

EDITORIAL

Le CRI est à votre écoute depuis huit ans !

L'histoire des Technologies de l'Information et de la Communication est si rapide qu'elle en devient vertigineuse : à peine nés, l'Internet et le Web ont pris une ampleur dépassant les pronostics les plus fous, et sont devenus des outils incontournables au moins dans le domaine professionnel. Et ce n'est qu'un début : demain, les réseaux d'infrastructures se conjugueront aux services les plus innovants pour permettre des usages qui transformeront le quotidien.

Mais pour le moment, les TIC ont encore besoin d'être comprises et appréhendées. Et c'est pour construire une culture qui les intègre pleinement que le CRI accompagne depuis près de huit ans les organismes publics de la Haute-Savoie dans leur apprentissage. Environ 1000 journées-hommes de formation ont ainsi été dispensées en 2002, sur des thèmes adaptés aux besoins et aux niveaux de connaissance des stagiaires. En 2002, ce sont également plus de 25000 utilisateurs qui sont passés par le CRI pour relever leur boîte aux lettres ou pour naviguer sur le web, parfois sans même percevoir son existence !

Pourtant, si ces utilisateurs n'ont jamais connu de problèmes de sécurité, ou s'ils sont certains d'avoir une connexion permanente et fiable, c'est parce que le CRI n'est pas un FAI comme les autres. Il apporte ses compétences en matière de connectique, d'accès, de sécurité ou de développement, et surtout il fait évoluer ces compétences en fonction des besoins. Il est normal qu'après huit ans de proximité et d'échanges, le CRI ait une excellente connaissance des attentes de ses usagers. EdRes 74 ou PingOO IGWan (page 2) en témoignent ; les efforts de communication et d'information engagés récemment par le CRI également, puisqu'ils traduisent la volonté d'améliorer encore les services proposés. ■

**HAUT DEBIT**

Le haut débit pour tous, c'est pour bientôt !

Le débit (théorique) à 64 kbits/s qui arrive sur votre machine vous désespère ? Vous rêvez de débits supérieurs qui réduiraient votre temps de connexion et donc votre facture ? Dans sa démarche volontariste d'aménagement du territoire et de développement économique, le département de la Haute-Savoie a décidé d'initier une expérimentation de réseau à haut débit par voie hertzienne. Les enjeux liés au développement des Technologies de l'Information et de la Communication (enjeux sociaux, économiques, culturels) ont révélé la nécessité de trouver une solution au manque actuel d'offres alternatives. Parce que le département n'est pas assez attractif aux yeux d'éven-

tuels opérateurs alternatifs (population peu dense, répartie de manière trop inégale sur un territoire au relief accidenté), la Haute-Savoie s'engage dans une expérience dont les résultats devraient guider dans la mise en place d'un réseau de données à haut débit basé sur la technologie hertzienne.

La technologie hertzienne ne viendra qu'en complémentarité des autres techniques existantes (fibre optique, câble, ...), et a été retenue en raison de sa capacité à s'adapter à un moindre coût au relief et à la démographie du département. Une expérimentation dans un premier temps est nécessaire pour valider complètement cette technologie, mais aussi pour

valider un modèle économique attractif pour un éventuel opérateur, et déclencher la concurrence nécessaire au développement de services et d'offres attrayants. Enfin, cette expérience devra valider les usages faits du haut débit.

Maître d'oeuvre du projet et logiquement retenu comme tête de réseau en raison de la proximité du CERN, le CRI s'est donné 3 ans pour valider ces points essentiels de l'expérimentation. Si cette période de test s'avère concluante, un déploiement sur le reste du territoire sera alors envisagé. ■

Cécile BLONAY.

**PingOO IGWan**

Un nouveau PingOO pour allier rapidité et sécurité.

L'accès aux Technologies de l'Information et de la Communication a un prix, et les offres de forfaits avantageux qui fleurissent plus particulièrement depuis l'arrivée de l'ADSL sont intéressantes à bien des niveaux : augmentation des débits, coûts forfaitaires pour des temps de connexion illimités, sont autant d'arguments qui incitent les utilisateurs à privilégier l'aspect économique aux dépens de la sécurité.

En effet, les dangers potentiels liés à ces types de forfaits sont trop souvent occultés, et les économies réalisées peuvent se révéler bien négligeables comparées aux dépenses liées aux problèmes de sécurité. Si les plus connus sont les dysfonctionnements, même mineurs, mais occasionnant une perte de temps onéreuse, les intrusions, dégradations ou destructions totales des fichiers constituent, en plus des coûts induits par les opéra-

tions nécessaires pour réparer les dégâts, une atteinte insupportable à la liberté de chacun. C'est pour résoudre vos exigences budgétaires tout en continuant à vous garantir un service sans failles sécuritaires, que le CRI a développé un PingOO routeur sécurisé spécialement adapté à l'ADSL (voir page 2). ■

Cécile BLONAY.



Un PingOO routeur sécurisé pour l'ADSL

Un nouveau type de routeur pour PingOO

PingOO IGWan - Internet Gateway to Wan (Routeur ADSL, VPN et Firewall) est né d'une forte demande de nos utilisateurs qui désiraient avoir des connexions rapides et une meilleure maîtrise des coûts de connexion. Pour répondre complètement à cette demande, le CRI a développé une solution, encore en phase expérimentale, fondée entièrement sur des logiciels libres et des standards ouverts.

Qu'est-ce que l'ADSL ?

La technologie ADSL (Asymmetric Digital Subscriber Line) permet de faire transiter sur une simple ligne téléphonique des données numériques avec un débit pouvant atteindre le Mbits/s (1 000 000 de bits/s), voire plus dans un avenir proche, et dans la mesure où la ligne ne dépasse pas 6 km. Cette limite en distance ne permet pas de distribuer l'ADSL à l'intégralité de la population. **Actuellement 80 % de la population pourrait bénéficier d'une couverture ADSL** (contre 60 % uniquement en Haute-Savoie).

L'ADSL utilise un principe asymétrique pour le transfert des données. En effet, le débit pour la voie descendante (ce que vous récupérez depuis l'extérieur) est plus important que celui de la voie montante (ce que vous envoyez vers l'extérieur). Les débits actuellement commercialisés sont :

Voie montante	Voie descendante
64 kbits/s	128 kbits/s
128 kbits/s	512 kbits/s
256 kbits/s	1024 kbits/s

Outre le débit qui est nettement plus important qu'une connexion RTC (avec un modem classique à la norme V90 nous avons des débits en voie montante de 33,6 kbits/s et en voie descendante de 56 kbits/s) ou qu'une connexion RNIS (en voie montante ou descendante : 64 kbits/s), l'ADSL a la particularité d'avoir une **tarification de type forfaitaire** (connexion illimitée) et ce quel que soit le nombre de données transférées (pas de surcoût en cas de gros transferts). L'utilisateur est à même de prévoir ses coûts de connexion à l'avance et cela évite les mauvaises surprises à la réception de la facture téléphonique.

Dans une offre ADSL nous avons deux acteurs. Le premier est le "fournisseur de connexion", celui qui va vous permettre de vous relier "physiquement" au réseau. Aujourd'hui en France, il n'en existe qu'un seul et c'est France Télécom. Le deuxième est le fournisseur d'accès Internet (FAI), qui vous permet d'accéder à Internet et vous offre différents services, tels que la messagerie ou de l'hébergement web. Il en existe plusieurs mais ils ne sont pas forcément présents partout.

ADSL et la sécurité

Le fait de se connecter à Internet quelle que soit la méthode, **entraîne des risques de piratage de sa propre machine**. En vous connectant, votre FAI vous affecte une adresse qui **rend votre machine visible du monde entier**. Dans une connexion classique (RTC ou RNIS), le problème se pose moins puisqu'en général, vous restez connecté moins longtemps et à un débit assez bas. Par contre l'aspect forfaitaire de l'ADSL (on reste connecté très longtemps voire en permanence) et son débit (votre machine peut répondre plus vite aux requêtes) attire fortement les pirates.

Très peu de personnes se soucient de la sécurité de leur machine, pourtant par défaut la majorité d'entre elles ne sont pas sécurisées. Que ce soit le mot de passe administrateur qui n'existe pas ou des failles de sécurité des services qui tournent dessus, personne n'est réellement conscient des risques, tant qu'il n'a pas été victime d'une agression. Les pirates cherchent des failles de sécurité pour s'introduire sur la machine. Dans le meilleur des cas, seules **des données confidentielles peuvent être lues** (ses messages, son compte en banque, ses photos ou vidéos personnelles), mais il y a des scénarii

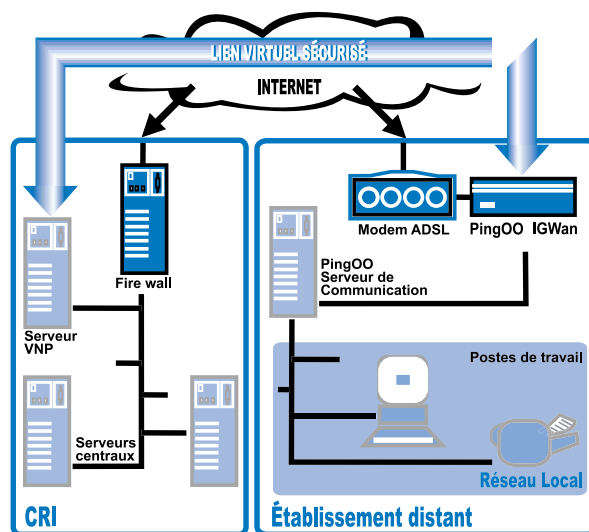
plus graves, comme la possibilité au pirate de **modifier les fichiers, d'y introduire des virus, de supprimer les données, ou d'utiliser la machine pour aller pirater une machine plus importante à ses yeux et d'en faire porter la responsabilité au "piraté"**.

VPN et Firewall

Pour remédier aux problèmes de sécurité, nous avons mis en place dans notre solution un **Firewall** (pare-feu). Cet outil permet de filtrer les éventuelles attaques venant de l'extérieur.

Afin de relier le réseau de l'établissement au réseau du CRI, et ce de manière sécurisée et confidentielle, nous avons mis en place ce que l'on appelle un VPN (Virtual Private Network, Réseau Privé Virtuel). D'ordinaire, pour relier deux réseaux distants et y faire transiter des données qui peuvent être confidentielles, on utilise des liaisons spécialisées, des liaisons RNIS ou d'autres technologies. Dans le cas d'une connexion ADSL, le seul moyen de faire la même chose est d'utiliser un VPN parce que le seul lien qui existe entre les deux réseaux, est le réseau Internet.

Toutes les données à destination du réseau du CRI sont cryptées par le routeur **PingOO IGWan** et décryptées par le serveur VPN au CRI (*voir schéma ci-dessous*). Aucune distinction n'est faite quant au type de données, le cryptage est fait "à la volée", le seul critère de sélection correspond à l'adresse de destination des données et non à leur contenu.



Le cryptage utilise le principe de clés asymétriques, avec une clé publique (connue de tous) qui permet de crypter des données, et une clé privée (connue par le serveur VPN ou le PingOO IGWan) qui permet le décryptage. A l'installation du routeur, nous faisons un échange de clés publiques pour que les deux machines puissent crypter avec la clé publique de l'autre.

Expérimentation

L'expérimentation a débuté le 16 octobre avec un seul établissement, et elle continue avec une dizaine d'établissements jusqu'à fin 2002. Les premiers retours que nous avons eus sont très satisfaisants, aussi bien sur la rapidité de la connexion, qu'au point de vue de la liaison virtuelle avec le CRI.

Déploiement

Afin de satisfaire un maximum d'établissements, le CRI a travaillé sur un processus d'installation rapide des routeurs. **Le déploiement officiel débutera en janvier 2003.** ■

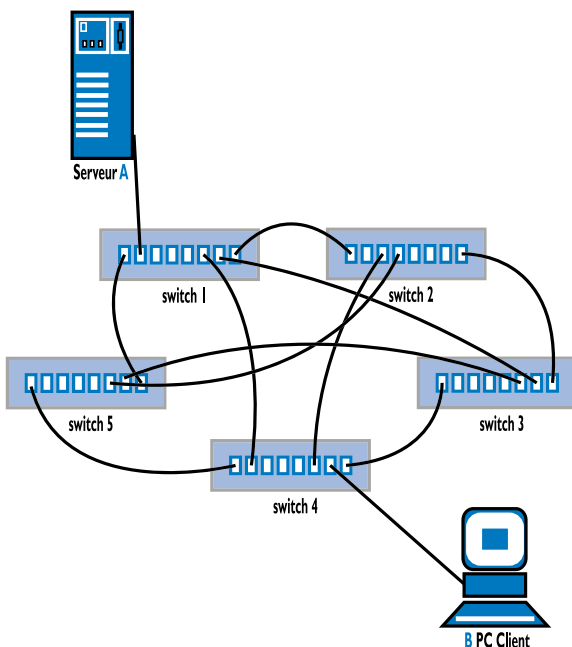
Un réseau : c'est bien ; un réseau qui fonctionne tout le temps : c'est mieux !

Suite de l'article "L'intérêt des réseaux informatiques" paru dans le précédent numéro de Réseaux74, accessible sur le web : <http://reseaux74.cri74.org/>

ARCHITECTURE ET TECHNOLOGIE RESEAU ADOPTEES :

En utilisant des technologies courantes en terme de réseaux locaux (réseau cuivre non-coaxial ou fibre optique à 10, 100 voire 1000 Mbits/s => connexion "en étoile" des postes sur des éléments centraux), lorsque l'on cherche une architecture (on parle aussi de **topologie**) à adopter pour pallier à tout problème de panne, on pourrait penser qu'il suffit de relier chaque équipement de concentration (hub) ou de commutation (switch) du réseau à l'ensemble des autres équipements constitutifs du réseau (voir schéma 1). Cette solution qui semble sans reproche comporte pourtant des imperfections notables : le nombre de ports utilisés sur chaque équipement uniquement pour le relier aux autres peut rapidement devenir énorme lorsqu'on atteint une taille et une complexité du réseau importantes (pour 5 switches, cela bloque déjà 4 ports...). De plus, le nombre de chemins possibles entre un point A et un point B est tellement important qu'il est source de complications (il faut que ce chemin soit le plus efficace, que tous les équipements du réseau se mettent d'accord pour savoir par où faire transiter les informations). Et dans un tel choix, on va se rendre compte qu'une grande partie des liens inter-équipements est tout simplement inutile.

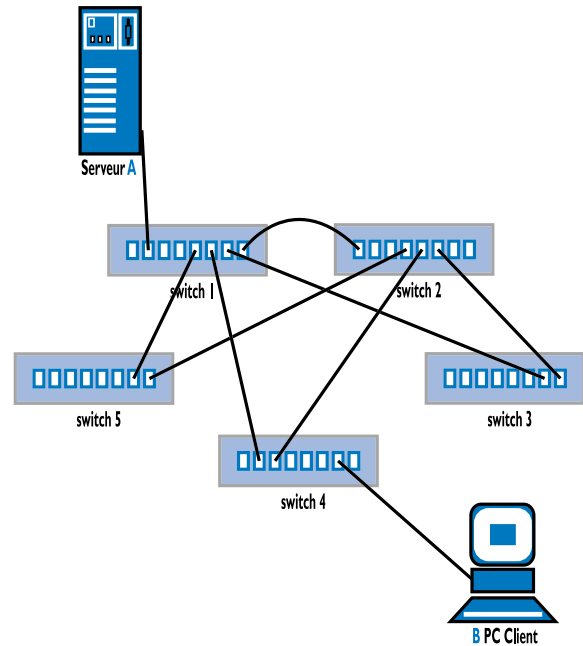
Schéma 1 :
redondance maximum sur un réseau local
(solution qui ne sera jamais retenue)



On trouve principalement deux topologies qui peuvent être appliquées pour offrir une redondance au niveau réseau. La première consiste à utiliser 2 switches fédérateurs sur lesquels seront raccordés par 2 liens chacun des autres commutateurs du réseau (voir schéma 2). On a ainsi une forte sécurité sur les pannes éventuelles mais l'inconvénient majeur est la nécessité d'avoir malgré tout un nombre important de liaisons inter-switchs qui peut être un facteur important lorsque les bâtiments n'offrent pas suffisamment de liaisons à travers le précablage (n'oublions pas que les switches peuvent être séparés par des étages, voire passer sous des cours, des parkings

sous lesquels on ne dispose pas toujours de plusieurs liens).

Schéma 2 :
redondance sur un réseau local avec 2 switches fédérateurs
(ici Switch1 et Switch2)



La deuxième solution (qui peut aussi être choisie en complément de la première citée précédemment, un mixage des 2 topologies est possible) consiste à mettre en place une boucle entre les différents équipements du réseau. En effet, à travers une boucle, pour aller d'un point à un autre, on a toujours deux chemins possibles à un instant "t". Dans le cas où une coupure surviendrait dans la boucle, il semblerait normal que tout le trafic réseau soit redirigé par le chemin encore valide. Dans un cas de figure mettant en scène 5 switches (commutateurs Ethernet) reliés en boucle, un fonctionnement "normal" fera transiter les informations entre une machine A et une machine B par un chemin (en général le plus court ou le plus rapide, voir schéma 3) et en cas de coupure de cette liaison "prioritaire", c'est l'autre partie de la boucle qui sera mise à contribution (voir schéma 4).

Ce dispositif qui semble assez évident dans la théorie n'est pas toujours facile à mettre en place dans la pratique et certaines précautions devront être suivies :

- Il faut éviter au maximum que 2 liens reliant des éléments entre eux passent physiquement par le même chemin. Dans l'exemple, si les liens sw1/sw5 et sw3/sw4 passent au même endroit dans un mur d'un bâtiment et qu'un coup de marteau piqueur malheureux soit donné juste à cet endroit (ou qu'un rongeur ait décidé de s'installer à proximité), on aura une rupture totale de la boucle et les deux parties seront totalement isolées. L'idéal (ce n'est pas toujours simple) est que les 2 liens de la boucle constituée empruntent des cheminements les plus distincts possibles afin qu'une perturbation ne puisse pas gêner les 2.

... page 4.

Schéma 3 :
fonctionnement normal sur une boucle établie à l'intérieur d'un réseau local

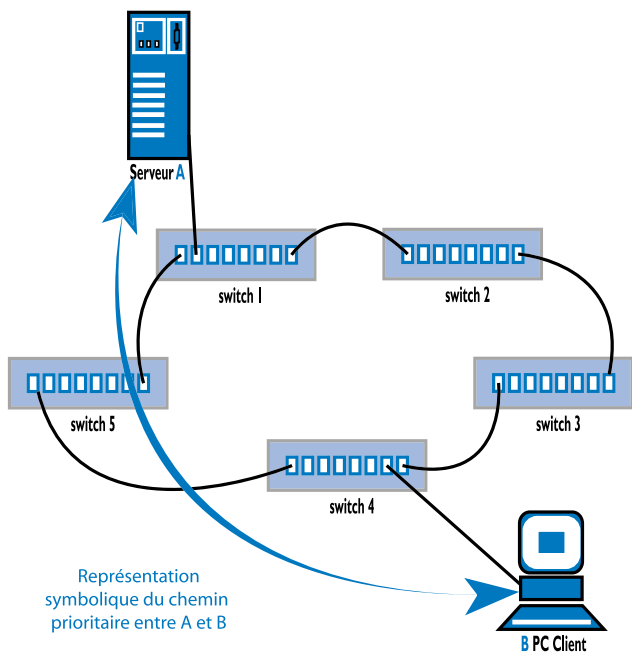
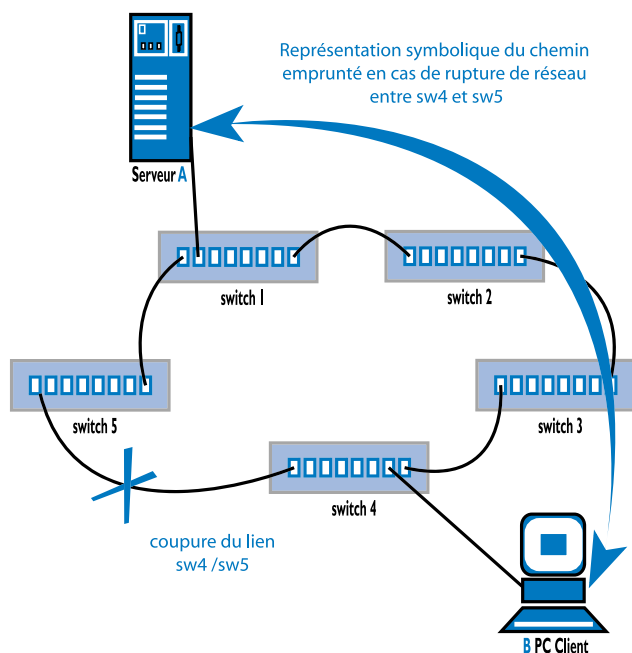


Schéma 4 :
Fonctionnement de secours en cas de problème sur la boucle



● Le fait que l'on mette en place une boucle dans le réseau est, en soi, perturbateur car à tout instant une information circulant sur celui-ci aurait deux chemins possibles. S'il y avait effectivement 2 chemins empruntés par les mêmes informations entre les mêmes machines, cela provoquerait des doublons dans les informations qui rendraient en fait impossible la communication et provoquerait en quelques secondes une saturation complète de la boucle et un blocage potentiel des équipements qui y sont reliés. En réalité, lorsque l'on met en place de telles boucles dans le réseau, il est absolument nécessaire d'utiliser du matériel adéquat qui soit correctement configuré pour qu'il gère lui-même, de façon automatique et en permanence, un point de rupture de la boucle. Ainsi, les équipements (dans notre exemple, les switches) communiquant entre eux et sous la responsabilité d'un matériel décideur (et assisté d'un secondaire en cas de problème sur le premier) vont provoquer eux-mêmes une

cassure en fonctionnement normal (dans le schéma 3, en estimant que c'est le switch1 qui soit "décideur" et le switch2 son secondaire, le lien sera coupé entre sw3 et sw4 au niveau de sw4). En cas de problème sur une partie de la boucle, les switches feront en sorte de rouvrir cet accès pour que les communications puissent continuer à transiter par le réseau (cette phase de transition prend tout de même quelques dizaines de secondes pendant lesquelles le réseau ne sera plus totalement opérationnel). Cette fonctionnalité repose sur le Spanning Tree qui, pour gérer ces effets de bouclages, est constitué de :

- un algorithme de calcul de la meilleure route en fonction de différents critères tels que le nombre d'intermédiaires, la nature des liens qui relient ces intermédiaires

- un protocole de communication STP (pour Spanning Tree Protocol, IEEE 802.1D) qui provoque les changements dans la topologie réseau utilisée en fonction des conditions) permettant de gérer ces effets de bouclage

- Pour permettre un accès permanent d'un serveur sur un tel réseau, il est de plus possible de s'orienter vers une utilisation de 2 cartes qui seront connectées à 2 switches différents de cette boucle avec une liaison réellement utilisée en fonctionnement normal et l'autre qui reste en attente ("standby", donc non active). Ainsi, si l'équipement auquel est relié le serveur par sa liaison principale venait à tomber en panne, la 2eme liaison prendrait le relais en quelques secondes afin que la coupure de service soit la plus courte possible.

Un grand nombre de technologies et notions abordées ici brièvement (mais aussi celles qui ont été volontairement écartées), étant particulièrement complexes, pourront faire l'objet d'un ou de plusieurs articles dans les prochains numéros de Rése@ux.74 tant le sujet est complexe et vaste. ■

Joël GOLLINET.



LIENS UTILES

Ping00

<http://www.Ping00.org/>

VPN - FreeS/WAN

<http://www.freeswan.org/>

Firewall - Netfilter

<http://www.netfilter.org/>

STP (Spanning Tree Protocol)

<http://www.labo-cisco.com/ArticleComp.asp?ARID=25>

EdRes74

<http://www.edres74.org/>

FORMATIONS

Afin d'accompagner l'appropriation des outils de communication utilisés sur les réseaux, le Centre de Ressources Informatiques propose des formations aux utilisateurs.

Internet pratique (2 jours)

Pour un apprentissage des principaux outils de l'Internet (navigation, courrier électronique, ftp, forums, moteurs de recherche...).

Langage HTML (2 jours)

Comment réaliser vous-même votre serveur et maîtriser votre éditorial.

Les prochaines sessions de formation organisées par le CRI :

16 et 20 décembre 2002

3 et 10 février 2003

10 et 17 mars 2003

VOEUX

Toute L'équipe du Centre de Ressources Informatiques vous souhaite un joyeux Noël, et une bonne année 2003 !



rése@ux.74

Lettre des technologies de l'information
Publication gratuite - N° d'ISSN : 1295-375X

Directeur de la Publication :

Joseph Bertholon, Président de l'Agence Economique Départementale Haute-Savoie.

Rédaction : Centre de Ressources

Informatiques - Bâtiment Le Salève

74 160 Archamps - Tél. : 04.50.31.56.30

Email : - reseau74@cri74.org

Web : - www.cri74.org

- reseau74.cri74.org

Siège : Agence Economique Départementale
BP 2444 - 74041 Annecy Cedex.

Tél. : 04.50.33.50.21 - Fax : 04.50.45.23.30

Édité avec le concours du Conseil Général de la Haute-Savoie.