# Quelques propositions pour une organisation des ressources réseaux prenant en compte les besoins du LACL

Document de travail proposé par Olivier Michel
LACL - P2 240 - olivier.michel@univ-paris12.fr
Version du 24 mars 2009.

## Table des matières

# 1 Introduction

À l'heure où les missions de l'université évoluent considérablement et où la demande de performance et de réactivité se fait de plus en plus forte, il nous apparaît clairement que la mise en œuvre actuelle des ressources informatiques par le CRI ne permet pas au LACL d'atteindre les objectifs d'excellence qu'il s'est fixé. En effet, de par ses activités de recherche en informatique (section 27 du CNU), le LACL a des besoins spécifiques que nous allons essayer de rendre explicites dans la section 2 ; nous proposerons une solution aux problèmes dans la section 3. Enfin, nous montrerons en section 4 combien l'approche proposée peut s'instancier avec les ressources dont dispose le laboratoire.

# 2 Les besoins du LACL

Nous donnons dans cette section la liste des services qui ne sont pas accessibles actuellement[1]. Nous insistons sur le fait que ces services sont des services standard qui représentent le minimum qu'un laboratoire est en droit d'attendre d'une université.

La liste qui suit n'est pas une liste figée dans le temps car le laboratoire est un lieu qui évolue constamment au grès des besoins de ses membres. On distingue trois types de services nécessaires

1. les services indispensables que l'on souhaite mettre en place pour les membres du laboratoire,
2. les ressources internes du laboratoires devant êtres accessibles depuis l'extérieur du laboratoire,
3. et enfin la protection des ressources du laboratoire.

Nous détaillons ces éléments dans les sections suivantes.

## 2.1 Services indispensables à mettre en place

Ces services concernent des outils permettant un travail efficace et une mise en commun des ressources du laboratoire. Ils représentent de plus (pour les CMS/Wiki par exemple), des éléments requis dans le cadre de projets (ANR, RNSC...) :

1. serveur CVS/SVN pour permettre le développement collaboratif, accessible via un serveur Web et ssh,
2. serveurs de CMS/Wiki pour les projets scientifiques (ANR et autres),
3. serveurs applicatifs dédiés reposant sur des technologies en développement,
4. serveur CIFS et NFS permettant la mise en commun d'espace disque,
5. adresses mails pérennes (et temporaires pour les visiteurs du laboratoire) en `@lacl.univ-paris12.fr`,
6. services `imaps` et `pop3s` ainsi que webmail en `https`,
7. liste de diffusions (internes et externes),

[1] Certains services sont parfois disponibles, l'accès ssh par exemple, mais avec de telles restrictions que leur usage est rendu difficile, sinon inutilisable.

8. utilisation, en interne au laboratoire, de protocoles exotiques (JXTA, p2p...),
9. utilisation de logiciels de téléconférences.

### 2.2 Accès aux ressources internes de l'extérieur du laboratoire

Les enseignants/chercheurs du laboratoires développent un grand nombre de collaborations avec des collègues extérieurs à l'université. Ils sont ainsi amenés à se déplacer, nationalement et internationalement. Lors de ces déplacements, il est indispensable de leur permettre l'accès à l'ensemble des ressources offertes par le laboratoire avec un maximum de sécurité et d'efficacité. Pour cela, nous avons identifié les services suivants :

1. accès, depuis l'extérieur via le protocole crypté et sécurisé ssh, aux ressources internes du laboratoire,
2. serveur VPN pour accéder, de l'extérieur du laboratoire, aux ressources internes de celui-ci.

### 2.3 Protection des ressources du laboratoire

Vivant dans un monde connecté et ouvert où les attaques technologiques ne sont pas rares, nous ne pouvons faire l'économie de protéger les ressources du laboratoire en ayant une maîtrise maximale sur les accès aux ressources. Ainsi, il nous semble essentiel de pouvoir offrir les services suivants :

1. ajout et retrait d'une ressource de calcul sur le réseau avec une adresse IP valide,
2. accès aux imprimantes et aux serveurs du laboratoire restreint aux membres du laboratoire,
3. protection à l'égard des attaques, virus... provenant du réseau (de l'université mais aussi d'Internet en général).

### 2.4 Un objectif permanent : la sécurisation des ressources

Il est important de remarquer qu'une propriété transversale attendue de tous ces services est la réactivité et l'évolutivité de ceux-ci. Bien entendu, nous souhaitons que tous ces services soient disponibles avec un niveau de sûreté et de sécurité maximal.

## 3 Une proposition de schéma technique

Nous proposons dans cette section une solution technique simple, robuste et éprouvée qui permettrait de répondre aux besoins de la section 2 par une gestion délocalisée de certaines ressources.

En effet, une solution (classique) de type « *sous-réseau autonome sur une classe IP privée avec une machine firewall en front-end* » permet d'adresser les problèmes précédemment décrits. Nous détaillons dans les sections suivantes les éléments permettant de comprendre le schéma proposé.

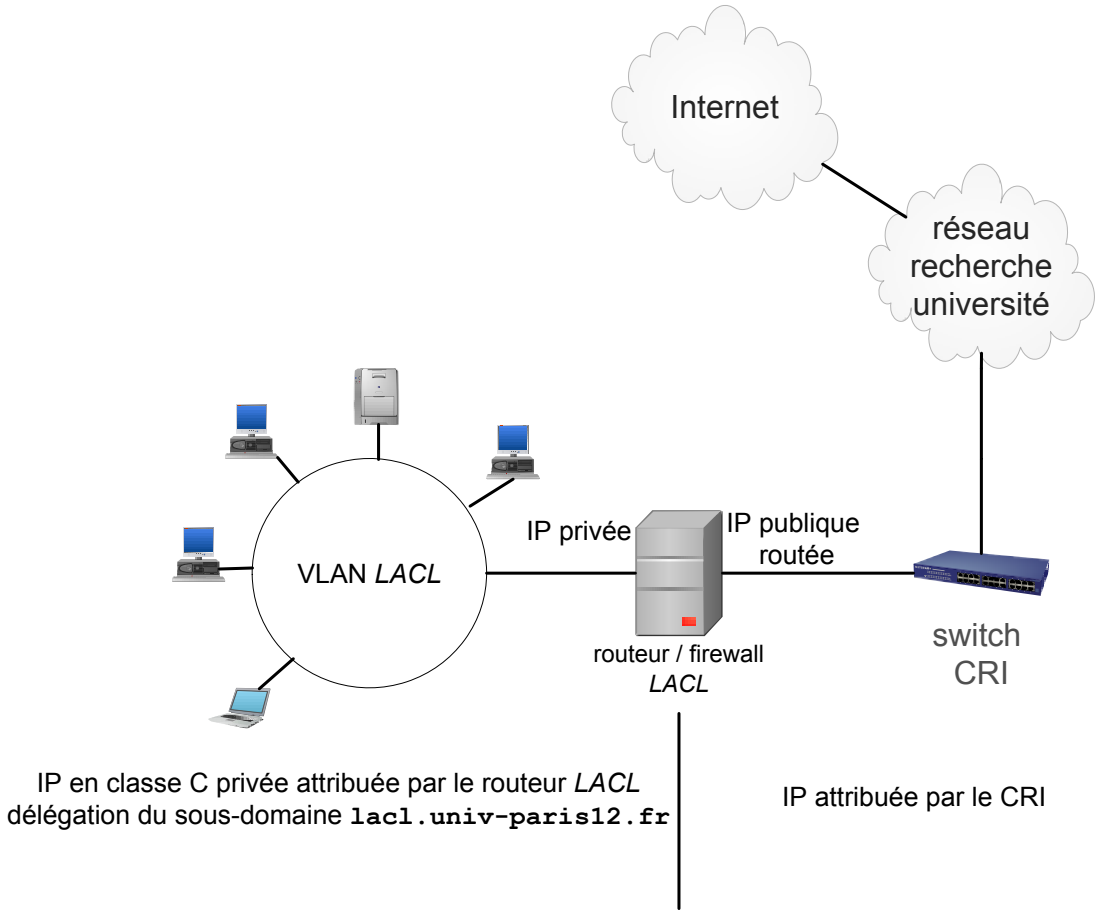


FIG. 1 – Proposition de schéma technique réseau pour le LACL.

## 3.1 Placement des prises réseaux sur un même VLAN, isolé

Le premier élément à mettre en place est de placer *toutes les prises réseau* (sauf une - voir point ci-dessous) du LACL sur un VLAN dédié, non routé et distinct des réseaux existants (*recherche*, *enseignement* et *administration*) de l'université. En effet, de par la configuration actuelle[2] il ne nous est pas possible d'avoir une mise en commun des ressources du laboratoire, *distincte* des autres machines de l'université.

Appelons ce VLAN le VLAN LACL. Il est essentiel que les prises de ce VLAN ne soient pas routées afin de forcer les machines du réseau LACL à passer par le routeur du laboratoire ; c'est lui qui aura la responsabilité de gérer les adresses IP assignées aux machines du VLAN. Ce routeur/firewall est présenté dans la section suivante.

[2]Toutes les machines se trouvent actuellement sur le réseau recherche. Cela a comme conséquence d'êtres accessibles par toutes les machines de ce réseau : vers, virus, attaques diverses et autres sources de problèmes mettent en danger les ressources informatiques du laboratoire.

### 3.2 Administration d'une machine firewall

Une machine effectuera le lien entre l'intérieur du sous-réseau LACL et le reste du monde : le *routeur/firewall*. Cette machine sera le point de passage du flux réseau entre les machines du VLAN LACL et le reste de l'université/internet. Inversement, elle sera le point de passage obligé de tout flux entrant. Ce point de passage étant unique, il sera plus facile pour le LACL de sécuriser l'accès à ses ressources.

### 3.3 Gestion déléguée du sous-domaine `lacl.univ-paris12.fr`

Dans cette configuration, la machine firewall gère tous les services réseaux se situant à l'interface des deux mondes. Afin de disposer d'un contrôle sur les services mail, web, ssh... il est essentiel que la sous-réseau `lacl.univ-paris12.fr` soit délégué à cette machine qui gèrera le DNS et tous les autres services de ce sous-réseau. La délégation de sous-réseau est un acte technique simple qui permet de déléguer la gestion d'un sous-réseau à une entité.

Afin de permettre la mise en œuvre des services décrits dans la section 2, il est essentiels que les *ports* de cette machine ne soient pas filtrés par le firewall de l'université. Ainsi (liste non exhaustive), les ports 22 (ssh), 25 (smtp), 80 (http), 443 (https), imaps (993), pop3s (995), 1194 (VPN), 2401 (cvs)8080 (http), ... **doivent êtres ouverts** et accessibles depuis toutes machine connectée à Internet. C'est le firewall de ce VLAN qui aura la responsabilité de filtrer le traffic indésirable, en accord avec la politique de sécurité du CRI et de l'université.

## 4 Mise en œuvre effective

Le schéma technique esquissé dans les sections qui précèdent est une solution robuste, maîtrisée et évolutive car extrêmement standard dans les laboratoires de recherche en informatique. La viabilité de ce projet repose sur deux éléments clefs :

1. Le laboratoire dispose en interne, via des enseignants/chercheurs spécialiste de la sécurité et de l'administration système, de toutes les ressources permettant une mise en place maîtrisée du schéma proposé. En particulier, ce schéma a déjà été mis en place, administré et validé pendant plusieurs années dans le cadre d'une précédente affectation d'un collègue.
2. Le LACL dispose de plus d'un ingénieur système qui administre au quotidien les ressources du laboratoire. Ses compétences permettrons une mise en œuvre rapide du schéma qui aura été défini avec le CRI et un pilotage au jour le jour de celui-ci.

Pour toutes ces raisons, nous aimerions entamer un cycle de réflexion avec les instances responsables au sein de l'université pour la mise en place et l'évolution des ressources informatiques. Pour que ce projet puisse être mené à bien dans les meilleures conditions, il nous semble essentiel que tous les acteurs - politiques et techniques - soient impliqués.