasin afin de souscrire deux accès différents : un pour sa télémaintenance et l'autre pour la liaison pontée

- suivre et ordonner le bon déroulement des opérations de ce rétrofit.

Voici une photo d'un routeur Cisco 878 vu de dos avec ses différentes connectiques :




Cisco 878 => utilisé principalement pour les accès SDSL

Pourquoi ce choix de matériel ?

Il répond aux exigences du magasin en termes techniques et matériel :

Ces types de routeurs offrent :

- haute performance pour l'accès haut débit.

- vpn ipsec avec cryptage 3DES ou AES

- fonction NAC (network admission control) et application de politique d'accès sécurisé

- commutateur 4 port 100mbs full duplex avec support des vlans.

- cpu MPC8272 de 400Mhz

## OUTILS DE SURVEILLANCE MIS EN PLACE. TRAVAUX EFFECTUES

L'architecture fonctionnelle ayant été revue, il a fallu ensuite mettre en place des outils de supervision.

Auparavant, nous attendions que le client nous appelle pour nous signaler une éventuelle avarie (problématique de passage de carte bleues, de carte cadeau, le distributeur automatique de billets qui ne fonctionne plus...)

Nous étions donc dans la réaction et non dans l'anticipation.

Par ailleurs, dans le cadre de négociations pour obtenir l'adhésion de nouvelles centrales quant à l'implémentation de solutions RML sur leurs magasins, certaines d'entre-elles nous ont demandé de pouvoir traiter de manière plus efficace les problématiques liées au réseau magasin.

Voici en bref, suivant un cahier des charges et des questions/réponses avec la centrale Scaso, une étude des engagements pris vis à vis des clients.

Ainsi, certaines centrales nous ont demandé, avant de basculer sur nos équipements et notre architecture RML, certaines garanties : en terme de service, d'architecture et d'équipements en place, voire de reporting.

C'est le cas par exemple de la centrales Scaso (Region Aquitaine)

Ils demandent par exemple d'avoir accès :

- aux tables de routages des routeurs,

- aux modèles de routeur mis en place,

- les conditions de maintenance de ces routeurs,

- les accès et descriptions techniques des ouvertures de lignes opérateur,

- les protocoles de communication utilisés,

- les conditions de mise en service des accès,

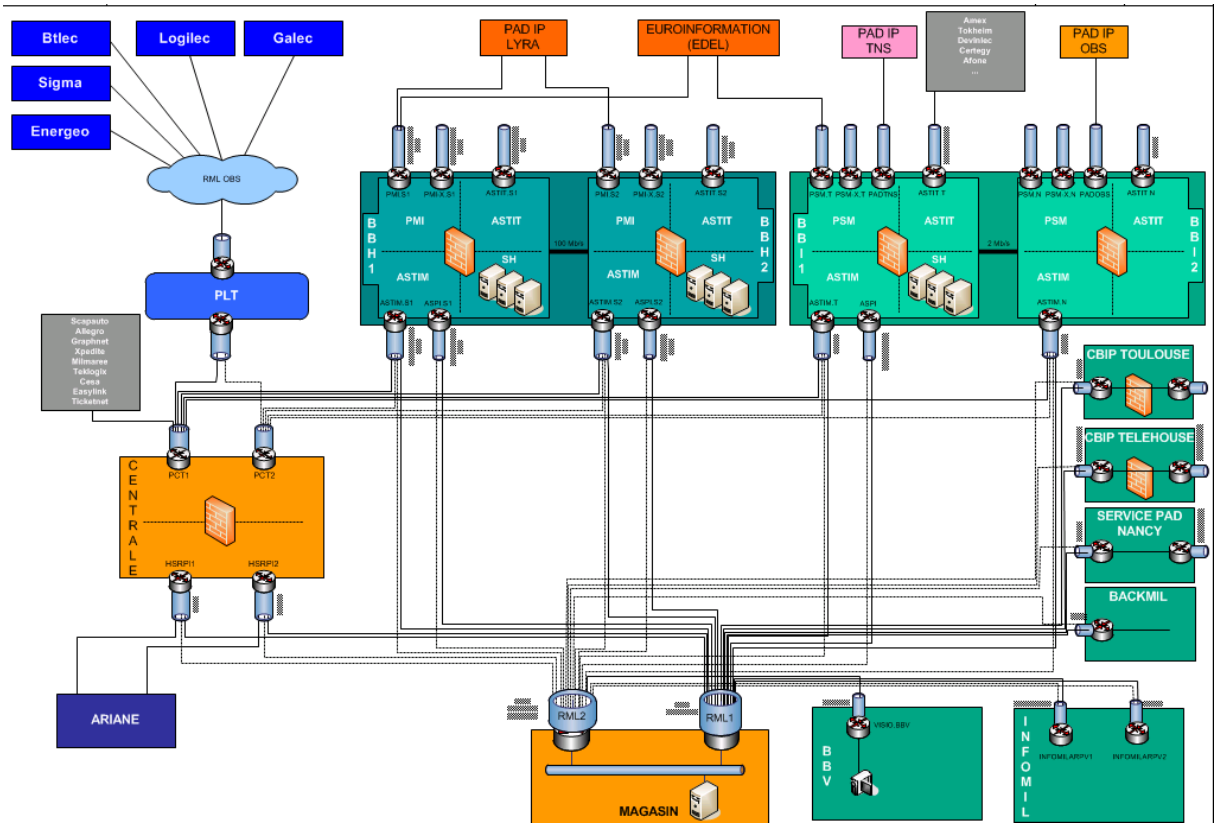
- la configuration renseignée sur les routeurs et l'accès en lecture sur la configuration de ces routeurs,

- les procédures de résolution en cas de panne,

- l'accès aux tickets d'incidents traitant de cette problématique au support pour suivre l'avancée de la résolution du problème,

- l'envoi automatique par mail à l'opérateur en cas de problème sur un accès.

Voici un exemple de schéma réseau magasin  ci-dessous  :




Cela  montre bien le nombre importants de tunnels vpn montés avec les différents prestataires externes, plus les routeurs centraux à surveiller.

Et ce pour un seul magasin !

Infomil équipe en système informatique à ce jour plus de 600 magasins Leclerc.

Ce schéma qui date de 2009, ne montre pas certains flux qui se sont rajoutés, notamment ceux nécessaires pour la supervision et la récupération de données via la console OSURI (via un tunnel vers un routeur intitulé ASPI-BBS) et les flux nécessaires pour le fonctionnement de Leclerc Drive en magasin (via un tunnel vers  un routeur intitulé ASTIMDRV-BBS)

Suite à l'étude du cahier des charges et des demandes clients énumérées ci-dessus, et l'étude de l'architecture réseau globale voici donc les outils développés :

- script de mise à jour automatique du firmware des routeurs,

- script de test de vie d'un équipement,

- script de latence,

- script de récupération de bande passante d'un équipement,

- script de récupération de valeurs sur routeur Cisco,

- une console de supervision. La récupération des informations routeur se fait via des requêtes SNMP. Ces récupérations se feront via des scripts Perl et intégrées dans une console de supervision Cacti,

- utilisation de l'application Nagios afin d'effectuer des surveillances, d'envoyer des mails automatique et de générer certains types d'alertes en cas de problème,

- génération d'alertes automatiques en cas de pertes de connexion sur un accès,

- génération de mails à 12h00 et 14h00 listant l'état des connexions du parc magasin

Pour ma part, je n'ai au final pas travaillé sur la console de supervision, j'ai travaillé uniquement sur la définition des indicateurs pertinents et à l'élaboration des scripts vbs.

Néanmoins, il est très important que je parle de cette console de supervision dans ce mémoire, car les fiches techniques rédigées à destination des techniciens se basent principalement sur cette console. De plus les alertes automatiques générées et les mails de surveillance arrivent directement à destination du support.

Il m'a donc été demandé de former les utilisateurs à l'utilisation de cette console. Pour cela il m'a fallu apprendre les tenants et les aboutissants de cette console. Pour terminer, il est en projet que j'élabore un dashboard pour surveiller la connectivité entre certains routeurs RML2 et le La110 FT branché dessus. Full duplex ? 100Mbps ? lien up ? présence d'erreurs crc sur l'interface ?

Nous y reviendrons donc plus tard.

Il faudra donc mettre en place des solutions adaptatives afin d'assurer la meilleure qualité de service chez nos différents clients. Des solutions de collecte et d'analyse d'indicateurs pertinents sur les équipements réseaux vont donc être mises en place.

## 1. Script de maj automatique des versions IOS Cisco

1er problème : uniformisation du parc avec la même version IOS sur les routeurs cisco selon leur modèle.

En effet, rien n'avait été fait sur les versions mises en place sur routeurs. Certaines versions obsolètes provoquaient notamment des pertes de paquets dues à des incompatibilités avec le DSLAM France TELECOM.

De plus, selon le modèle de routeur Cisco et la version IOS qui était mise en place sur ce routeur, les indicateurs n'étaient pas stockés au même endroit dans les mibs, ce qui pouvait poser problème parfois pour les récupérer sur la console de supervision CACTI

Voici comment a été mis en œuvre ce script :

- lecture du fichier source contenant l'adresse ip et le nom du routeur,

- vérification de la présence du fichier firmware sur le serveur,

- vérification de la présence du serveur tftp,

- vérification du modèle de routeur,

- lancement du service serveur tftp,

- connexion au routeur avec gestion login/mot de passe selon le type de routeur,

- faire en sorte que le routeur redémarre entre 2h00 et 3h00 du matin une fois la maj terminée pour éviter tout impact sur l'activité client en pleine journée,

- lancement des timers : de calcul durée de mise à jour et de timer de connexion (timeout au bout de 3h00),

- récupération de l'adresse ip du serveur tftp,

-lancement des commandes de maj selon les différents modèles de routeurs présents sur le parc,

Voici les principales commandes jouées :

*"Copy startup-config tftp:"*

*"Copy flash tftp:" vlan.dat et/ou dhcp-database*

*Format flash:*

*Copy tftp: flash fichier firmware, dhcp-database et vlan.dat*

Pour terminer :

- programmation du redémarrage du routeur,

- déconnexion du routeur,

- écriture des différents cas (réussi ou pas, cas d'erreurs) dans un fichier résultat.txt,

- arrêt du service tftp,

<u>Exemples de cas de dysfonctionnements :</u>

- pas de routeur compatible pour ce site,

- pas de lancement du serveur tftp,

- routeur inaccessible,

- telnet non accepté,

- pb login/mdp,

- fichier firmware absent,

- crc incorrect sur le fichier,

- ios déjà à jour,

- flash déjà à jour,

Et lors de la copie :

- pb tftp,

- pb copie vlan,

- pb copie dhcp,

- pb maj firmware,

- pb recup vlan,

- pb recup dhcp,

- pb checksum,

- commande non connue pour ce modèle,

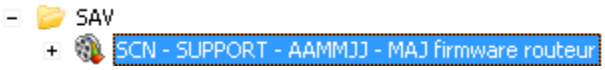
- autre problème

Pour executer massivement ce script sur notre parc de routeurs, nous avons fait le choix du logiciel MediaTransfer.

Je pars du principe que tous les équipements sont déjà configurés pour joindre ce serveur, situé dans nos locaux à Infomil Toulouse..

2 - Déploiement par Media Transfer

Voici le scénario qui a permis de déployer massivement ce script




Celui-ci exécute les commandes suivantes :

| Commande | Paramètres |
|---|---|
| Commentaire | mise a jour des firmware d'euipements réseaux |
| Commentaire | ********Début parametres à modifier********** |
| Commentaire | fichier sources des routeurs a mettre a jour |
| Commentaire | liste de diffusion media-transfert |
| Commentaire | ********Fin parametres à modifier********** |
| Appeler | SODICHAR-N032 |
| Envoyer | D:\Srv_020_(Fichiers)\ficZADS\Executable\Support Administration\SCN - SUPPORT - AAMMJJ - MAJ FIRMWARE ROUTEURS\tftpd32.exe |
| Envoyer | D:\Srv_020_(Fichiers)\ficZADS\Executable\Support Administration\SCN - SUPPORT - AAMMJJ - MAJ FIRMWARE ROUTEURS\tftpd64.exe |
| Envoyer | D:\Srv_020_(Fichiers)\ficZADS\Executable\Support Administration\SCN - SUPPORT - AAMMJJ - MAJ FIRMWARE ROUTEURS\tftpd32.ini |
| Envoyer | D:\Srv_020_(Fichiers)\ficZADS\Executable\Support Administration\SCN - SUPPORT - AAMMJJ - MAJ FIRMWARE ROUTEURS\MAJ_firmware.exe |
| Envoyer | D:\Srv_020_(Fichiers)\ficZADS\Executable\Support Administration\SCN - SUPPORT - AAMMJJ - MAJ FIRMWARE ROUTEURS\source_routeurs.txt |
| Envoyer | D:\Srv_020_(Fichiers)\ficZADS\Executable\Support Administration\SCN - SUPPORT - AAMMJJ - MAJ FIRMWARE ROUTEURS\Referenciel_materiel_firmware.txt |
| Exécuter distant | "c:\temp\support\MAJ_firmware\MAJ_firmware.exe" "resultat.maj" "Referenciel_materiel_firmware.txt" "source_routeurs.txt" |
| Rapatrier | c:\temp\support\MAJ_firmware\resultat.maj |
| Supprimer source | |
| Supprimer distant | c:\temp\support\MAJ_firmware\tftpd64.exe |
| Supprimer distant | c:\temp\support\MAJ_firmware\tftpd32.ini |
| Supprimer distant | c:\temp\support\MAJ_firmware\tftpd32.exe |
| Supprimer distant | c:\temp\support\MAJ_firmware\MAJ_firmawe.exe |
| Supprimer distant | c:\temp\support\MAJ_firmware\source_routeurs.txt |
| Supprimer distant | c:\temp\support\MAJ_firmware\Referenciel_materiel_firmware.txt |

1 - Appel du client, ou de la liste de clients pour lesquels il faut mettre à jour le routeur sur site

2 - envoi des fichiers nécessaires sur site :

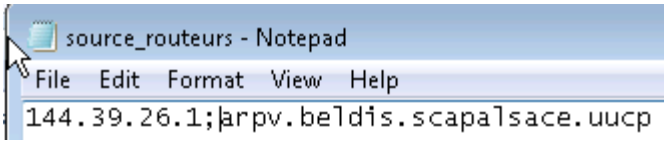
- serveur tftp,

- script de maj routeur,

- fichier source_routeurs.txt contenant la liste des routeurs à mettre à jour,

Le fichier doit respecter le formalisme suivant :

Adresse ip;nom complet dns




1 routeur par ligne.

- fichier "référentiel matériel firmware.txt" qui contient les différents modèles de routeur avec leurs versions firmware, IOS respectives

Referenciel_materiel_firmware - Notepad

File Edit Format View Help

```
repertoire contenant les firmwares sur site;\\distribution\$distributions$\_Atelier support\_SAV\outilsRouteurs\

modele routeur;firmaware;IOS;checksum;;config exclue;crc;
Cisco 888;c880data-universalk9-mz.152-2.T.bin;15.2(2)T;fb0270bb2b5f0fc543cb525b90da4dab;;9487E27F8
Cisco887;c880data-universalk9-mz.152-2.T.bin;15.2(2)T;fb0270bb2b5f0fc543cb525b90da4dab;;8487E27F8
Cisco 881;c880data-universalk9-mz.152-2.T.bin;15.2(2)T;fb0270bb2b5f0fc543cb525b90da4dab;;9487E27F8
Cisco 877;c870-advipservicesk9-mz.124-24.T7.bin;12.4(24)T7;1ddd9232d890d0ab43016f92b4e1ad86;;9304BAD68
Cisco 871;c870-advipservicesk9-mz.124-24.T7.bin;12.4(24)T7;1ddd9232d890d0ab43016f92b4e1ad86;;9304BAD68
Cisco 878;c870-advipservicesk9-mz.124-24.T7.bin;12.4(24)T7;1ddd9232d890d0ab43016f92b4e1ad86;;9304BAD68
cisco AIR-AP1242AG-E-K9;c1240-k9w7-tar.124-25d.JA2.tar;12.4(25d)JA2;--;;17A4F1000
cisco AIR-AP1242G-E-K9;c1240-k9w7-tar.124-25d.JA2.tar;12.4(25d)JA2;--;;16A4F1000
cisco AIR-AP1230B-E-K9;c1200-k9w7-tar.123-7.JA5.tar;12.2(8)JA;--;;168386000
cisco AIR-AP350-IOS-UPGRD;c350-k9w7-tar.123-8.JEA3.tar;12.3(8)JEA3;--;;197968000
```

3 - rapatrier le résultat

4- supprimer les fichiers qui ont été envoyés en local.

Ce scénario a été joué une fois par jour, à raison de 20 routeurs par jour.

Un fichier excel a été mis à jour pour suivre le déploiement de cette nouvelle version IOS.

Le redémarrage des routeurs ayant été programmé dans la nuit, cette mise à jour fut totalement transparente pour les magasins.

## 2. Console de supervision Osuri

La console de supervision Osuri est une interface graphique librement inspiré de Cacti.

Les valeurs récupérées des routeurs sont stockées dans une base .rrd (round robin database)

RRdTool est un outil de gestion de base de données, utilisé par Cacti (dans notre cas donc par Osuri).

Cet outil permet la sauvegarde cyclique de données et le tracé graphique de données chronologiques.

Exemple de données pouvant être récupérées : température d'un processeur, bande passante utilisée par un routeur, sa mémoire utilisée...

Cacti permet d'afficher de manière graphique des performances réseaux ou serveurs, en se basant sur des indicateurs présents sur les équipements supervisés.

Il permet donc de faire des études d'indicateurs sur une période donnée, mais ne permet pas de connaître la mesure de l'indicateur en temps réel ( à 5 minutes près).

A l'aide de templates, ce logiciel permet de créer de manière générique des graphiques dans le but de pouvoir les réutiliser dans le temps.

Afin de mieux appréhender cette console, qui est relativement complexe, il m'est obligé d'aborder un peu de théorie sur les protocoles suivants avant de lister les différents indicateurs qui ont été récupérés :

- SNMP

- Cacti

- Rrdtool

## 2.1. SNMP

Les indicateurs sur routeur sont récupérés via des requêtes snmp

Snmp, pour Simple Network Management Protocol est un protocole de gestion de réseaux et d'applications.

L'environnement de gestion snmp est constitué de quatre composantes :

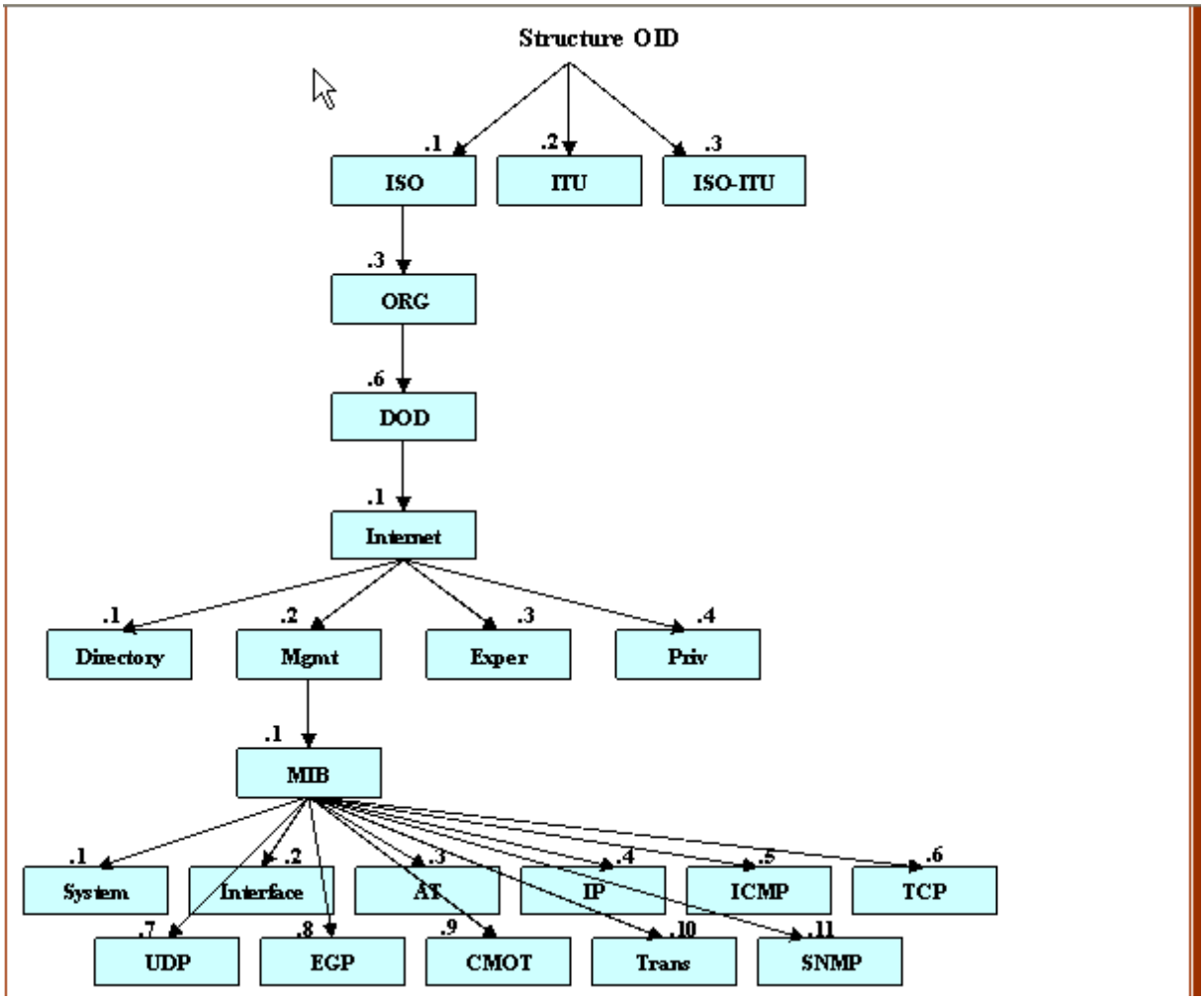
- Les équipements gérés (commutateurs, routeurs, ponts, serveurs...). Ce sont des éléments contenant des objets de gestion appelés "agent"; L'agent présent sur l'équipement supervisé répond aux requêtes de la station de supervision. Ces agents vont chercher les objets de gestion sur les équipements comme par exemple des informations sur le matériel, le nombre de paquets reçus ou transmis par cet équipement.

- la station de supervision. Il s'agit en général d'un poste de travail, elle exécute les applications de gestion qui contrôlent les éléments réseaux.

- les agents (MIB). Collection d'objets résidant dans une base d'information virtuelle.

La MIB est une structure arborescente dont chaque nœud est défini par un OID (Object Identifier). Chaque équipement à superviser possède sa propre MIB

Voici un exemple de structure table OID.




Par exemple, si on veut récupérer la donnée Mgmt il faut donc appeler l'OID 1.3.6.1.2

- le protocole snmp qui permet à la station de supervision d'interroger les équipements réseaux, et de recevoir des alertes si nécessaire.

SNMP est un protocole réseau de niveau 7 du modèle OSI.

SNMP utilise le protocole UDP. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents.

Il existe quatre types de requêtes :

- GetRequest : permet la recherche d'une variable sur un agent

- Getnextrequest : permet la recherche de la variable suivante

- GetBulk : permet la recherche d'un ensemble de variables regroupées

- SetRequest : permet de changer la valeur d'une variable sur un agent

La réponse SNMP sera systématiquement obtenue par un GetResponse.

En effet, s'agissant des routeurs et conformément à nos règles d'ingénierie, le choix a été fait d'aller chercher les informations directement sur les routeurs Cisco. Ce ne sont pas eux qui généreront des alertes.

Une exception tout de même : le push d'information a été mis en place sur des serveurs critiques (serveurs hébergés notamment). Mais ce sont des cas isolés.

Pour terminer, l'outil net-snmp permettra au mieux d'utiliser ces requêtes, et nous permettra surtout d'utiliser le snmpwalk qui permet de faire des getrequest successifs.

Exemple de requête snmp pour récupérer la version IOS selon le modèle de routeur (voir annexe ci-dessous pour script perl intégral)

snmpwalk -On -v2c -c edifie $ip 1.3.6.1.2.1.1.2.0

-On : permet d'afficher numériquement l'OID

-v2c : version de snmp

-c : community (dépend du fichier de configuration snmp)

$ip : adresse ip du routeur

1.3.6.1.2.1.1.2.0 => OID

Apres recherche, le nombre d'indicateurs récupérables et affichables sont beaucoup trop volumineux.

Nous ne parlerons pas des alertes car celles-ci ne seront pas utilisées dans notre cas.

En effet, tout dépend des mibs à disposition, et ces mibs varient selon le modèle de routeur, le modèle d'IOS... il n'est donc pas utile de lister toutes les variables récupérables par modèle de routeur et d'IOS.

Pour les mibs : Sur le site Cisco : on peut trouver : quelle mib pour quel routeur => http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Dans notre cas, une dizaine de mibs différentes sont utilisées, et sont exploitées avec l'outil net-snmp en multithreading à travers des librairies perl ou php. Il serait fastidieux et inutile de les lister.

Les indicateurs récupérés seront énumérés suite à la présentation de la console Osuri.

Nous allons maintenant aborder le fonctionnement générique de rrdtool, qui permet le stockage en base de données des valeurs des indicateurs récupérés.

## 2.2. Rrdtool

Round Robin Tool. Il s'agit d'un logiciel qui permet la gestion de base de données .rrd .

Il permet donc notamment le stockage des indicateurs liées à la console de supervision Osuri

Fonctionnement global :

Lorsqu'on surveille l'état d'un système, il est pratique d'avoir les données disponibles de manière régulière dans le temps. Malheureusement, il peut être parfois laborieux de récupérer la donnée à l'heure exacte que l'on souhaite. Rrdtool permet de récupérer les données suivant l'intervalle de temps pour lequel vous l'avez paramétré et va automatiquement la stocker en base.

Grâce à rrdtool il est possible ensuite de consulter les données avec 1 minute d'intervalle par exemple, mais vous pourrez également effectuer une moyenne des valeurs des données relevées.

En effet, lorsque vous créer et configurez votre base de données rrd, vous définissez l'intervalle de temps pour lequel les données seront récupérées, et quel type de calcul vous souhaitez effectuer par rapport à ces valeurs :

Moyenne des valeurs relevées ? Minimums ? Maximums ? Total ? Dernière ?

Il est possible de plus, de faire plusieurs calculs pour un graphe par exemple.

L'avantage majeur est que les données sont conservées dans le temps de manière périodique.

Les archives sont conservées sur une période de temps prédéfinie. Une fois cette période écoulée, les données sont automatiquement écrasées par les suivantes.

La base. rrd est toujours de taille fixe.

Exemple d'utilisation :

Vous voulez stocker 200 valeurs d'un indicateur sur un intervalle de 5 minutes, la base rrd allouera un espace pour 200 valeurs et un en-tête. Dans l'en-tête sera stocké un pointeur pour indiquer dans quel espace a été écrite la dernière valeur. Les nouvelles valeurs seront donc inscrites dans l'archive RRA (Round Robin Archive) de manière cyclique. Cela limitera automatiquement le nombre de données à 200. Mais vous pouvez très bien dans une RRd stocker plusieurs RRA.

Exemple :

1 archive avec 200 valeurs sur un intervalle de 5 minutes, une seconde archive de 1000 valeurs sur un intervalle de 2h00, et enfin une dernière avec 100 valeurs par exemple sur un intervalle de 60 jours, ce qui vous permet de conserver un historique (moins fin que les deux autres).

Ce fonctionnement garantit donc de manière efficace le non grossissement de la base de données. Les données anciennes sont automatiquement écrasées. On connait dès le début la taille de la base.

De plus il est possible, lors de la définition de la base, de choisir de conserver un certain nombre de valeurs plus longtemps, pour avoir une période d'historique plus importante.

Ces différentes utilisations nous permettront, par exemple, de connaitre l'utilisation de la bande passante sur les 5 dernières minutes, la disponibilité du lien LAN, la quantité de trafic sur les 10 dernières minutes sur un lien ATM…

Rrdtool permet des générer des rapports au format numérique ou graphique en se basant sur les données stockées dans une ou plusieurs bases de données rrd. Le graphe est bien sûr pleinement configurable. Taille, couleur, contenu du graphe...

Enfin, et non des moindre, cet outil peut permettre également de détecter un comportement anormal sur les valeurs relevés via :

- un algorithme pour prédire les valeurs relevées dans le temps

- Une mesure des déviations entre ce qui est prédit et les valeurs observées.

- un mécanisme qui permet de dire si une valeur ou une séquence de valeurs sont anormales par rapport à ce qui devrait-être.

Ce mécanisme permet donc de relever de manière aisée les potentielles pannes sur les équipements surveillés.

Cet outil a été créé par Tobias Oetiker. Osuri s'appuie sur cet outil pour sauvegarder des données et effectuer des tracés de graphique de manière chronologique. Grâce à cet outil, il est possible de superviser la température d'un serveur, récupérer des données matérielles sur un équipement, la disponibilité d'une connexion ADSL, SDSL…

IL s'agit d'un outil de base de données, exploité par Cacti. Osuri dans notre cas.

### 2.3. Cacti

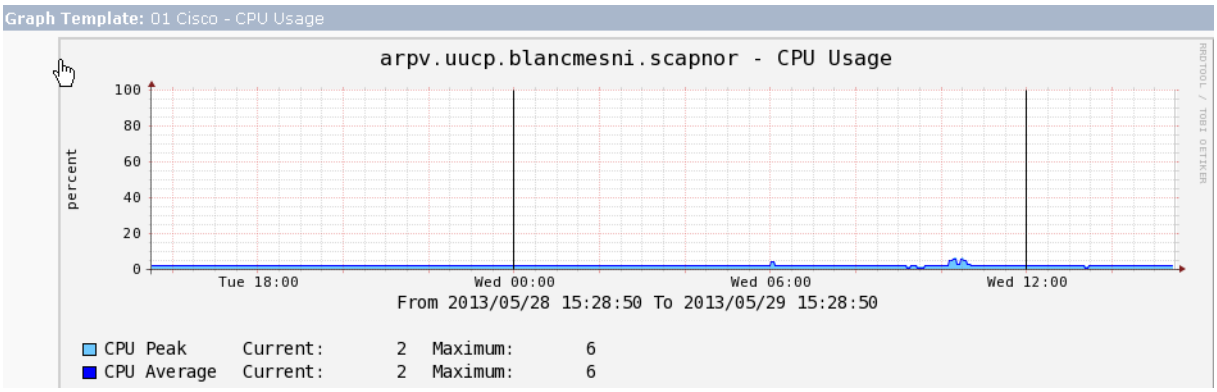
Cacti est un logiciel de supervision basé sur rrdtool. Il permet d'afficher des graphiques en se basant sur les différents paramétrages effectués sur rrdtool.

Cacti nécessite un serveur apache, une base de données Mysql/php pour fonctionner correctement.

### 2.4. Présentation des indicateurs récupérés sur Osuri

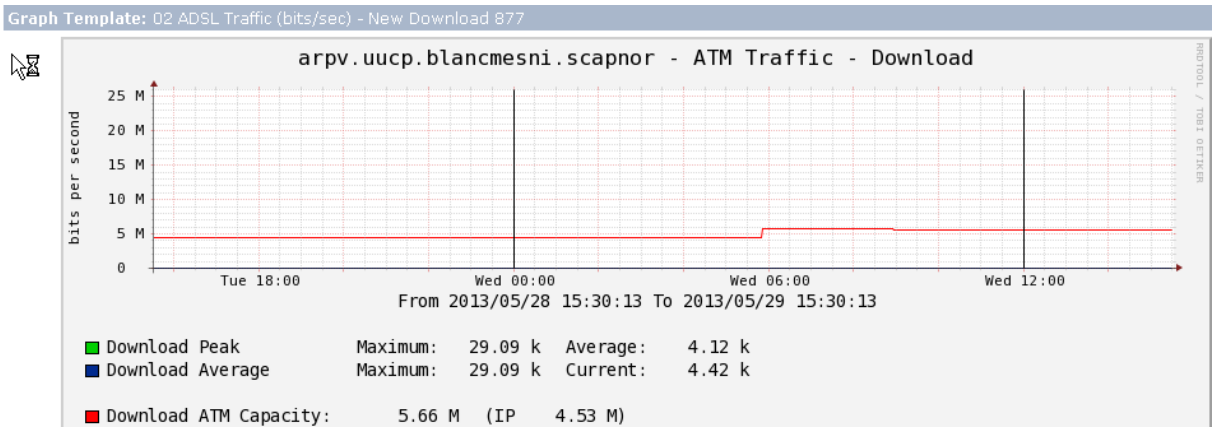
Osuri étant librement inspiré de Cacti, voici plusieurs exemples d'indicateurs que nous avons jugé bon de récupérer :

- Cpu usage




Ce graphe permet dans le temps de connaître l'évolution de la charge cpu d'un routeur.

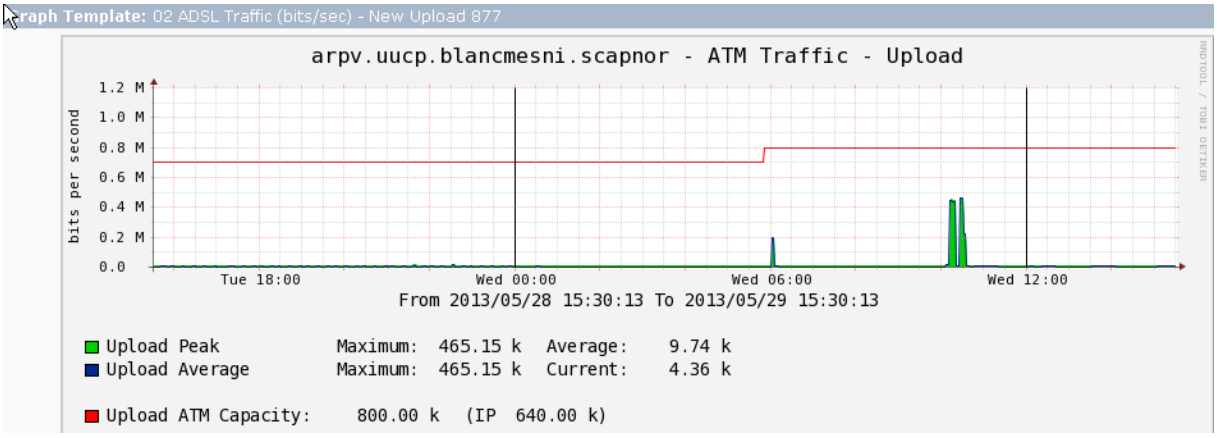
- ATM Traffic download




Ce graphe permet de récupérer la valeur en download de l'interface ATM du routeur.

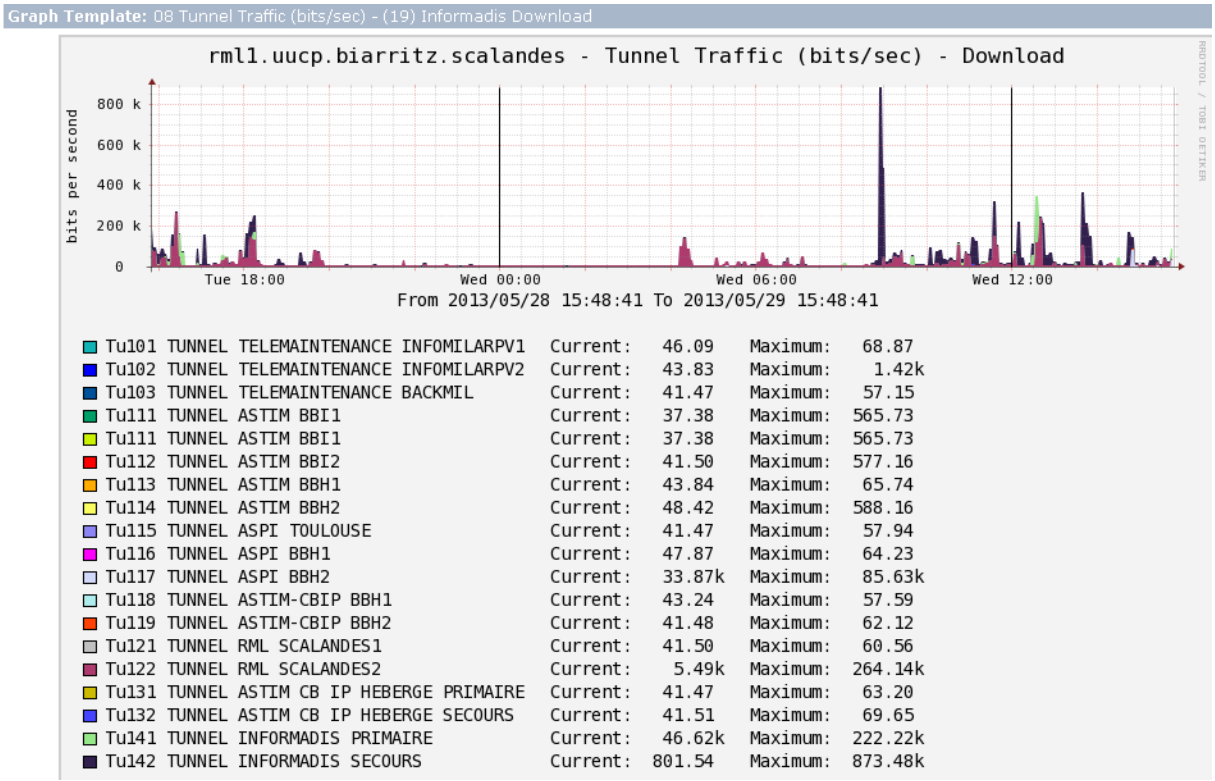
On peut donc facilement voir si le routeur est saturé ou non.

- Traffic Upload sur patte ATM



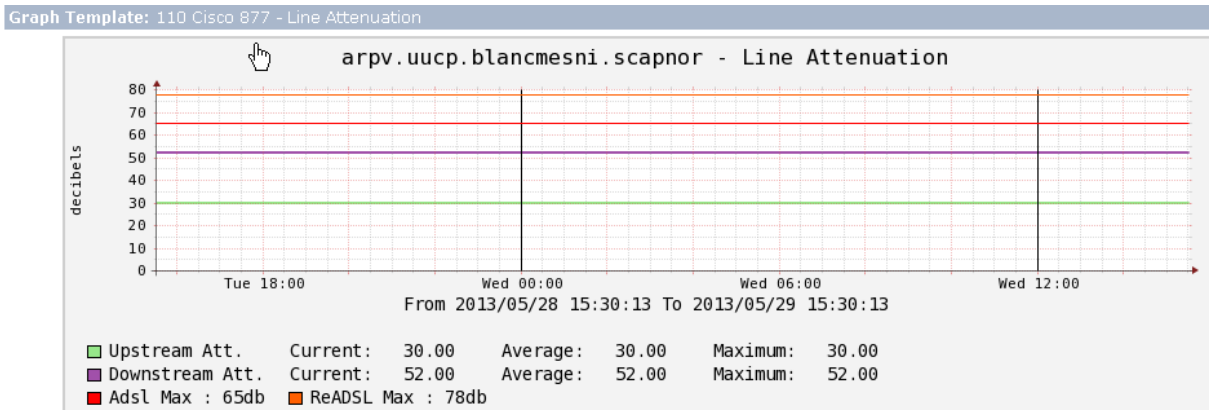

Même principe que l'ATM traffic download, mais cette fois ci dans le sens montant (magasin vers extérieur)

- Traffic par tunnel en download/upload (uniquement sur routeurs rml)




Permet de voir si un tunnel bgp utilise de manière anormal la bande passante en download ou en upload.

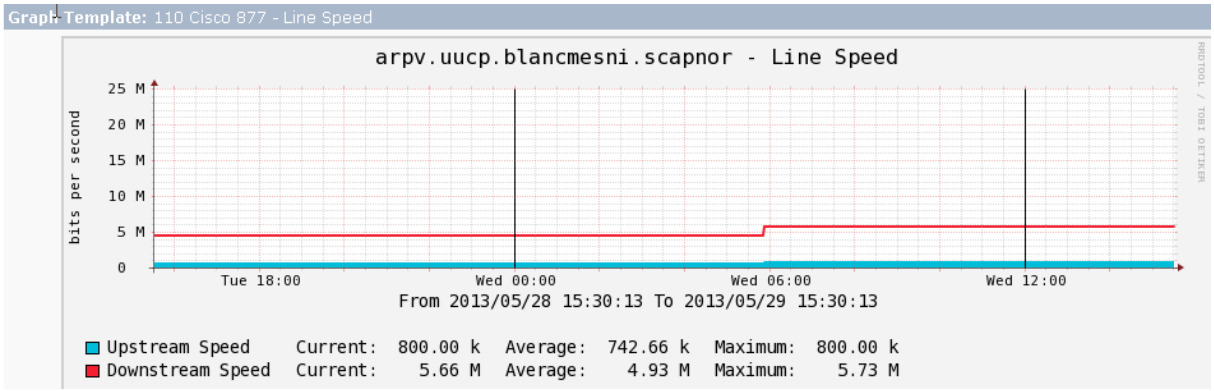
-Atténuation de la ligne




L'atténuation est calculée en fonction de la distance qui sépare le NRA de la boucle locale magasin et le diamètre de la section de la paire de cuivre

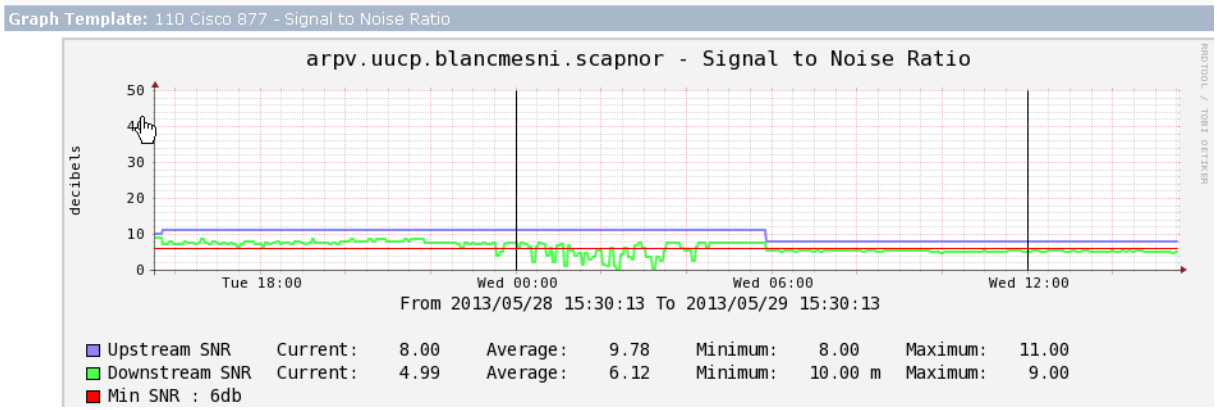
Plus l'atténuation est faible, plus les débits seront élevés.

-Vitesse de la ligne




Permet de connaître la vitesse de syncrhonisation de la ligne en download/upload

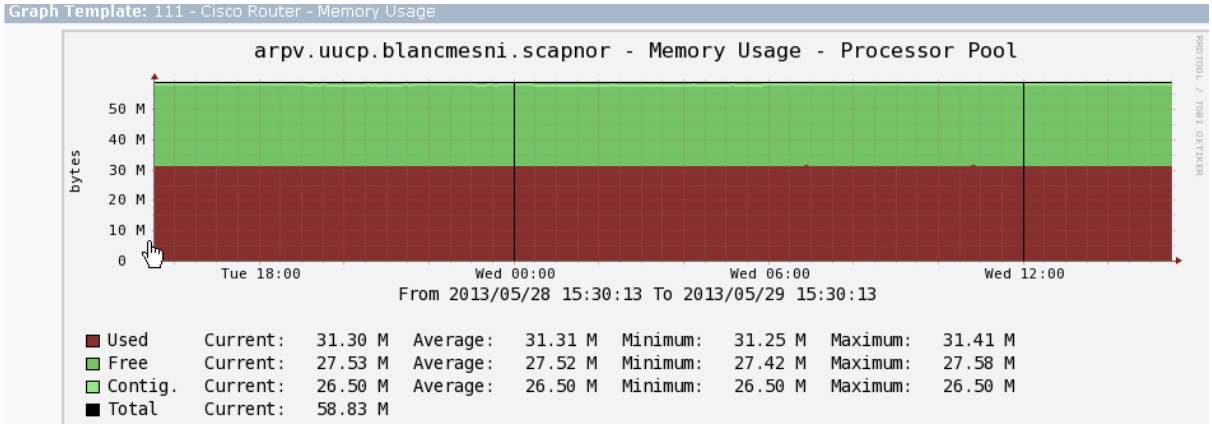
- Signal marge bruit




Le SNR (signal to noise ratio) est la mesure en décibel de la force du signal par rapport au bruit sur la ligne.

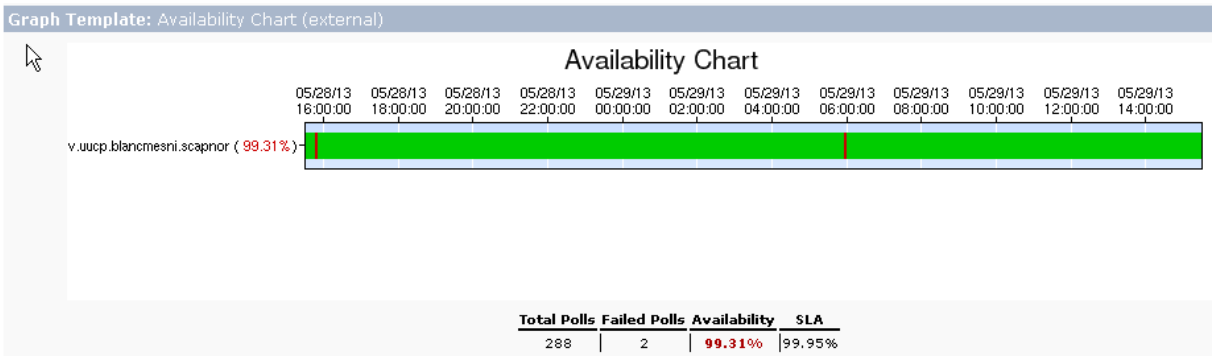
Plus la valeur de SNR est élevée, meilleure est la qualité de la ligne.

- Mémoire utilisée sur le routeur




Ce graphe montre la mémoire libre et utilisée sur le routeur

- Availability Chart (issu de nagios)

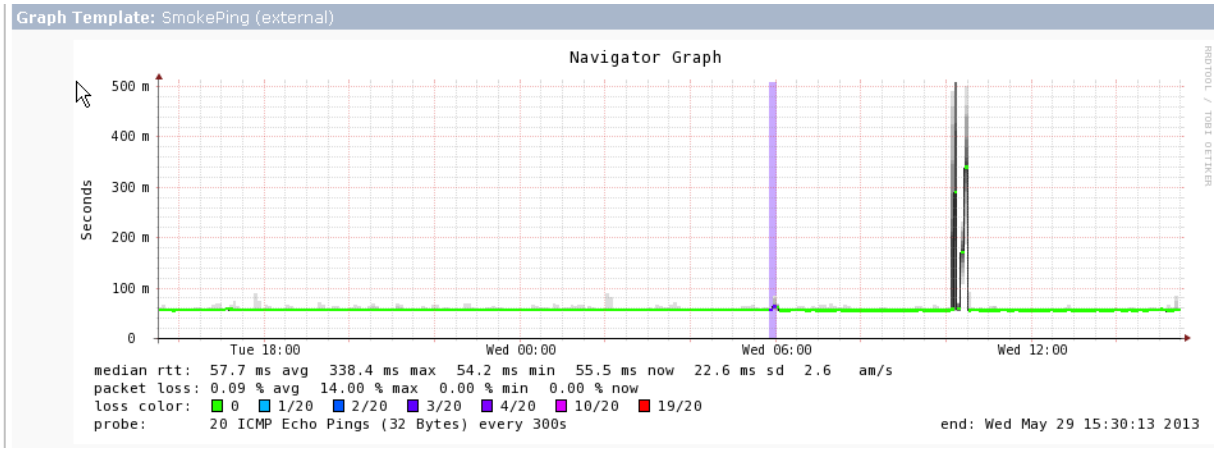



Ce graphe permet de voir de manière rapide la disponibilité du service.

Rouge : coupure

Vert : service opérationnel

- Smokeping




Ce graphe permet de connaitre les pertes de paquets subies par l'équipement réseau et la latence sur l'accès.

Toutes les 300 secondes 20 paquets icmp sont envoyés

La valeur médiane de ces 20 paquets est indiquée par un point sur le graphique

La valeur des 20 paquets est ensuite indiquée successivement en fond avec un aplat de couleur grise

Cette console permet une première analyse en cas de problème, mais manque malheureusement un peu de finesse.

Cet outil évite aux techniciens de se connecter au routeur et de récupérer manuellement via des commandes Cisco les différentes valeurs relevées sur ce graphe. De plus, ces différentes valeurs étant conservés dans le temps, il est possible de voir de manière simple et efficace si un dysfonctionnement a eu lieu, et de situer l'anomalie à 5 minutes près. (Les valeurs sont récupérées toutes les 5 minutes)

Néanmoins, du fait de ces 5 minutes lors des récupérations des valeurs, l'analyse se doit d'être encore plus fine dans certains cas. Avec cet outil, il est relativement difficile par exemple d'isoler des pertes de paquets sur une courte période de temps par exemple.

D'où la nécessité de développer des outils supplémentaires afin d'effectuer des surveillances permanentes sur les équipements en cas de besoin.

## 3. Scripts de surveillance

Afin de mettre en place des outils de surveillance plus fin, des scripts ont donc été développés par notre équipe d'ingénieur support.
Une aide à l'utilisation de ces scripts a été rédigée à l'attention des techniciens.

Les résultats sont incorporés dans un fichier texte et peuvent ensuite être exploités sous forme de graphique sous Excel 2010

### 3.1. Test de vie d'un équipement local en magasin

Ce script s'appuie sur un ping lancé toutes les secondes avec un time-out fixé à 500ms.

Un fichier texte est généré dans lequel n'apparaissent que les éventuelles déconnexions.

Il a permis de mettre en évidence un problème d'indisponibilité d'une imprimante dans la nuit, ce qui provoquait un dysfonctionnement lors de la fermeture magasin.

### 3.2. Test de latence réseau

Cet utilitaire permet de lancer un ping vers une machine tiers.

Une série de 100 pings est lancée.

On récupère alors la date à laquelle la série de ping a été effectuée (avec les secondes), le % de pertes de paquets, le temps max, le temps moyen et le temps min pour joindre l'ip paramétrée.

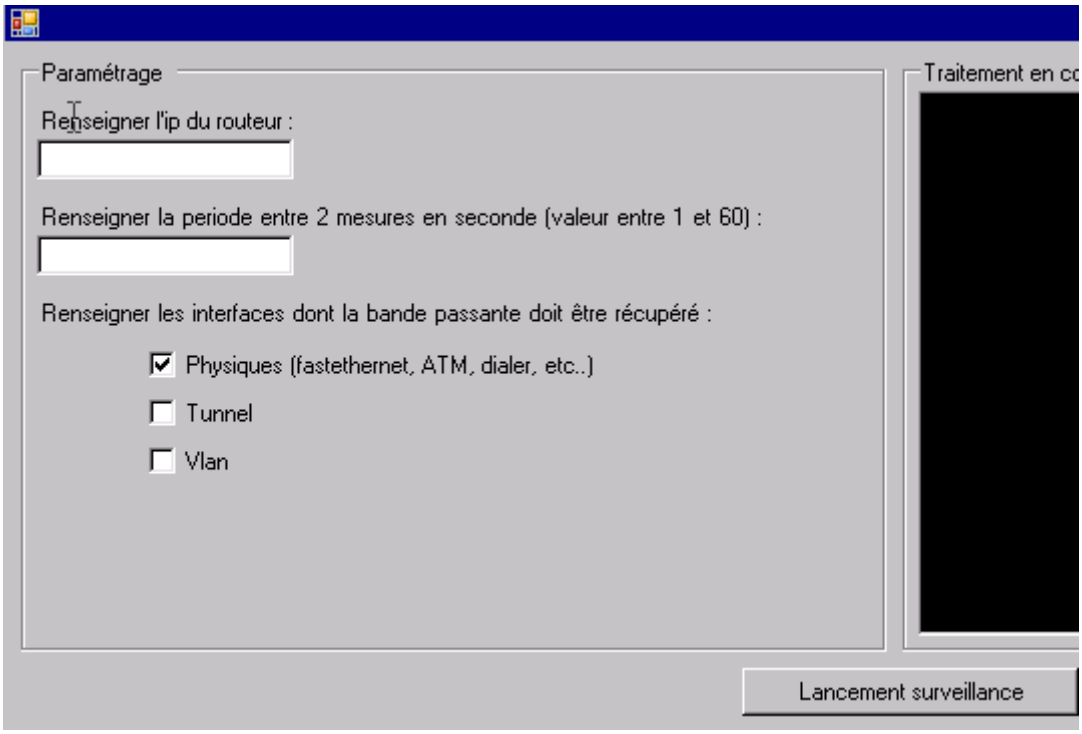
Exemple de fichier résultat :

```
jour/mois/annee;heure;% de pertes;tps max;tps moyen;tps min;
04/06/13;16:37:29;0;0;0;0;
04/06/13;16:37:34;0;0;0;0;
04/06/13;16:37:39;0;0;0;0;
04/06/13;16:37:45;0;1;0;0;
```

Cet utilitaire a permis de déterminer dans un cas précis que les coupures applicatives dont était sujet le magasin étaient dues à des temps de latence élevés et non à des pertes de paquets.

### 3.3. Récupération bande passante des interfaces d'un routeur

Cet utilitaire permet de récupérer en temps réel la bande passante des interfaces actives d'un routeur (ATM, DIALER...) d'un équipement Cisco (commutateur, routeur...)




Il faut saisir l'adresse ip du routeur ainsi que la période de récupération des informations.

Les résultats sont transmis sous format .txt, mais pour pouvoir être exploitable, il faut ensuite les importer sous Excel sous forme de graphes

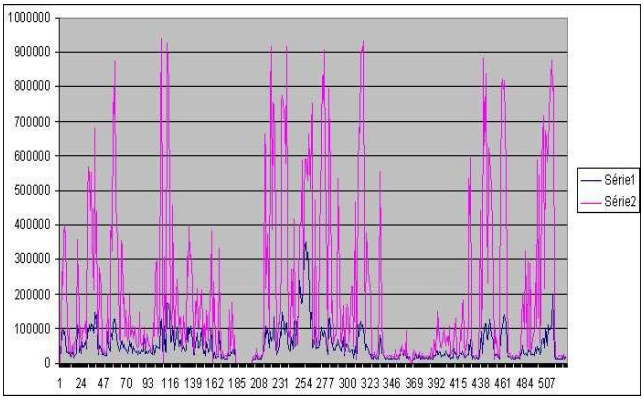
Fichier résultat (valeur en kbits/s)

resultat_test_BW_140.14.26.1.txt - Bloc-notes

Fichier Edition Format Affichage ?

```
heure;ATM0 download;ATM0 upload;Dialer1 download;Dialer1 upload;FastEthernet0 download;
15:43:35;3705;7229;-6817;7136;113;53;2052;4154;16;14;16;14;0;0;
15:43:46;-15689;-30232;-10687;-29269;1038;523;-8655;-14748;-69;-16;-29;-31;-5;-9;
15:43:50;9964;19834;20630;20044;4036;2042;5131;15504;17;14;0;0;14;17;
15:43:55;11853;22587;23121;21167;4410;2384;5010;14184;7;9;7;9;14;17;
15:44:00;10928;20936;204;20462;4423;2421;5027;14925;7;9;7;9;0;0;
15:44:06;10420;20362;-710;19736;3992;2139;4874;14144;0;0;0;0;0;0;
15:44:16;9840;18495;19637;17919;4072;2143;4169;12656;9;7;9;7;9;7;
15:44:26;7466;14298;14733;13849;3932;2031;3077;10668;7;9;0;9;7;9;
15:44:36;7923;14920;-11627;14447;3963;2075;3086;11169;365;0;14;9;0;0;
15:44:46;7303;14179;14470;13745;3958;2067;3077;10672;9;7;9;7;9;7;
15:44:56;7346;14186;14516;13728;3942;2044;3093;10683;7;9;0;0;7;9;
15:45:05;7222;14090;-7634;13675;3972;2120;3092;10681;0;0;7;9;0;0;
15:45:16;7463;14315;14728;13852;4042;2108;3077;10660;24;20;24;20;9;7;
15:45:25;7424;14252;14745;13793;3941;2057;3077;10661;0;0;0;0;7;9;
15:45:36;7209;14078;-7585;13668;3937;2060;3099;10678;22;24;7;9;0;0;
15:45:46;7348;14216;14490;13748;3928;2051;3077;10661;0;0;17;14;23;14;
15:45:55;7338;14162;14535;13717;3931;2060;3077;10661;0;0;0;0;7;9;
15:46:05;7324;14157;-6739;13702;3963;2119;3092;10677;16;16;7;9;37;66;
15:46:16;7235;14092;14284;13674;4035;2108;3077;10662;0;0;9;7;0;0;
15:46:26;7310;14153;14526;13707;3996;2093;3073;10662;0;0;0;0;28;22;
15:46:36;7339;14189;-6926;13731;3964;2085;3117;10707;22;24;7;9;0;0;
15:46:46;7294;14211;14420;13765;3940;2033;3077;10745;56;0;9;7;0;0;
15:46:55;7297;14173;14568;13790;3946;2060;3086;10688;16;14;16;14;20;16;
15:47:05;7354;14216;-7124;13696;3930;2053;3084;10684;16;16;7;9;0;0;
```

Importation sous Excel qui permet un meilleure lisibilité




Cet utilitaire a pu régler de nombreux cas de saturation de bande passante par un équipement bien précis. Exemple :

Une caisse vérolée, une caisse qui tente de charger en boucle un fichier et qui sature le réseau, un équipement qui fait du transfert de données massif.

La console de supervision n'était pas assez "filtrante" pour pouvoir résoudre ce genre de problèmes.

# RESULTATS

Voici donc les procédures qui ont été rédigées à l'attention des techniciens support.

Ces procédures se basent principalement sur la visualisation des graphes Osuri, et comportent quelques commandes Cisco à afficher pour affiner le debugging.

En suivant, des cas d'utilisations des scripts au sein du support ont été également détaillés.

## 1. Rédaction de fiches à l'attention des techniciens

CAS 1 : Procédure RML : ATM traffic download > 80% pendant 5minutes

Informations à collecter pour poser le contexte de la problématique :

Type de routeur : ## arpv, rml, arpvd##

Modèle de routeur : ## à compléter##

Version IOS du routeur : ## à compléter##

Rappels et informations clés :

**Atm traffic download : signification**

L'interface Atm (Asynchronous Transfer Mode) est l'interface sur laquelle transitent les données ADSL entre le magasin et l'extérieur; Cet indicateur permet donc de vérifier le trafic entrant sur notre routeur.

**Symptômes d'un trafic entrant trop important**

- Bande passante saturée

- Perte de paquets ou temps de réponse important lors d'un ping

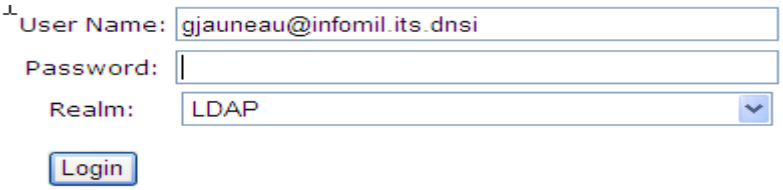
- Lenteur générale lors de la navigation sur internet

- Perturbation des applications dont les flux passent par ce routeur

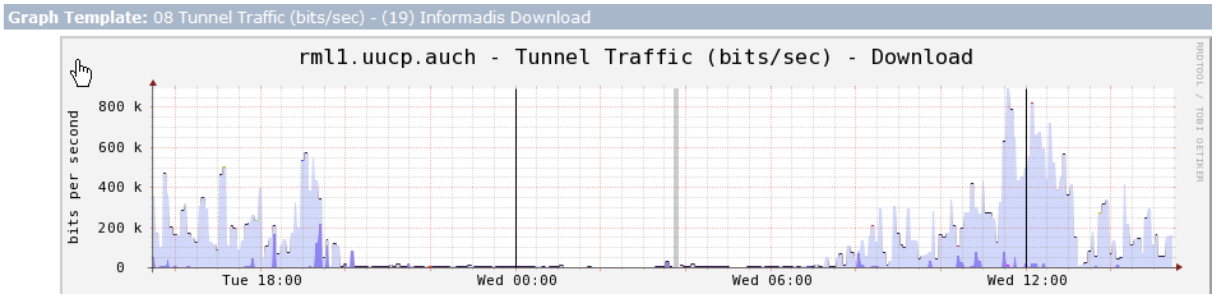
**Debugging**

1 - connexion sur la console Osuri

Renseigner votre login/mdp puis cliquez sur login




Sélectionner ensuite le routeur qui est remonté en anomalie puis allez voir le graph "Tunnel Traffic - Download" afin de pouvoir déterminer quel tiers ou qui sollicite fortement ou à tort le routeur




2 - connexion sur le routeur

Depuis gestion.infomil :

*Rlo -ry "nom_routeur.nom_magasin"*

*Password : xxxxx*

*En*

*Password : xxxxx*

3 - Commandes utiles :

=> Clear ip accounting /* cette commande permet d'effacer la table des données des différentes adresses ip qui ont fait transiter des informations par le routeur */

Attendre une vingtaine de secondes et taper la commande suivante :

=> Sh ip accounting

```
9MANDIS-RML1#sh ip accounting
   Source          Destination          Packets          Bytes
172.25.1.102     149.57.25.102            1509         852039
216.57.211.252   216.57.211.255              4            384
208.29.211.190   149.57.3.12                 4            192
216.57.211.248   216.57.211.255              8            768
```

Relever l'adresse ip qui génère le plus de paquets/octets. Essayer de déterminer qui administre ce réseau.

4 - Actions à mener

1) En fonction des différents éléments collectés (tunnel, adresse source/destination) essayer de déterminer le "coupable". (qui ? pourquoi ? utilisation normale ? virus ?)

2) Demander au responsable informatique du magasin s'il a connaissance d'un téléchargement ou d'une utilisation importante de bande passante.

3) En dernier recours, redémarrer le routeur et solliciter les Ingénieurs supports pour analyse plus poussée

CAS 2 : Procédure RML : Cpu du routeur RML > 85%

Informations à collecter pour poser le contexte de la problématique :

Type de routeur : ## arpv, rml,arpvd##

Modèle de routeur : ## à compléter##

Version IOS du routeur : ## à compléter##

Rappels et informations clés :

**Le cpu sur routeur : qu'est-ce que c'est ?**

Le processeur, ou CPU, est le composant de l'ordinateur qui exécute les programmes informatiques. Il permet donc, sur un routeur, d'exécuter le calcul des règles de routages, des algorithmes, et d'effectuer les instructions nécessaires au bon fonctionnement du routeur entre autres.

**Quels peuvent être les symptômes d'une utilisation importante ou anormale de cpu sur routeur ?**

- des baisses constatées au niveau des performance du routeur

- telnet impossible ou connexion telnet très lente

- temps de réponse importants lors d'une commande sur routeur

- perte de paquets ou temps de réponse importants lors d'un ping

- le routeur n'arrive plus à envoyer ses tables de routages aux autres routeurs

**Debugging :**

1 - connexion  sur routeur

Depuis gestion.infomil :

*Rlo -ry  "nom_routeur.nom_magasin"*

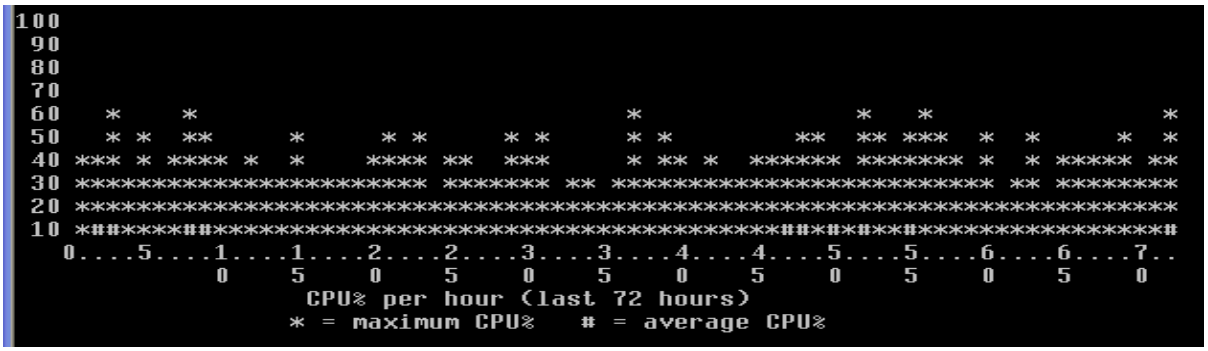
*Password : xxxxx*

*En*

*Password : xxxxx*

2 - commandes utiles

=> Sh processes cpu history :




Ce graphique permet de voir, en pourcentage, l'utilisation du cpu max sur les 72h et l'utilisation moyenne.

On devrait donc voir plafonner à un moment l'utilisation cpu à plus de 85% si une alerte a été générée

=> Sh processes cpu  sorted 5min :

Cette commande permet d'afficher par ordre décroissant les processus qui utilisent le plus le cpu sur les cinq dernières minutes => relever les processus les plus gourmands en cpu

=> Sh log :

Affiche les différentes anomalies constatées par le routeur

3 - Actions à mener

Une fois les éléments collectés :

1 ) Déterminer à quoi correspond ce process gourmand.

2) Ce cas a-t-il déjà été recensé ? => faire une recherche dans les talomi afin de voir si des actions ont déjà été menées sur ce type de problème ou sont en cours

3) Faire l'historique des problèmes sur ce routeur. Pb déjà rencontré ? Fréquence du pb ?

4 ) En dernier recours, monter en escalade niveau 2 si la cause du problème n'a pu être déterminée pour analyse affinée, et redémarrer le routeur si problème bloquant pour le magasin.

CAS 3 Procédure RML : atténuation > 50db ou fluctuation régulière

Informations à collecter pour poser le contexte de la problématique :

Type de routeur : ## arpv, rml,arpvd##

Modèle de routeur : ## à compléter##

Version IOS du routeur : ## à compléter##

Rappels et informations clés :

L'atténuation : qu'est-ce que c'est ?

L'**atténuation** est la réduction de l'amplitude et de l'énergie d'un signal à travers le média qu'il traverse. Autrement dit, plus la distance qui sépare le magasin du Dslam est courte, meilleurs seront les débits; Plus l'atténuation sera faible, meilleurs seront les débits. En théorie : Cette atténuation est calculée selon deux paramètres : la distance jusqu'au Dslam et le diamètre des lignes. Plus le diamètre des lignes est important, plus l'atténuation est faible; Dans les faits, selon l'age de la ligne, l'oxydation de la paire cuivre, la desserte interne du magasin etc..., ce paramètre peut varier également

Conséquences d'une atténuation trop importante ?

- Bande passante disponible plus petite que ce qu'elle devrait.

- Perte de paquets

- Perte de connexion

- Temps de réponse important

**Debugging :**

1 - connexion  sur routeur

Depuis gestion.infomil :

*Rlo -ry  "nom_routeur.nom_magasin"*

*Password : xxxxx*

*En*

*Password : xxxxx*

2 - commandes utiles

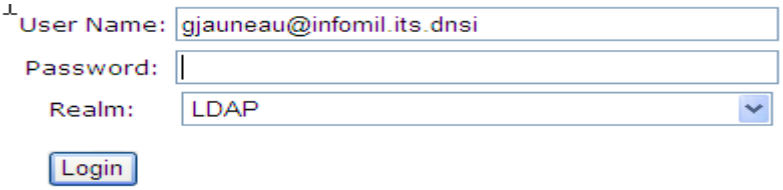
=> Sh dsl int atm0

Valable uniquement sur les routeurs ADSL

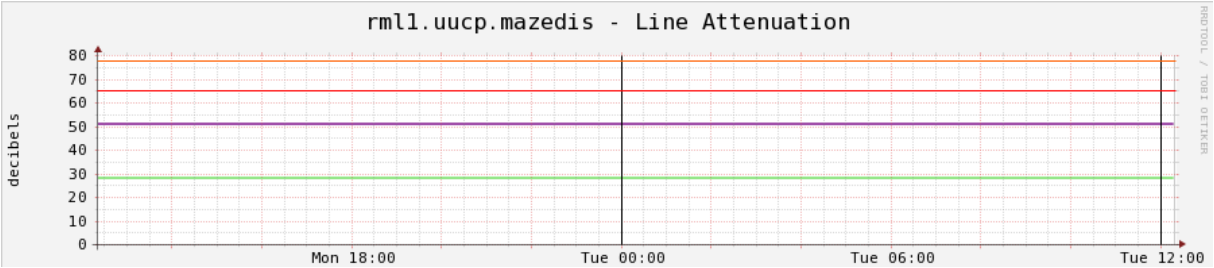
Cette commande permet de retourner quelques données intéressantes sur la ligne ADSL. Dans notre cas, c'est la valeur d'atténuation qui nous intéresse => la relever.

2 - Connexion sur la console Osuri

Renseigner votre login/mdp puis cliquez sur login



Sélectionner ensuite le routeur qui est en anomalie et vérifier sa valeur d'atténuation et vérifier qu'il n'y ait pas de fluctuation régulière




4 - Actions à mener

Dans ce genre de cas, on a à faire à une problématique d'ordre matériel ou environnementale

1) Solliciter l'opérateur. Essayer de savoir si des travaux ont eu lieu sur la ligne. La vétusté de la ligne peut être en cause. Ouvrir un incident dans tous les cas

2) Demander à l'opérateur la distance entre le Dslam et le magasin

3) Se renseigner auprès du magasin si des travaux n'ont pas lieu actuellement à l'hyper. Demander au magasin de faire vérifier sa desserte interne si pas de problème détecté par l'opérateur sur la ligne.

Cas 4 : Procédure RML : signal marge bruit : < 6db ou fluctuation régulière

Informations à collecter pour poser le contexte de la problématique :

Type de routeur : ## arpv, rml, arpvd##

Modèle de routeur : ## à compléter##

Version IOS du  routeur : ##à compléter##

Rappels et informations clés  :

**Signal marge bruit**  : signification

La marge au bruit est la différence entre les parasites présents sur la ligne et le signal ADSL. Plus la marge bruit est élevée meilleure sera la qualité du signal. Ce signal marge bruit est influencé par l'ensemble des composantes électromagnétiques situées dans le magasin.

Symptômes d'un problème de marge bruit trop faible :

- ralentissements fréquents/latence

- pertes de synchronisation du routeur fréquentes

**Debugging**

1 - connexion  sur routeur

Depuis gestion.infomil :

*Rlo -ry  "nom_routeur.nom_magasin"*

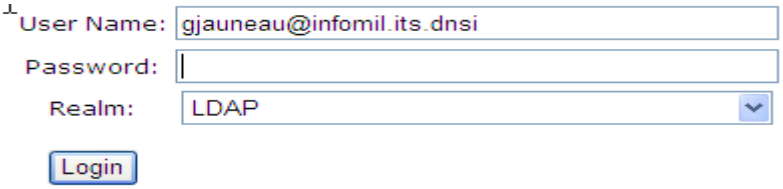
*Password : xxxxx*

*En*

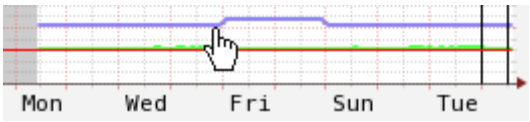
*Password : xxxxx*

2 - Connexion sur la console Osuri

Renseigner votre login/mdp puis cliquez sur login




Sélectionner ensuite le routeur qui est remonté en anomalie puis allez voir le graph "Signal to noise ratio" afin de voir si l'on est dans un cas de fluctuation anormale de marge bruit ou si la marge bruit est constamment en dessous de 6db




3 - commandes utiles

=> Sh dsl int atm0

⚠Valable uniquement sur les routeurs ADSL

Cette commande permet de retourner quelques données intéressantes sur la ligne ADSL. Dans notre cas, c'est la valeur de noise margin qui nous intéresse => la relever.

Lors d'un problème de marge bruit le problème est dans la majorité des cas environnemental

- faire changer le filtre ADSL

- faire changer le câble Rj11

- le routeur est-il branché sur une multiprise ? si oui le faire brancher sur une prise à part

-vérifier que la connexion sur la tête de ligne ne soit pas défectueuse

Cas 5 Procedure Rml : Memory usage > 75%

Informations à collecter pour poser le contexte de la problématique :

Type de routeur : ## arpv, rml,arpvd##

Modèle de routeur : ## à compléter##

Version IOS du routeur : ## à compléter##

Rappels et informations clés :

**Memory usage : signification**

Tout équipement informatique nécessite de la mémoire afin de pouvoir faire tourner des programmes sur l'équipement; chaque programme qui tourne se verra réservé une partie de la mémoire de l'équipement, et libérera cette mémoire lorsqu'il n'en aura plus besoin. Si trop de programmes tournent en même temps, il peut alors arriver que la mémoire sature, provoquant des dysfonctionnements sur les équipements en question.

**Symptômes d'une mémoire saturée**

- apparition de problèmes d'allocation mémoire dans les logs du routeur

- refus de connexion telnet sur le routeur

- impossible d'afficher une quelconque commande tel que show processor memory

- apparition de messages "low memory"

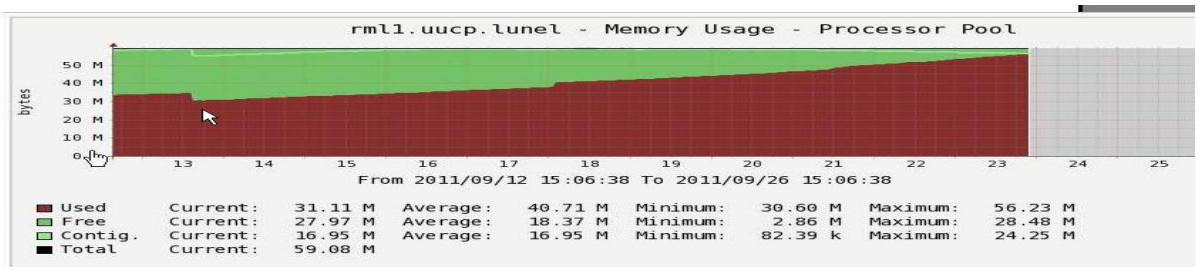
- indisponibilité totale du routeur

**Debugging**

1 - connexion sur la console Osuri

Renseigner votre login/mdp puis cliquez sur login

Sélectionner ensuite le routeur qui est remonté en anomalie puis allez voir le graph "Memory usage" afin de pouvoir déterminer si on est bien dans le cas d'un problème d'utilisation mémoire trop importante;




<u>2 - connexion sur le routeur</u>

*Depuis gestion.infomil :*

*Rlo -ry "nom_routeur.nom_magasin"*

*Password : xxxxx*

*En*

*Password : xxxxx*

<u>3 - commandes utiles:</u>

=> Show processes memory : Cette commande permet de montrer un tableau résumant les différents process utilisant de la mémoire.

```
Processor Pool Total:   61954664 Used:   52243476 Free:    9711188
      I/O Pool Total:   12582912 Used:    3726384 Free:    8856528

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
  33   0 4019243768 3189105264      39180     626724          0 BGP I/O
   0   0 2391189720  145787956   15561204     667924          0 *Dead*
 166   0 1966608184 1966580576      16320      14148          0 Crypto IKE Dispa
 167   0 1962290224 2038380464     385300      52272          0 Crypto IKMP
   3   0 1854802940     103644      11752       2268          0 BGP Scheduler
 158   0 1330021916 1328788040      31140     360624          0 Crypto Support
 226   0  491855712          0      13244          0          0 PDU DISPATCHER
   0   0  151327472  117395180   28142380          0          0 *Init*
```

Allocated : mémoire allouée au process depuis son dernier reboot

Freed : quantité mémoire libérée par ce process

Holding : la quantité mémoire toujours utilisée actuellement par le process

Variantes:

=> sh processes memory sorted allocated;

=> sh processes memory sorted holding (permet de trier par ordre décroissant les process selon la colonne souhaitée)

=>sh memory dead : bloc mémoire non réalloué par le routeur

<u>4 - Actions à mener</u>

A partir des différents éléments collectés, déterminer le process pouvant provoquer cette anomalie mémoire.

Voir avec le magasin si une utilisation particulière du réseau a été faite.

Tenter de debrancher pendant 30s le cable entre le routeur et le commut voir si cela fait chuter l'utilisation mémoire. Redémarrer le routeur et remonter aux IS pour analyse de cette utilisation anormale si besoin.

Cas 6 Procédure RML : Atm traffic upload > 80% pendant 5 minutes

Informations à collecter pour poser le contexte de la problématique :

Type de routeur : ## arpv, rml, arpvd##

Modèle de routeur : ## à compléter##

Version IOS du  routeur : ##à compléter##

Rappels et informations clés  :

**Atm traffic upload : signification**

L'interface Atm (asynchronous Transfer mode) est l'interface sur laquelle transitent les données ADSL entre le magasin et l'extérieur; cet indicateur permet donc de vérifier le trafic sortant sur notre routeur.

Symptômes d'un trafic sortant trop important

- Bande passante saturée

- Perte de paquets ou temps de réponse importants lors d'un ping

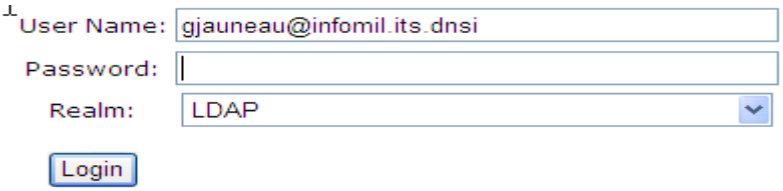
- Lenteur générale lors de la navigation sur internet

- Perturbation des applications dont les flux passent par ce routeur

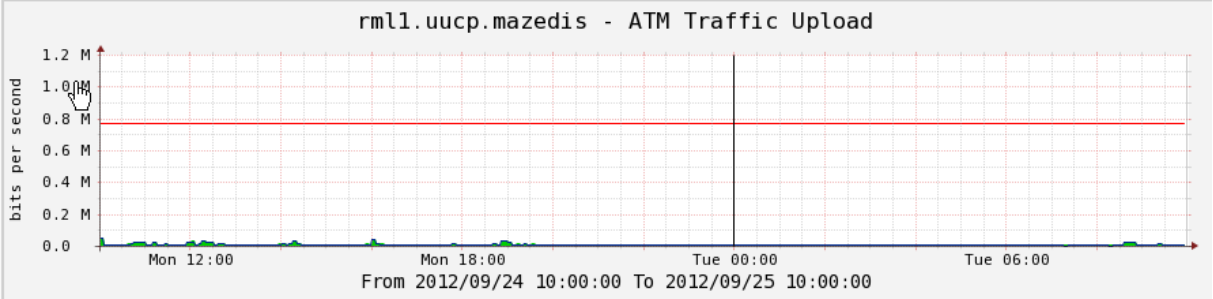
**Debugging**

1 - Connexion sur la console Osuri

Renseigner votre login/mdp puis cliquez sur login




Sélectionner ensuite le routeur qui est remonté en anomalie puis allez voir le graph "Tunnel Traffic - Upload" afin de pouvoir déterminer quel tiers sollicite fortement ou à tort le routeur




<u>2 - connexion sur le routeur</u>

Depuis gestion.infomil :

*Rlo -ry "nom_routeur.nom_magasin"*

*Password : xxxxx*

*En*

*Password : xxxxx*

<u>3 -commandes utiles:</u>

=> Clear ip accounting /* cette commande permet d'effacer la table des données des différentes adresses ip qui ont fait transiter des informations par le routeur */

⚠Attendre une vingtaine de seconde et taper la commande suivante :

=> Sh ip accounting

```
AMANDIS-RML1#sh ip accounting
   Source          Destination          Packets          Bytes
 172.25.1.102     149.57.25.102          1509         852039
 216.57.211.252   216.57.211.255            4            384
 208.29.211.190   149.57.3.12               4            192
 216.57.211.248   216.57.211.255            8            768
```

Relever l'adresse ip qui fait transiter le plus de paquets/octets. Essayer de déterminer à qui appartient ce réseau.

4 - Actions à mener

1) En fonction des différents éléments collectés (tunnel, adresse source/destination) essayer de déterminer le "coupable". (qui ? pourquoi ? utilisation normale ? virus ?)

2) Demander au responsable informatique du magasin s'ils ont connaissance d'un envoi important de données ou d'une utilisation importante de bande passante.

3) En dernier recours, redémarrer le routeur et solliciter les IS pour analyse plus poussée

---

Une fois ces procédures rédigées, j'ai donc fait prendre connaissance aux techniciens de ces nouvelles documentations supports.

Celles-ci ont permis :

- Des temps de traitement moins longs lors d'appels pour des problématiques d'ordre réseau.

- Un debugging plus efficace et une meilleure remontée d'informations de leur part.

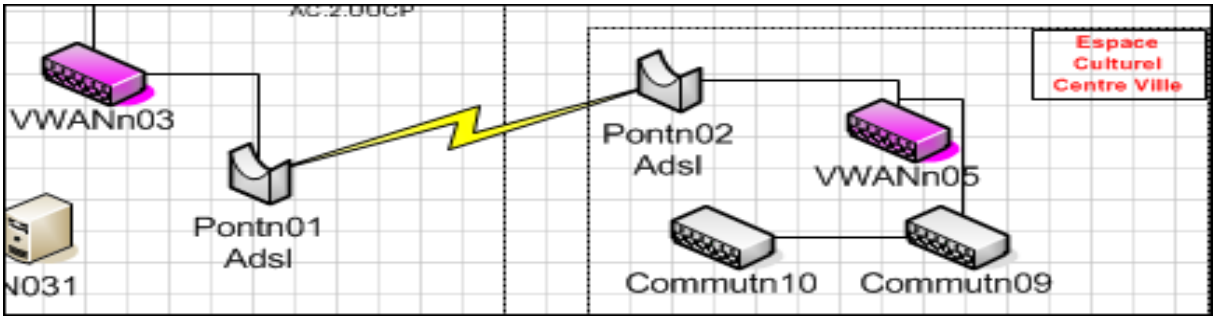
- Une meilleure compréhension du problème

## 2. Cas concrets de résolution de problèmes grâce aux scripts développés

Dans cette partie je traiterai de quelques cas concrets qui ont été résolus grâce à l'utilisation de ces scripts.

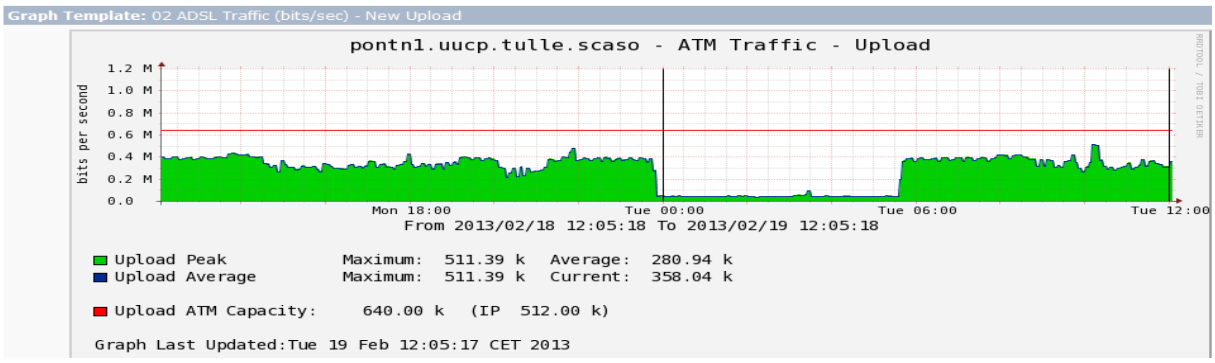
1 - Dossier sur Tulle.

Problématique de lenteur entre l'espace culturel et l'hypermarché




L'espace culturel se plaignant de manière récurrente de lenteurs, nous a sollicité pour faire vérifier cette liaison pontée.

D'après la console Osuri, cette lenteur provenait d'un fort taux d'upload sur la ligne




Mais comment déterminer le coupable ?

Equipement sur réseau tiers qui sature la ligne ? Caisse vérolée ? Qu'est ce qui pourrait provoquer cette utilisation anormale de bande passante ?

Grâce au script de "récupération bande passante" développé, ce script a été joué pour récuperer les valeurs de bande passante transitant sur les interfaces du :

-Vwann03

- Pontn1

-Pontn2

-Commutn09

Exemple de fichier résultat pour le pontn1 sous format excel :

| ATM0 download | ATM0 upload | Dialer1 downl | Dialer1 upload | FastEthernet0 download | FastEthernet0 upload | FastEthernet3 download | FastEthernet3 upload |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 45 | 373 | 116 | 389 | 327 | 20 | 56 | 8 |
| 45 | 529 | 64 | 547 | 481 | 20 | 32 | 7 |
| 45 | 519 | 49 | 517 | 451 | 20 | 40 | 8 |
| 39 | 535 | 102 | 560 | 495 | 17 | 22 | 7 |
| 39 | 492 | 38 | 522 | 460 | 17 | 30 | 7 |
| 47 | 428 | 58 | 450 | 386 | 21 | 28 | 8 |
| 46 | 526 | 120 | 538 | 470 | 21 | 39 | 7 |
| 42 | 459 | 39 | 461 | 401 | 18 | 21 | 7 |
| 37 | 473 | 37 | 495 | 433 | 17 | 26 | 8 |

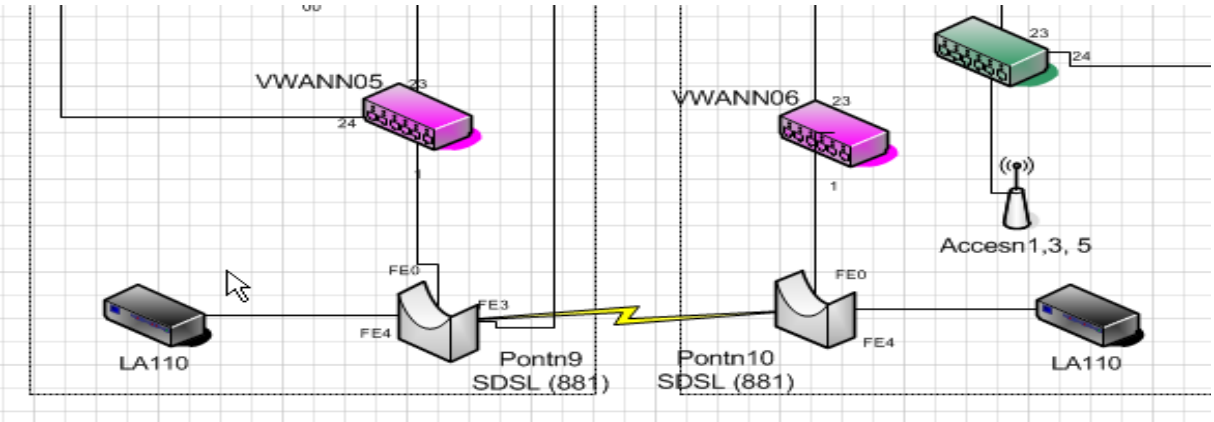
En traçant les différents taux d'upload et download sur les interfaces, j'ai mis en avant que les trois caisses de l'espace culturel essayaient en permanence de récuperer un fichier présent sur le serveur evolutel manager.

Suite à la mise en place manuelle de ces fichiers sur les caisses, celles-ci ne sollicitaient plus à tort le serveur, et, de ce fait le taux d'upload est revenu à la normal, et l'espace culturel a à nouveau pu travailler normalement.

Sans ce script, il aurait été très laborieux de récupérer, interface par interface sur chaque commut, vwann, etc les valeurs du traffic (ie lancer la commande manuellement toutes les 20s sur chaque interface...)

2 - Dossier sur le Leclerc de Vaudry.

Lenteurs inexpliquées  sur le drive (liaison pontée pontn9-pontn10)

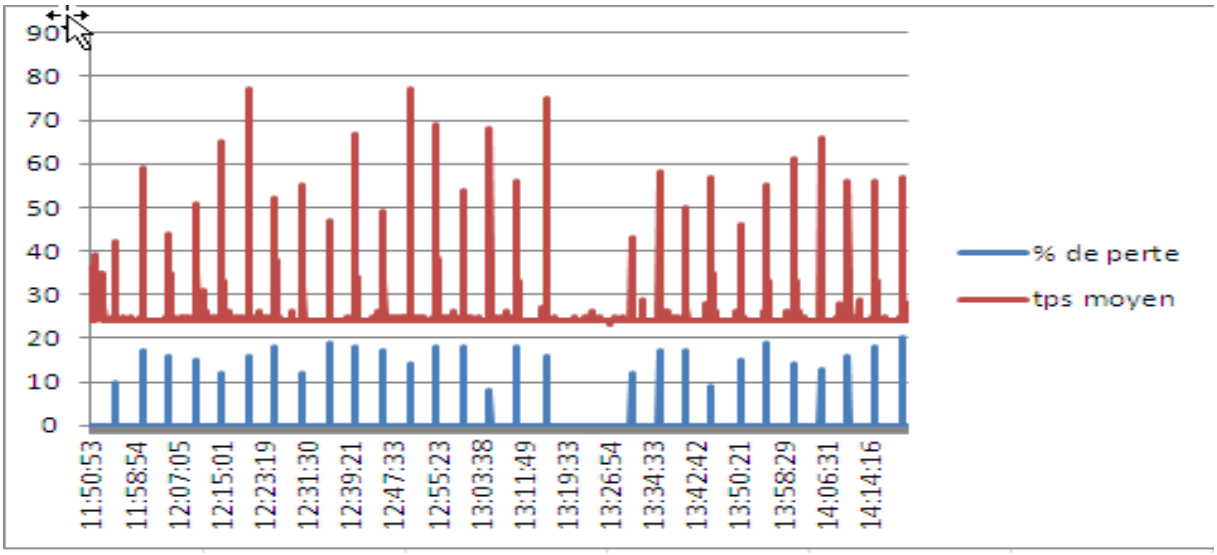



Le magasin nous a sollicité car il constatait de nombreuses lenteurs et des coupures réseaux sur l'espace culturel.

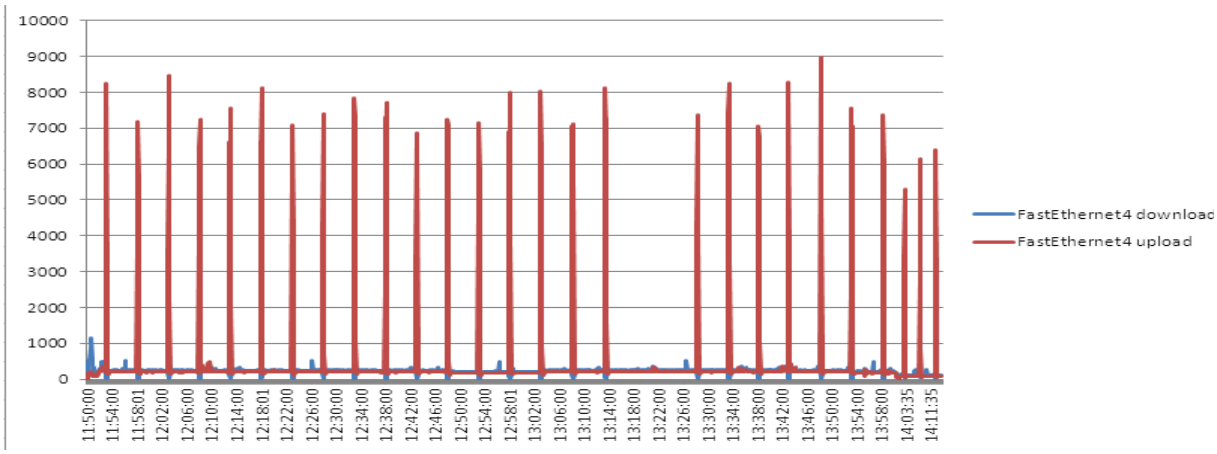
Pb constaté uniquement pour le tiers.

Nous ne constations pas de problème au niveau des logs routeurs, pas de pertes de paquets lorsqu'on pinguait la wan du pontn9 ou pontn10, et la console Osuri ne traçait rien de flagrant.

Grâce à l'utilisation du script test latence réseau, nous avons pu constater l'anomalie de manière plus fine




Puis le script de bande passante a été joué, pour mettre en évidence une surcharge réseau sur la liaison pontée (en kbp/s)




Après analyse, il a été montré que nous avions un problème sur les flux d'administration sur ce site.

C'était donc la récupération d'information pour la console Osuri qui provoquait cette latence anormale; En effet, un serveur image mis en place à des fins de tests, provoquait cette latence anormale sur nos équipements pontés.  Ces scripts ont donc pu mettre en avant cette problématique et permettre d'isoler rapidement le problème.

## Conclusion

Pour terminer, la mise en place de ces outils et le développement de ces scripts ont participé à l'amélioration de la qualité de service réseau au sein de notre entreprise.

L'acquisition de ces nouvelles connaissances et sources de données ont apporté une valeur ajoutée à l'entreprise et à moi-même.

Il en est ressorti de plus, une meilleure satisfaction client du fait de notre réactivité sur ces différents types de problématiques.

Le cahier des charges, dont les grandes lignes ont été citées plus haut, a été respecté.

Pour ma part, la mise en place et le développement de ces scripts vb m'ont permis de les appliquer dans d'autres domaines de compétence (récupération de données en table sql, récupération de données diverses...). Ce mémoire a donc été bénéfique autant pour moi que pour la société.

Les techniciens, grâce à ces outils, sont devenus, plus réactifs, plus autonomes et ont obtenu une meilleure compréhension des termes et des problématiques soulevés. Cela s'est ressenti, en tant qu'ingénieur support, par une amélioration de la qualité de leur travail dans ce domaine. 80% des dossiers traitants de ce domaine sont dorénavant solutionnés au niveau 1 par les techniciens. Ils sont dans la plupart des cas devenus autonomes pour traiter ce type de problématiques.

En terme de client, de nouveaux marchés se sont ouverts :

En effet, la centrale Scadif (magasins E.Leclerc de la région parisienne) ont signé un contrat pour mettre en place cette architecture dite "rml". Celle-ci est actuellement en cours de déploiement.

Autre point, la centrale Lecasud, qui gérait elle-même les flux monétiques des magasins, a également signé un contrat pour faire passer ces flux dorénavant par notre réseau et notre passerelle.

Cela a donc, malgré les coûts de développement, été bénéfique à la société.

Mais il reste encore de nombreuses choses à faire pour  améliorer cette qualité de service sur nos infrastructures réseaux.

J'ai été sollicité pour mettre en place un dashboard sur la console Osuri, qui listerait l'état des boitiers LA110, qui sont connectés actuellement sur certains de nos routeurs RML2

La réflexion suivante doit être posée : l'interface est-elle up ?  en 100Mbps ? En full-duplex ? Utilisation de Nagios ? Script vb ?

Il reste donc encore des choses à faire.

Enfin dernier point et non des moindre : les flux vidéos.

A ce jour aucune QOS n'a été paramétrée sur nos routeurs.

Il faudrait, afin que les visio-conférences ne saturent pas nos accès par exemple, ni ne perturbent l'activité magasin dans certains cas, attribuer des règles de QOS spécifiques sur les routeurs Cisco.

Mais c'est encore en phase de projet pour l'instant.

Il reste donc encore de nombreux points qui peuvent être vus afin de toujours et encore améliorer la qualité de service pour le client.

Enfin, Microsoft préconisant l'utilisation de powershell dans un futur proche, il faudrait envisager de migrer ces scripts en Powershell. A voir pour un avenir proche...

# Annexes :

## 1 - Caractéristiques techniques d'un routeur Cisco 870 series

**Tableau 7.** Caractéristiques matérielles

| Caractéristiques | Spécification |
|---|---|
| **Mémoire DRAM par défaut** | 128 Mo |
| **Mémoire DRAM maximale** | 256 Mo |
| **Mémoire Flash par défaut** | 24 Mo |
| **Mémoire Flash maximum** | 52 Mo |
| **Réseau WAN** | • 871 : Ethernet 100 Mbits/s<br>• 876 : ADSL sur RNIS (matériel prêt pour ADSL2/ADSL2+)<br>• 877 : ADSL sur ligne téléphonique analogique (matériel prêt pour ADSL2/ADSL2+)<br>• 878 : G.SHDSL (support 2 et 4 fils)<br>• Performances IMIX : 3 Mbits/s |
| **Commutateur LAN** | 4 ports gérés 10/100BASE-T avec auto-détection MDI/MDX [Media Device In/Media Device Cross Over] pour liaison croisée automatique |
| **WLAN 802.11b/g** | En option sur tous les modèles |
| **Port Console** | RJ-45 |

| Caractéristiques | Description |
|---|---|
| **Protocoles de routage et fonctionnalités générales du routeur** | • Protocoles RIP (Routing Information Protocol) v1 et v2<br>• Protocole L2TP (Layer 2 Tunneling Protocol)<br>• Cisco Express Forwarding (CEF) Port Address Translation (PAT)<br>• RFC 1483/2684<br>• Protocole PPP (Point-to-Point Protocol) sur ATM (PPPoA) (modèles DSL uniquement)<br>• Protocole PPPoE (PPP over Ethernet)<br>• Protocole STP (Spanning-Tree Protocol) 802.1D<br>• Protocole DHCP (Dynamic Host Configuration Protocol) serveur / relais / client<br>• Listes de contrôle d'accès<br>• Encapsulation GRE (Generic Routing Encapsulation) |
| **Nombre d'utilisateurs** | • 20 |
| **Fonctionnalités IPv6** | • Architecture d'adressage IPv6<br>• Résolution de noms IPv6<br>• Statistiques IPv6<br>• Traduction et transport de paquets IPv6 entre des points d'extrémité IPv6 uniquement et IPv4 uniquement<br>• Protocole ICMP (Internet Control Message Protocol) v6<br>• Protocole DHCP (Dynamic Host Configuration Protocol) IPv6 |
| **Fonctionnalités DSL et ATM (modèles DSL uniquement)** | • Débit ATM variable en temps réel (VBR-rt)<br>• Débit ATM non spécifié (UBR), constant (CBR) et variable non en temps réel (VBR-nrt)<br>• Support des pannes ATM OAM F5 (Opération, Administration et Maintenance).Vérification de continuité F5 par segment et de bout en bout, et prise en charge ILMI (Integrated Local Management Interface)<br>• 10 circuits virtuels |

| Caractéristiques | Description |
|---|---|
| **Fonctions de sécurité** | • Pare-feu à inspection d'état<br>• Pare-feu de niveau 2 (Cisco 871 uniquement)<br>• Transparence NAT<br>• Support de pare-feu pour les clients Skinny<br>• Cryptage IPSec 3DES avec accélération matérielle<br>• Cryptage IPSec AES avec accélération matérielle<br>• Client et Serveur Cisco Easy VPN<br>• Client et agrégation IPSec 3DES<br>• IPSec passthrough<br>• PPTP (Point-to-Point Tunneling Protocol) pass-through<br>• L2TP pass-through<br>• 802.1X<br>• Proxy d'authentification HTTPS (Secure HTTP), FTP et Telnet |
| **Fonctions Qos** | • Weighted Fair Queuing (WFQ)<br>• Class-Based WFQ (CBWFQ)<br>• Low-Latency Queuing (LLQ)<br>• Class-Based Traffic Shaping (CBTS) (Cisco 871 uniquement)<br>• Class-Based Traffic Policing (CBTP) (Cisco 876, 877 et 878 uniquement)<br>• MIB Class-Based QoS<br>• Pré fragmentation avant cryptage<br>• Ajustement de la TX ring<br>• Groupage des circuits virtuels ATM<br>• Policy-based routing (PBR)<br>• File d'attente par circuit virtuel - Per-VC queuing<br>• Formatage de trafic par circuit virtuel - Per-VC traffic shaping |

| Caractéristiques | Description |
|---|---|
| **Protocoles de routage** | • Open Shortest Path First (OSPF)<br>• Border Gateway Protocol (BGP)<br>• Enhanced Interior Gateway Routing Protocol (EIGRP) |
| **Fonctionnalités générales de routage** | • 3 VLAN 802.1q pour les réseaux LAN filaires et sans fil<br>• Protocole WCCP (Web Content Caching Protocol)<br>• Zone démilitarisée (DMZ) |
| **Fonctions de sécurité** | • Système de détection des intrusions (IDS) et de prévention des intrusions (IPS)<br>• Dynamic Multipoint VPN (DMVPN) (GRE multipoint et protocole NHRP [Next Hop Resolution Protocol])<br>• Lock and Key<br>• Filtrage des URL : Websense et N2H2<br>• Certificats numériques (PKI) |

| Caractéristiques | Description |
|---|---|
| **Fonctions QoS** | • Mécanismes de qualité de service : Priority et custom queuing<br>• CBWRED (Class-Based Weighted Random Early Detection)<br>• NBAR (Network-based application recognition)<br>• Link Fragmentation and Interleaving (LFI)<br>• Protocole RSVP (Resource Reservation Protocol)<br>• Compression d'en-tête RTP (Real Time Protocol)<br>• Services différenciés (DiffServ)<br>• Pré-classification des paquets pour la QoS en environnement IPSEC et pré fragmentation<br>• Class-Based Marking (CBM) |
| **Fonctions multicast** | • Protocol Independent Multicast (PIM) Sparse Mode<br>• PIM Sparse-Dense Mode<br>• Auto route processing (Auto-RP) |
| **Fonctions de haute disponibilité** | • Protocole MHSRP (Multigroup HSRP) |

2 - Exemple de script perl incorporé afin de pouvoir récupérer la version IOS d'un routeur pour l'exploiter ensuite dans OSURI : Ce script n'a pas été réalisé par mes soins mais est utile à la compréhension pour la récupération des informations sur les routeurs.

```
***

#! /usr/bin/perl

=head

 <title>
Recherche du modele du routeur
</title>
 <summary>
Description du script
</summary>

$File: //depot/POSU (Osuri)/main/LSCR/PERL/discover_device_model.pl $
$Author: fcristina $
$DateTime: 2012/09/05 11:50:48 $
$Revision: #2 $
$Change: 204112 $

=cut

use strict;
use warnings;
use diagnostics;
use IO::File;
use threads;

my $root = "/opt/OSURI/LSCR";
my $data_in=();


# Traitement des arguments passÃs
if ($#ARGV == -1) {
   die "Les arguments doivent Ãtre ARPV ou ARPVD, NOOB !\n";
}
elsif ( $ARGV[0] eq "ARPV" ) {
   $data_in   = ("$root/DATA_IN/arpv.csv");
}
elsif ( $ARGV[0] eq "ARPVD" ) {
   $data_in   = ("$root/DATA_IN/arpvd.csv");
}

my $data_out = "$root/DATA_OUT/discover_model_$ARGV[0].txt";
my $log_file = "$root/LOG/discover_device_$ARGV[0]".getdate('jour').".log";

#-----------------------------------------------------
# Date
#-----------------------------------------------------
```

```
sub getdate {
   my ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(); # Date au format UNIX
   my $date = sprintf("%02d-%02d-%02d - %02d-%02d-%04d",$hour,$min,$sec,$mday,$mon+1,1900+$year); #
Date au format humain
   my $jour = sprintf("%04d-%02d-%02d",1900+$year,$mon+1,$mday); # Date au format humain
   if ($_[0] =~ /jour/){
      return ($jour);
   }
   else{
   return ($date);
   }
}

my $log = IO::File->new("$log_file",'w') or die ("Impossible d ecrire dans le fichier $log_file : $! \n");
print $log getdate('date')."\n";

my $sortie = IO::File->new("$data_out",'w') or die ("Impossible d ecrire dans le fichier $data_out : $! \n");
print $sortie getdate('date')."\n";

sub defID{
    my ($ip,$description) = @_;
    my $ID_model = "unknown";
    my $version = "unknown";
    my @snmpIOS =();
    my $snmpmodel = `snmpwalk -On -v2c -c edifie $ip 1.3.6.1.2.1.1.2.0`;
    if ($snmpmodel =~ /569/){$ID_model = "877";}
    elsif ($snmpmodel =~ /570/){$ID_model = "878";}
    elsif ($snmpmodel =~ /571/){$ID_model = "871";}
    elsif ($snmpmodel =~ /620/){$ID_model = "1841";}
    elsif ($snmpmodel =~ /837/){$ID_model = "881";}

    if ($ID_model ne "unknown"){
    @snmpIOS = `snmpwalk -On -v2c -c edifie $ip 1.3.6.1.4.1.9.9.25.1.1.1.2.7`;
        foreach my $i (@snmpIOS){
        chomp ($i);
        if ($i =~ /Version/)
            {
            (undef, undef, $version) = split(/,/, $i);
            }
        }
    print $sortie "$description;$ip;$ID_model;$version\n";
    }
    else{print $sortie "$description;$ip;$ID_model\n";}


}

my $fh = IO::File->new("$data_in",'r') or die ("Impossible de lire dans le fichier $data_in : $! \n");


# Je parse le fichier en entrer que je mets dans un tableau.
my @devs;
while (my $line = $fh->getline()) {
   my ($central, $magasin, $nom, $reseau, $ip, $type, $note) = split(';',$line);
   my $description = "$nom.$reseau.$magasin.$central";
   if (($ip) and ($description !~ /galec/))
   {
      print "$ip;$description;$type;$note\n";
      print $log "$ip;$description;$type;$note\n";
      my @t = ($ip, $description);
```

```
      push @devs, \@t;
    }
    else
    {
      print "BUG : $ip;$description;$type;$note\n";
      print $log "BUG : $ip;$description;$type;$note\n";
    }
}

my $nb_process = 40;
my $nb_compute = scalar @devs;
my $i=0;
my @running = ();
my @Threads;

while (scalar @Threads < $nb_compute) {
        @running = threads->list(threads::running);
        print "LOOP $i\n";
        print "  - BEGIN LOOP >> NB running threads = ".(scalar @running)."\n";

        if (scalar @running < $nb_process) {
                my $dev_aref = shift @devs;
                my $thread = threads->new( sub { defID(@$dev_aref )});
                push (@Threads, $thread);
                my $tid = $thread->tid;
                print "  - starting thread $tid\n";
        }
        @running = threads->list(threads::running);
        print "  - AFTER STARTING >> NB running Threads = ".(scalar @running)."\n";
        foreach my $thr (@Threads) {
                if ($thr->is_running()) {
                        my $tid = $thr->tid;
                        print "  - Thread $tid running\n";
                }
                elsif ($thr->is_joinable()) {
                        my $tid = $thr->tid;
                        $thr->join;
                        print "  - Results for thread $tid:\n";
                        print "  - Thread $tid has been joined\n";
                }
        }
        @running = threads->list(threads::running);
        print "  - END LOOP >> NB Threads = ".(scalar @running)."\n";
        $i++;
}

print "\nJOINING pending threads\n";
while (scalar @running != 0) {
        foreach my $thr (@Threads) {
                $thr->join if ($thr->is_joinable());
        }
        @running = threads->list(threads::running);
}

$fh->close() or warn (" Fermeture de $data_in impossible : $! \n");

$log->close()  or warn (" Fermeture de $log_file impossible : $! \n");

$sortie->close()  or warn (" Fermeture de $sortie impossible : $! \n");
```

3 - Script vb de récupération latence réseau

```
Module test_latence_reseau



'*************************************************************************
**************************************************
    ' main

'*************************************************************************
**************************************************
    Sub Main()
        Dim ip As String = InputBox("Veuillez renseigner l'adresse ip à
surveiller")
        Dim fil_result As String = AppDomain.CurrentDomain.BaseDirectory &
"resultat_latence_" & ip & ".txt"
        Dim ping_result As System.Net.NetworkInformation.PingReply
        Dim cpt = 0
        Dim result = ""
        Dim max_value = 0
        Dim min_value = 100000
        Dim average_value = 0
        Dim loss_value = 0
        Dim date_debut = ""


        'on ecrit l'entete
        Dim swriter As New IO.StreamWriter(fil_result, True)
        swriter.WriteLine("jour/moi/annee;heure;% de perte;tps max;tps
moyen;tps min;")
        swriter.Close()
        swriter.Dispose()


        'verification de la coherence de l'@ du routeur
        If ip.Split("."c).Length <> 4 Then
            MsgBox("l'ip est invalide")
            Environment.Exit(546)
            Exit Sub
        Else
            Dim sDecoupe As String() = ip.Split("."c)
            Dim i As Int16
            For j = 0 To 3
                If Not Int16.TryParse(sDecoupe(j), i) OrElse i < 0 OrElse i
> 255 Then
                    MsgBox("l'ip est invalide")
                    Environment.Exit(545)
                    Exit Sub
                End If
            Next j
        End If


        'on lance la récuperation
        MsgBox("lancement de la surveillance sur l'ip : " & ip &
CChar(vbCrLf) & "le fichier resultat sera : " &
AppDomain.CurrentDomain.BaseDirectory & "resultat_latence_" & ip & ".txt")
```

```
        While True
            'on réinitialise les valeurs
            date_debut = System.DateTime.Now.ToString
            cpt = 0
            result = ""
            max_value = 0
            min_value = 100000
            average_value = 0
            loss_value = 0

            'lancement d'un ping 100 fois d'affilé
            While cpt < 100
                Dim sping = New System.Net.NetworkInformation.Ping
                ping_result = sping.Send(ip, 1000)
                sping.Dispose()
                cpt += 1
                result &= ping_result.RoundtripTime & ";" &
ping_result.Status.ToString & CChar(vbCrLf)
            End While
            Dim tab_result = result.Split(CChar(vbCrLf))

            'recuperation % perte.
            cpt = 0
            While cpt < tab_result.Length - 1
                If tab_result(cpt).Split(";"c)(1) <> "Success" Then
loss_value += 1
                cpt += 1
            End While

            If loss_value < 100 Then
                'recuperation valeur min.
                cpt = 0
                While cpt < tab_result.Length - 1
                    If tab_result(cpt).Split(";"c)(1) = "Success" Then
                        If CInt(tab_result(cpt).Split(";"c)(0)) < min_value
Then min_value = CInt(tab_result(cpt).Split(";"c)(0))
                    End If
                    cpt += 1
                End While
                'recuperation valeur max.
                cpt = 0
                While cpt < tab_result.Length - 1
                    If tab_result(cpt).Split(";"c)(1) = "Success" Then
                        If CInt(tab_result(cpt).Split(";"c)(0)) > max_value
Then max_value = CInt(tab_result(cpt).Split(";"c)(0))
                    End If
                    cpt += 1
                End While
                'recuperation valeur moyenne.
                cpt = 0
                While cpt < tab_result.Length - 1
                    If tab_result(cpt).Split(";"c)(1) = "Success" Then
                        average_value +=
CInt(tab_result(cpt).Split(";"c)(0))
                    End If
                    cpt += 1
                End While
                average_value = CInt(average_value / (100 - loss_value))
```

```
                result = loss_value & ";" & max_value & ";" & average_value
& ";" & min_value & ";"
            Else
                result = loss_value & ";--;--;--;"
            End If

            'on ecrit dans le fichier résultat avec gestion du verrouillage
du fichier resultat
            Dim erreur = True
            While erreur
                Try
                    swriter = New IO.StreamWriter(fil_result, True)
                    swriter.WriteLine(Replace(System.DateTime.Now.ToString,
" ", ";") & ";" & result)
                    swriter.Close()
                    swriter.Dispose()
                    erreur = False
                Catch
                End Try
                Threading.Thread.Sleep(100)
            End While

            'Si la surveillance a mis moins de 5s on patiente
            If date_debut = System.DateTime.Now.ToString Then
                Threading.Thread.Sleep(5000)
            End If
        End While
    End Sub
End Module
```

**Bibliographie**

http://doc.ubuntu-fr.org/cacti

http://www.cacti.net/

http://oss.oetiker.ch/rrdtool/

http://doc.ubuntu-fr.org/rrdtool

http://fr.wikipedia.org/wiki/RRDTool

Procédure installation BBS - Infomil - etd - u202612 - v3.0.-.docx

Liste_Demandes_Reseau_Metier.4.0. - version annotée par Infomil+observation_scaso.pdf

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

http://www.frameip.com/snmp

-batch.pdf (issu du site développez.com)

-faqvbs.pdf (issu du site développez.com)

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6f3a.shtml

base de données Talomi. Logiciel de hot-line développé par Infomil

## Résumé et mots clés

**Administration routeurs et surveillance des différents accès réseaux des centres Leclerc administrés par Infomil**

Memoire d'ingénieur CNAM, 2013


## Resumé

Suite aux contraintes clients, la refonte de l'architecture réseau et les données réseaux de plus en plus volumineuses, la mise en place de nombreux outils de surveillance réseau ont été créés.

Il a donc été développé une console de supervision. Des mails automatiques sont générés de manière périodique listant les anomalies. Des scripts de surveillance ont été mis en place.

Chaque outil a une utilisation différente et répond à un besoin :

- Les scripts vb  pour analyse en temps réel d'une problématique.

- La console d'administration pour historiser les informations routeurs et pour avoir un visuel rapide de l'état du service.

- La génération de mail afin d'alerter les techniciens et améliorer leur réactivité.

Enfin, la rédaction de procédures a été nécessaire pour orienter les techniciens dans le debugging réseau.

Ces outils ont permis d'améliorer notre réactivité sur des problématiques réseaux, augmentant la satisfaction client.

De nouveaux marchés ont été récupérés suite à la mise en place de ces outils (centrale Scadif en cours de déploiement RML)



Mots clés : Cisco, routeur, surveillance, script, cacti, administration



## SUMMARY

Network Administration on  Cisco' router. Creation of vb scripts and a console of administration to react quickly and well in case of breakdown.