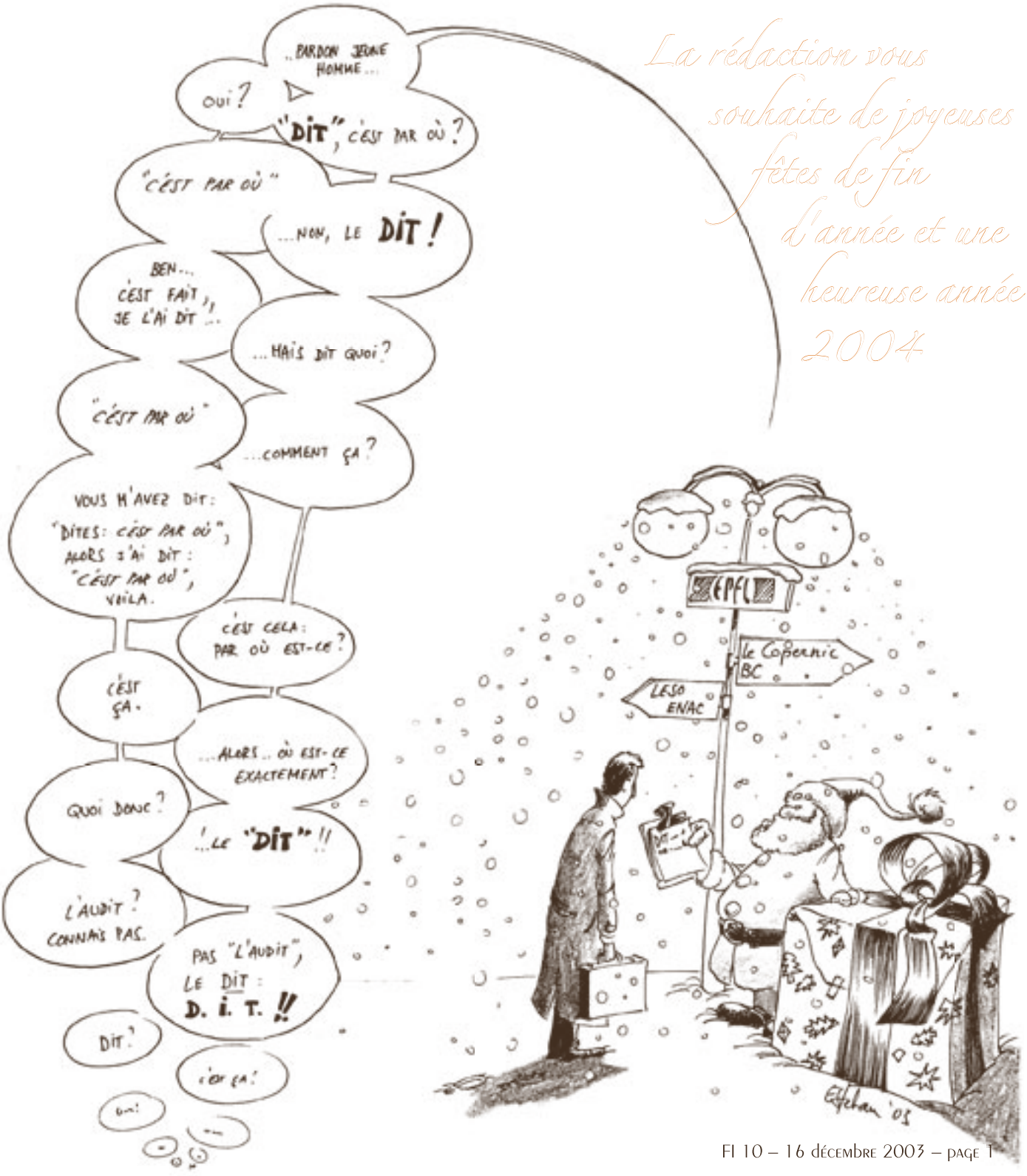
ECOLE POLYTECHNIQUE
FEDERALE DE LAUSANNE

flash informatique

p/a EPFL - Domaine IT – CP 121 – CH 1015 Lausanne – tél. +41 21 69 322 11 – web: http://dit.epfl.ch



La rédaction vous souhaite de joyeuses fêtes de fin d'année et une heureuse année 2004

DIT-info

Dernières nouvelles du mail à l'EPFL

Tous les messages entrant à l'EPFL, quel que soit le serveur de destination (mailbox centralisé proposé par le DIT ou serveur local d'institut) passent depuis le 12 novembre par une passerelle centrale qui effectue une vérification des adresses. Les messages passent ensuite par un filtre qui permet de rejeter:

- les messages infectés par des virus connus;
- les messages comportant des annexes dangereuses: .exe, .pif. .asp ..; la liste des extensions rejetées est maintenue à jour à l'adresse: ***mailwww.epfl.ch/danger.html.***

Les messages entrants et sortants ne sont plus limités en taille de façon centralisée. Ces limites de taille sont décidées par les administrateurs de serveurs de messagerie; pour information, pour un utilisateur du service **Mailbox** ou des serveurs Exchange, la limite de taille vient d'être portée à 10MB pour les messages entrants. Pour les messages destinés à des boîtes qui seraient sur d'autres serveurs (gérés par des instituts ou laboratoires), c'est la taille maximale éventuellement décidée par les administrateurs de ces serveurs qui intervient.

Depuis l'annonce du filtre anti-spams MailCleaner (voir FI 8/03, ***http://dit.epfl.ch/publications/FI03/fi-8-3/8-3-page7.html***), plus de 700 personnes s'y sont abonnées. A présent, seuls les messages en provenance de l'extérieur sont filtrés. Les messages internes (EPFL--> EPFL) ne seront donc plus freinés par ce filtre. Rappel: pour s'abonner à MailCleaner, aller sur l'adresse: ***mailcleaner.epfl.ch***.

Service Mailbox

Au mois d'octobre dernier, le service Mailbox a été doté d'un troisième serveur de messagerie afin d'accueillir les nouveaux arrivants des sections de Mathématiques et de Physique de l'UNIL et également de permettre une augmentation des quotas. Ce service est donc maintenant composé de trois serveurs de messagerie pour le stockage des messages et de deux frontales pour l'accès au service via les protocoles POP3/POP3S et IMAP/IMAPS. Rappelons que le service Mailbox peut être aussi accédé à travers une interface Web à partir de l'adresse ***mailbox.epfl.ch***.

Les quotas sont fixés maintenant à 40 MB pour les étudiants et jusqu'à 60 MB pour le personnel. Ces quotas sont déjà actifs sur deux des trois serveurs et ils seront mis en place d'ici la fin de l'année sur le troisième. Ce délai doit permettre de déplacer progressivement certains utilisateurs pour équilibrer la charge sur les trois serveurs.

N'oublions pas encore de rappeler que dans la configuration des clients de messageries usuels – Mozilla, Netscape Messenger, Outlook Express, Outlook, Eudora, ... – pour le service Mailbox, le serveur entrant (Incoming Mail Server) doit être **mailbox.epfl.ch** et non plus **imap.epfl.ch** !

Jacqueline.Dousson@epfl.ch, Domaine IT

Flash informatique

Les articles ne reflètent que l'opinion de leurs auteurs. Toute reproduction, même partielle, n'est autorisée qu'avec l'accord de la rédaction et des auteurs.

Rédacteur en chef:	Jacqueline Dousson, fi@epfl.ch
Mise en page & graphisme:	Appoline Raposo de Barbosa
Comité de rédaction:	Omar Abou Khaled, Jean-Daniel Bonjour, Nicolas Bouche, Milan Crvcanin, Jean-Damien Humair, Pierre Kuonen, Jacques Menu, Maciej Macowicz, Philippe Pichon, Daniel Rappo, François Roulet, Christophe Salzmann & Jacques Virchaux
Impression:	Atelier de Reprographie EPFL Tirage: 4000 exemplaires
Adresse Web:	***http://dit.epfl.ch/publications/***
Adresse:	DIT-GE EPFL, CP 121, CH-1015 Lausanne Téléphone: +41 21 69 32246 & 32247

Abonnez-vous à la version électronique du Flash informatique en envoyant un courrier à: fi-subscribe@listes.epfl.ch

Pourquoi l'idée saugrenue de construire un réseau de quarantaine nous est-elle venue et comment l'avons nous réalisée ?

Richard.Timsit@epfl.ch, Domaine IT

A la fin du mois de juillet 2003 nous nous sommes trouvés dans une situation bien embarrassante. Des centaines de machines porteuses du ver de la famille Lovsan (***http://vil.nai.com/vil/content/v_100552.htm***) manifestaient une activité sur le réseau qu'il était impossible de tolérer. Cependant, aucune des mesures que nous pouvions prendre n'était satisfaisante.

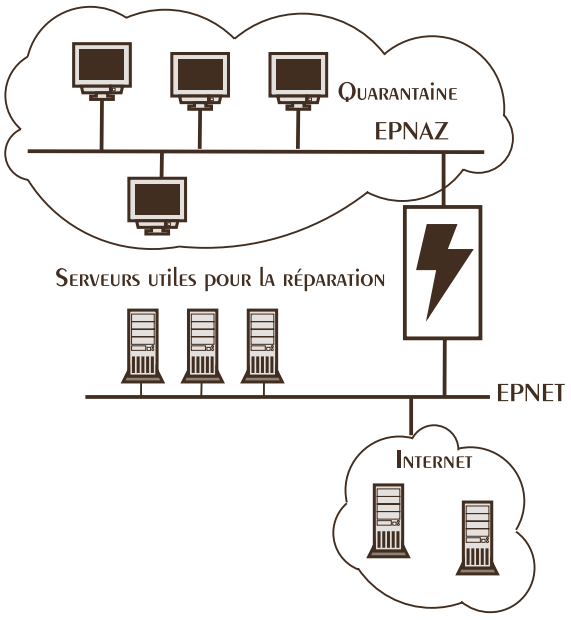
- Couper la machine du réseau, privait son administrateur de tous les moyens mis à disposition pour la réparer (nous ne fournissions pas de CD car la version d'antivirus changeait de jour en jour).
- Interdire seulement l'accès à Internet pour permettre la réparation sur Intranet –solution adoptée– présentait l'inconvénient de laisser la machine polluer l'Intranet.

C'est dans le souci de trouver une alternative à ces deux solutions décevantes que l'idée d'un réseau de quarantaine a germé et que nous l'avons réalisée.

Principe de la solution

Nous basculons dans ce réseau toute machine nécessitant d'être isolée d'EPNET (Intranet EPFL) et/ou d'Internet et nous nous donnons du même coup les moyens:

- d'**avertir** l'utilisateur de la machine,
- de mettre à sa disposition les outils de **diagnostic** et de réparation
- d'offrir une solution pratique de **rétablissement** sur EPNET



Protrait robot de la solution

Les réseaux de campus ou d'entreprise sont aujourd'hui entièrement construits à l'aide de réseaux virtuels (Vlan) si bien que fabriquer le réseau de quarantaine en faisant basculer les machines à isoler dans un tel Vlan s'est imposé naturellement comme le principe de la solution. En effet une machine est reliée à un port d'un équipement actif du réseau (un switch) et chaque port de cet équipement est associé à un Vlan. Ce dernier est choisi en fonction de l'unité à laquelle appartient la machine. En général toutes les machines d'une unité appartiennent à un même Vlan qui recouvre en fait un subnet. Changer brutalement le Vlan du port sur lequel est raccordé une machine va bouleverser sa participation au réseau.

Veiller à ne pas bloquer la machine et continuer de lui donner les services essentiels à sa survie en réseau pour permettre sa réparation, tel est le point essentiel du cahier des charges de ce projet de quarantaine.

Le port sur lequel la machine est raccordée est donc basculé dans un Vlan préparé pour accueillir la nouvelle venue. Cette préparation consiste à offrir tous les services essentiels pour qu'une machine correctement configurée sur EPNET continue à fonctionner. Un routeur par défaut en fonction de son Vlan (en fait son subnet) d'origine est mis à sa disposition. Elle bénéficie aussi d'un service de résolution de noms IP (DNS) et d'un distributeur d'adresses IP (DHCP) au cas où elle en serait tributaire. Ceci afin que l'utilisateur de l'ordinateur n'ait pas l'impression qu'il se soit planté (impression d'autant plus légitime rappelons le que cet ordinateur a de bonnes raisons de dysfonctionner). Dès ce moment là, on va tenter d'avertir et d'informer, en envoyant un popup quand c'est possible (machine sous Windows) et/ou en imposant une page html d'alerte pour toute URL réclamée...

C'est alors que l'utilisateur peut suivre les liens proposés et accéder aux ressources qui vont lui permettre de réparer sa machine et de revenir blanchi sur EPNET.

Seules des liaisons HTTP et HTTPS sont possibles et avec certains sites uniquement.

- ***Winsec.epfl.ch*** (pour les consignes de réparation et les patchsWindows)
- ***linuxline.epfl.ch*** (idem pour Linux)
- ***sunline.epfl.ch*** (idem pour Solaris)
- ***download.microsoft.com***
- ***windowsupdate.com***
- ***vil.nai.com*** (information sur les méfaits des vers et virus en cause)

D'autres liens seront ajoutés en fonction des besoins. Tout est fait à l'heure où cet article est rédigé pour qu'une machine atteinte d'un ver de la famille Blaster ou de la famille Sdbot puisse être nettoyée, patchée et abonnée à une mise à jour

automatique de son antivirus (EPO, cf ***http://dit.epfl.ch/SA/publications/FI03/fi-6-3/6-3-page1.html***).

Enfin, des formulaires pour réclamer aide et remise en service sur EPNET sont mis à disposition.

Détails d'implémentation

Le dispositif mettant en liaison le Vlan de quarantaine avec le réseau EPNET peut être construit d'une multitude de façons. La version présentée donne satisfaction au moment où cet article est écrit, mais elle n'a été mise à l'épreuve qu'avec quelques dizaines de machines mises en quarantaine et devra certainement être améliorée pour faire face aux offensives attendues sur un parc de machines vulnérables aussi vaste que le nôtre ;-).

Deux machines Linux munies chacune de 2 interfaces réseau et reliées entre elles par un câble croisé se partagent la délicate activité d'assurer de vrais faux services et de ne laisser passer que ce qu'il faut.

Les machines entrant en quarantaine gardant leur configuration réseau vont recourir (comme on l'a mentionné plus haut) à un routeur par défaut pour toute communication avec les machines étrangères à leur sous-réseau. Elles perdront donc tout contact avec les machines de leur unité à moins que celles-ci soient aussi tombées en disgrâce. Offrir ce routeur par défaut est un premier devoir et en même temps une première chance car cela rend possible le confinement du trafic.

Le serveur de noms est un service facile à offrir grâce à la coopération entre un serveur-cache standard sur le réseau EPNET et celui qui répondra aux requêtes de machines en quarantaine. Le service DHCP est d'autant plus facile à offrir que le couple adresse IP et adresse physique des candidats à la réparation est connu au moment de la sortie d'EPNET. La machine gardera cette adresse IP pendant tout le temps qu'elle sera en quarantaine, un *reboot* s'imposera donc au moment de son retour au net.

Reste à acheminer les requêtes http aux serveurs qui doivent être accédés et à forcer une page de retour pour toutes les autres. Ce travail est confié à un tandem Squid/Jesred mais de nombreux modules de proxy-redirection d'URL pouvant travailler en mode transparent peuvent être choisis.

Enfin, voulant offrir la possibilité aux malheureuses victimes des virus et des faiblesses de la marchandise d'un certain constructeur d'avoir recours à *windowsupdate,* il nous a fallu aussi perméabiliser l'HTTPS. Ceci est fait simplement en réalisant une translation d'adresse pour ce protocole à travers nos deux machines d'interface. La réalisation du proxy transparent réclamant le secours d'Iptables sous Linux - pour substituer le port de destination 80 par celui que l'on a choisi pour le proxy, on en profitera pour rajouter les lignes qu'il faut dans la table de translation pour que les adresses source des requêtes HTTPS soient translatées sur chaque machine avec l'adresse de son interface propre. Sur la machine d'interface avec le réseau de quarantaine on donne l'adresse du réseau privé et sur l'autre machine, l'adresse de son interface sur EPNET.

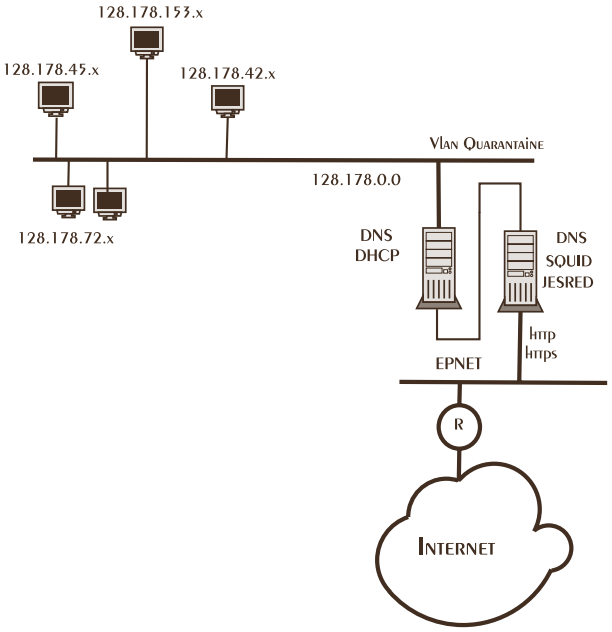


Schéma plus détaillé

Bilan provisoire

Les machines atteintes d'un virus qui déclenchent une activité réseau suffisamment anormale pour imposer leur coupure nous donnent souvent un moyen aisé de les détecter pour les basculer automatiquement. C'est le cas des vers de la famille Blaster. Une cascade d'automates intervient sur les équipements et prépare l'accueil de la machine en quarantaine. Les messages envoyés sur cette machine sont spécifiques à son problème. Sa sortie de quarantaine se fait automatiquement pour autant que les vulnérabilités aient été colmatées.

Parfois la détection est plus délicate, la décision du basculage est manuelle, mais le reste du processus ne change pas.

Disposer d'un tel outil s'avère précieux. Soustraire du réseau tout en permettant la réparation… à l'aide du réseau, est un bien grand service rendu. Malheureusement nous sommes aussi honteux d'avoir recours à un tel service à une si grande échelle sur notre campus. Cela signifie que notre parc de machines est mal géré. Il vaut mieux prévenir que guérir, on ne le dira jamais assez en matière d'informatique car les virus de demain ne ressembleront peut-être pas à ceux d'aujourd'hui et risquent de transformer notre réseau de quarantaine en un immense et désolant cimetière. ■

Knoppix et VPN, voyagez léger

Vittoria.Rezzonico@epfl.ch, SB-IACS & Daniel.Grandjean@epfl.ch, Domaine IT

Le Guide du routard galactique a son mot à dire au sujet des serviettes: la serviette, nous apprend-il, est sans doute l'objet le plus vastement utile que puisse posséder le routard interstellaire, dixit *Douglas Adams, The Hitchhiker's Guide to the Galaxy*.

Avec le client VPN [***http://dit.epfl.ch/SA/publications/FI03/fi-7-3/7-3-page7a.html***] installé et configuré sur votre machine, vous êtes de n'importe où connecté comme si vous étiez présent sur EPNET, le réseau de l'école. Toutefois malgré les progrès de la miniaturisation, votre ordinateur représente toujours un excédent de bagages. Aussi nous vous proposons, pour votre prochain périple, de n'ajouter à votre serviette qu'un CD *bootable* Linux et une clef mémoire USB. Ceci vous permettra d'utiliser les ressources des machines que vous n'aurez aucune peine à emprunter, arguant en toute bonne foi, que **vous n'y toucherez pas !**

De nombreuses distributions CD ou DVD *bootables* sont disponibles aujourd'hui. Chacune couvre un besoin comme d'avoir une démo Linux, un routeur, un serveur d'impression, un firewall, un lecteur multimédia, etc. Mais récemment une distribution Linux de cette famille est devenue très populaire.

- Son CD offre sur un système de fichier compressé une distribution Linux complète avec 2G octets d'applications, dont une suite Office, des jeux, des outils de développement, de communication, de dessin, d'édition multimédia, le tout dans une interface graphique léchée.
- Elle intègre un excellent programme d'autodétection de la configuration matérielle pour tirer au mieux parti des configurations des machines les plus exotiques. Juste pour cela, elle est un précieux outil de diagnostic et d'installation Linux.
- Elle est mise à jour très fréquemment suivant de près les développements matériels et logiciels. La cohérence est préservée par l'interface utilisateur.
- Elle ne permet pas par défaut d'altérer les données de la machine hôte. Ses applications sont lancées sans privilège indu.
- Elle permet le stockage aisé de données persistantes. Vous pouvez ainsi créer et sauver des documents sur un support de données amovible; ils seront à l'avenir accessibles d'un redémarrage à l'autre, d'une machine à l'autre. Ce même support peut être encrypté pour préserver vos informations confidentielles contre la copie ou la perte du média.
- Elle est basée sur une distribution réputée et vivante, la Debian.
- Elle vous paraîtra, une fois cet article lu, raisonnablement facile à personnaliser.

Le non de cette merveille ? **Knoppix**, du nom de son créateur Klaus Knopper.

Les ingrédients

Un CD Knoppix

Cuisiné selon les indications données ici ou plus simplement gravé à partir de la page ***http://network.epfl.ch/knoppix/.***

Une clef mémoire USB

Cette clef étant le support d'échange entre toutes les machines visitées, nous vous conseillons de garder les choses simples. Formatez la clef avec un système de fichiers FAT. Elle pourra être lue et écrite par tous les systèmes d'exploitation et machines qui sauront la reconnaître. Elle sera utile même en l'absence de Knoppix.

PC du genre Intel

Il doit avoir un BIOS qui permette de démarrer depuis le CD-ROM, bien sûr un lecteur de CD et une interface USB.

Un câble de rallonge USB

Il augmente le confort, car il peut être ardu, voire impossible, d'enficher sa clef au milieu d'une forêt de connecteurs et de fils.

Mémoire flash USB

C'est vos finances et vos besoins qui dicteront la taille de la mémoire. Choisissez de préférence une clef avec un commutateur pour la vérouiller en mode lecture uniquement. Ce mode préserve vos données contre de mauvaises manipulations et réduit la fatigue de la clef. Les mémoires NAND-flash ont, selon leur provenance et leur mise en oeuvre, une durée de vie comprise entre 10K et 1000K cycle d'écriture. Le nombre de cycles en lecture est illimité. Une alternative à la clef est un adaptateur USB pour les cartes-mémoires SM, CF, SD ou memory stick. Cette approche n'est pas forcément plus volumineuse et permet d'utiliser la mémoire de votre appareil de photos ou de votre caméscope.

Comment fabriquer un CD VPN-Knoppix

Ingrédients

- Un CD Knoppix
- Un ordinateur avec
  - un lecteur CD-ROM;
  - un graveur CD ou une manière de graver un CD (autre machine avec un graveur connecté au réseau);
  - au moins 3.5 GB d'espace disque libre;
  - un total de RAM+swap d'au moins 1GB.

Partie 1: la rémastérisation

Cette partie consiste à personnaliser le contenu du système de fichiers *live* qui se trouve comprimé dans le fichier `/cdrom/KNOPPIX/KNOPPIX`. Puisque l'on veut ajouter le client VPN aux programmes préexistants, il faut en passer par là.

Préparation

- Démarrez sur le CD Knoppix, créez un système de fichiers ext2 (ou ext3) dans l'espace libre.
  Soit `$KNX` le répertoire de travail, c'est-à-dire celui où vous placerez tous vos fichiers Knoppix (situé sur la partition créée auparavant et montée à la main en étant root, ceci est important pour éviter les erreurs dues à l'option *nodev*).

```
cd $KNX
mkdir addons
cp -Rp /KNOPPIX source/
cp -Rp /cdrom master/
```

  on peut éviter de copier le gros fichier KNOPPIX
- Copiez les fichiers nécessaires (dans notre cas le client VPN) dans `$KNX/source/var/tmp/`, puis

```
chroot $KNX/source
```

- Lancez **dselect** et enlevez quelques paquetages (la Knoppix fait presque **exactement** 700MB!).
- Installez le client VPN (qui se trouve dans `/tmp/`) comme d'habitude, acceptant toutes les réponses proposées par défaut.
  Les clefs EPFL ne `doivent` pas traîner sur un CD:

```
rm -f /etc/CiscoSystemsVPNClient/Profiles/*
```

- Modifiez le script `/etc/init.d/knoppix-autoconfig` comme suit: ajoutez vers la fin du fichier

```
# EPFL VPN Client fixes
# link fix
rm -f /etc/CiscoSystemsVPNClient/vpnclient.ini
cp /KNOPPIX/etc/CiscoSystemsVPNClient/ \
vpnclient.ini /etc/CiscoSystemsVPNClient/
[ -d /home/knoppix/Profiles ] && cp - \
a /home/knoppix/Profiles/*.pcf /etc/ \
CiscoSystemsVPNClient/Profiles/
# end EPFL VPN Client fixes
```

- Modifiez les scripts `/etc/init.d/knoppix-halt` et `/etc/init.d/knoppix-reboot` comme suit:

  au début du fichier après

```
PATH=/sbin:/bin:/usr/bin:/usr/sbin
export PATH
```

- Ajoutez

```
# VPN Profile cleanup
# if profiles in home and on filesystem differ
# copy filesystem profiles in home after a backup
for f in `ls /etc/CiscoSystemsVPNClient/ \
Profiles/*.pcf`; do \
cmp /etc/CiscoSystemsVPNClient/Profiles/ \
`basename $f` /home/knoppix/Profiles/`basename \
$f` > /dev/null || (cp /home/knoppix/Profiles/\
`basename $f` /home/knoppix/Profiles/`basename \
$f`.old; cp /etc/CiscoSystemsVPNClient/ \
Profiles/`basename $f` /home/knoppix/Profiles/);\
done
# end VPN Profile cleanup
```

- Sortez avec un ctrl-D du chroot.
- Faites le nettoyage (videz `$KNX/source/tmp`, purgez `$KNX/source/root` et enlevez `$KNX/source/.rr_moved`). Si vous voulez des icônes pour démarrer et arrêter le client VPN, vous pouvez les créer maintenant comme indiqué à la page *http://seismo.ethz.ch/linux/vpnclient.html*. Cette procédure créera des fichiers dans `/home/knoppix/Desktop`. Repérez-les et copiez-les dans `$KNX/source/etc/skel/Desktop`.
- Mastérisation, première partie (cela peut prendre longtemps!). La commande magique est

```
mkisofs -R $KNX/source | create_compressed_fs \
- 65536 > $KNX/master/KNOPPIX/KNOPPIX
```

Partie 2: modification du boot

```
cp $KNX/master/KNOPPIX/boot.img $KNX/addons/ \
boot-orig.img
cd $KNX/addons
cp boot-orig.img boot-epfl.img
mkdir /tmp/mnt
mount -oloop boot-epfl.img /tmp/mnt
```

Voilà maintenant, vous avez la partie du CD qui contrôle le boot dans le répertoire `/tmp/mnt`.

- modifiez le `boot.msg` pour y mettre un message personnalisé
- modifiez le `syslinux.cfg` pour faire un `home=scan` par défaut et changer la disposition du clavier si nécessaire.
- modifiez la page de garde de démarrage comme suit: créez une image avec une taille de 640x400 et au maximum 16 couleurs. Ensuite exécutez la commande

```
bmptoppm monimage.bmp | ppmtolss16 > /tmp/\
mnt/logo.16
```

C'est tout pour les modifications du boot.

```
umount /tmp/mnt
cp boot-epfl.img $KNX/master/KNOPPIX/boot.img
```

- Dernière manipulation, il faut recalculer les sommes md5 des fichiers que l'on a alterés (`$KNX/master/KNOPPIX/KNOPPIX` et `$KNX/master/KNOPPIX/boot.img`) en utilisant la commande `` `md5sum fichier` ``. Ensuite remplacez les anciennes sommes qui se trouvent dans le fichier `$KNX/master/KNOPPIX/md5sums`.
- Il est temps de créer le CD Knoppix tout nouveau tout beau.

```
cd $KNX/master
mkisofs -r -J -b KNOPPIX/boot.img -c KNOPPIX/ \
boot.cat -o $KNX/addons/myknoppix.iso $KNX/ \
master
```

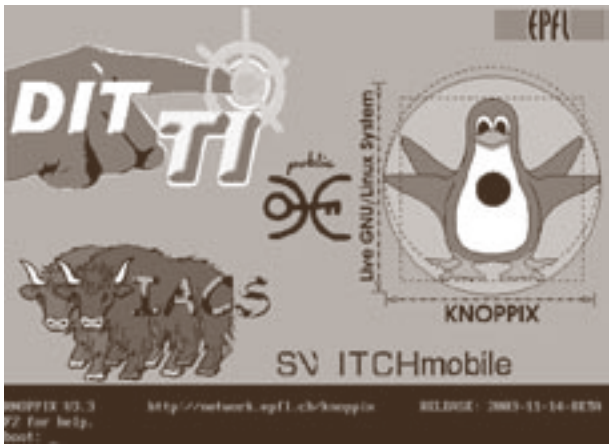
Maintenant, gravez `$KNX/addons/myknoppix.iso`. Utilisez ce nouveau CD pour démarrer votre PC. ■

Comment utiliser Knoppix ?

- Insérer le CD Knoppix dans le lecteur de votre ordinateur.
- Insérer votre clef-mémoire dans une des prises USB du même ordinateur
- Faire démarrer l'ordinateur depuis le CD.

Seule cette dernière opération peut s'avérer délicate sur une machine inconnue. Mais souvent, le BIOS des machines démarre depuis le CD présent dans le lecteur à la mise sous tension si celui-ci est bootable. Sinon regardez dans la configuration du BIOS et mettez le CD avant le disque dur HDD dans l'ordre d'initialisation. Les BIOS récents ont souvent une touche spéciale qui permet de choisir au démarrage et pour une seule fois un autre média (F12 Boot Menu). Cette dernière particularité permet de démarrer depuis un CD sur les machines dont le BIOS est verrouillé par l'administrateur.

La machine charge SysLinux et vous présente une invite de commande. À ce stade vous pouvez donner des options de démarrage ou *cheat codes*. Pour le moment, admirons l'écran et attendons la suite.



Knoppix démarre. Si tout se passe sans problème, vous êtes dans l'environnement graphique KDE, dans une session ouverte en tant qu'utilisateur **knoppix**.

Bienvenue à Knoppix !

Home sweet home

Le PC a démarré avec Knoppix et la clef USB pour la première fois. C'est le moment de configurer un répertoire privé *(home directory)* persistant sur votre clef. Vous pourrez laisser dans cet espace disque les fichiers et les configurations du système que vous retrouverez au prochain redémarrage, sur cette machine ou une autre.

Obtenons d'abord le fichier de configuration du client VPN. Ce fichier contient les informations nécessaires pour établir une connexion avec les concentrateurs VPN. Il peut également contenir vos réglages personnels et vos mots de passe, pratique que nous déconseillons fortement.

Télécharger la configuration du client

- Ouvrir une fenêtre **Konsole** en cliquant l'icône dans la barre d'outils au pied de l'écran.

- Taper la commande epfl_profile.
- Une fenêtre Mozilla s'ouvre. Passé les questions usuelles, vous arrivez à un formulaire qui requiert votre numéro Sciper et votre mot de passe Gaspar. Chose faite, sauvegardez sur disque le fichier **EPFL_LAN.pcf** dans le directoire **/home/knoppix/Profiles**.
- Quittez Mozilla.

Créer le home directory

Avec la souris, en bas à gauche de l'écran, sélectionnez le Pingouin. C'est le menu KNOPPIX.

- Choisir > **Configure** > **Create a persistent KNOPPIX home directory**. Vous serez guidé pas à pas au cours de la manipulation.

- Première question, et **YES** vous voulez continuer.
- Choix de l'emplacement de votre home: Votre clef USB sera un device de type /dev/sd. S'il n'y a pas de disque SCSI sur votre machine, ce sera très probablement /dev/sda ou /dev/sda1. En cas de doute, regardez ce qui change dans le menu qui vous est offert en démarrant sans la clef USB.
- Choisissez l'option qui crée une image dans le système de fichiers (NO, par opposition à utiliser tout l'espace disponible).
- Choix de la taille de votre home. Il sera matérialisé par un fichier de la dimension choisie et nommé **knoppix.img**. Il n'est généralement pas nécessaire d'avoir un grand espace. Tout ce que vous allouez est perdu pour l'usage de la clef avec *d'autres* systèmes, alors que la totalité de l'espace FAT est disponible pour Knoppix. Le défaut de 30M est très confortable.

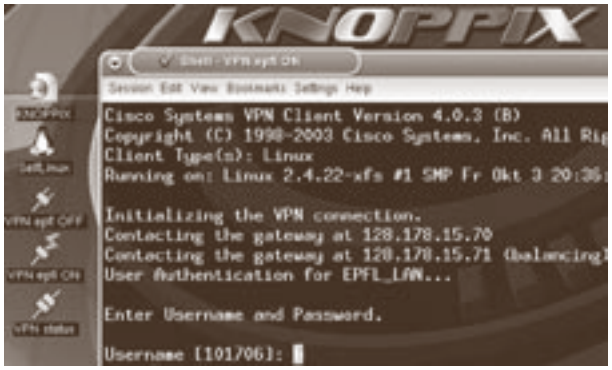
Knoppix et Disaster Recovery

Une distribution Knoppix est un élément indispensable de la boîte à outils du gestionnaire de systèmes. Elle peut être enrichie à loisir des outils que l'on considère comme indispensables à cet apostolat ;-). On peut la configurer pour qu'elle puisse assurer l'intérim d'un service particulier en cas de coup dur. Toutefois, dans le cadre de Disaster Recovery ou de restauration après sinistre, une meilleure approche s'impose. Comme ce type d'intervention se planifie à l'avance, on prépare un CD/DVD bootable qui correspond à la machine à restaurer. Ce CD contiendra toutes les informations propres à ce système telles que les partitions des disques, la configuration du RAID logiciel, le bootloader, le kernel en production, les utilitaires spécifiques à du matériel spécialisé. Un tel disque est facilement créé par et à partir de la machine que l'on souhaite protéger. L'outil qui vous assistera dans cette tâche est **Mondorescue** (***www.mondorescue.org*** ou le mirroir suisse ***http://samba.epfl.ch/mondo)***. **Mondorescue** crée un ou plusieurs CD/DVD bootables qui contiennent la configuration et tout ou partie des données de la machine où il s'exécute. Ces médias permettent de dépanner ou de reconstruire un système après un sinistre total. Ils sont également une excellente première étape pour rétablir un système d'exploitation au niveau où la restauration des sauvegardes est opérationnelle. Le point fort est que le CD démarre avec le kernel et les drivers de la machine originale, ce qui permet de travailler dans l'environnement utilisé en production. **Mondorescue** peut être exécuté régulièrement pour avoir des images de CD à jour. On les déposera sur une autre machine, et leur présence selon les règles de Murphy tiendra la foudre à distance. Un CD Mondorescue est indispensable entre les pages du livre de bord de tout serveur qui se respecte.

- Choix paranoïaque: souhaitez-vous chiffrer votre home? C'est un choix que nous laissons à votre discrétion. Mais attention, pour décoder votre *home* il faudra taper une *passphrase* d'une taille minimale de 20 caractères, et cela peut devenir pénible à l'autre bout du monde avec un clavier très exotique. Si vous voulez vraiment cette sécurité, il peut être préférable de faire un second système de fichiers non nécessaire au démarrage de Knoppix.

Une fois la création terminée, redémarrons la machine et cette fois votre *home* Knoppix est dans la clef.

A ce stade, si votre machine est branchée à un réseau, cliquez sur l'icône [VPN epfl ON] ou passez la commande **vpnclient connect EPFL_LAN**. Vous serez connecté à EPNET. L'icône [VPN satus] ou la commande **vpnclient stat** retourne l'état de la connexion. Pour vous déconnecter, cliquez [VPN epfl OFF]



Voilà, vous avez fait d'une pierre deux coups. Premièrement, vous avez un CD Knoppix personnalisé. Compatible avec l'infrastructure SWITCHmobile [***http://dit.epfl.ch/publications/FI03/fi-6-3/6-3-page3.html***], utile dans toute la galaxie. Deuxièmement, vous avez créé une distribution personnalisée de Knoppix. Nous souhaitons que cela vous ait donné l'envie d'en faire d'autre avec vos outils favoris, vos supports de cours ou autres réalisations personnelles. Et là, seule votre imagination est la limite.■

Journée de présentation de la technologie DSP

Polydôme de l'EPFL
mardi 20 janvier de 8h30 à 17h30

Le **Laboratoire de Production Microtechnique de l'EPFL** organise une journée de présentation des solutions de traitement numérique de la vidéo et des télécommunications sur DSP en collaboration avec deux partenaires industriels ATEME et TEXAS INSTRUMENTS.

Cette journée est une opportunité pour découvrir la technologie DSP ainsi que ses applications au domaine de la vidéo.

Elle s'adresse tant aux néophytes intéressés par ces technologies qu'aux utilisateurs avertis et tout sera mis en œuvre pour favoriser les échanges d'informations. Aux présentations orales s'ajouteront des démonstrations de matériel et de logiciel de compression vidéo réalisées par les partenaires et des industriels locaux.

Pour tout renseignement, consulter le lien ***http://www.ateme.com/products_fr.php?url=/products/seminar_lausanne_fr.php*** ou contacter ***communication@ateme.fr***.

Projet KTI/CTI n° 6546.1 FHS-ET

Autonomous Wireless LAN Management

Vincenzo.Inguscio@eif.ch,
Eric.Marchon@eif.ch &
Jean-Frederic.Wagen@eif.ch, Ecole d'ingénieurs et d'architectes de Fribourg



Résumé

Les **Wireless Local Area Networks** (WLAN) deviennent de plus en plus populaires. Standardisés dès 1999 par l'IEEE sous les normes 802.11b, g, et a, ces technologies connues sous le nom *grand public* Wi-Fi [1]-[3], permettent l'interconnexion d'ordinateurs grâce à un réseau sans fil. Les WLANs connaissent depuis le début des années 2000 un essor fulgurant chez les privés, dans les entreprises et notamment, en émergeant sous la forme de Hot Spots pour l'accès public à l'Internet. Un tel déploiement de bornes d'accès, appelées APs (Access Points) conduit au problème de l'allocation des 11 canaux radio définis dans la bande ISM (Industrial, Scientific & Medical) dont l'utilisation peut se faire sans licence. La norme 802.11b ne prévoit pas de système automatique de répartition de ces canaux. Ainsi, un tel système a été développé dans le cadre d'un projet de diplôme à l'école d'ingénieurs et d'architectes de Fribourg (EIA-FR) puis lors du projet KTI/CTI no 6546.1 grâce à la collaboration de Swisscom Innovations et de l'EPFL. Le système développé permet une répartition optimale des canaux radio. Le développement a abouti à une application distribuée et autonome permettant la gestion de ces canaux et pouvant fonctionner aussi bien dans le contexte d'opérateurs WLAN que dans celui d'une entreprise. Le système a été nommé **Resource Management Engine** (RME). L'objectif du RME est d'obtenir la meilleure qualité de service (QoS). Ainsi le RME optimise la répartition des canaux radio afin de minimiser les interférences pour assurer des débits aussi élevés que possible sur chaque AP. Le processus d'optimisation du RME est basé sur les informations disponibles dans les APs. Le protocole SNMP [4]-[5] *(Simple Network Management Protocol)* est utilisé pour mesurer les paramètres nécessaires aux processus d'optimisation. Le protocole SNMP est aussi utilisé pour configurer le canal radio de chaque AP. Le processus d'optimisation du RME a été mis en oeuvre en JAVA dans l'environnement flexible et évolutif que sont les agents logiciels ou *software agents* [6]. Les agents RME ont été testés dans un environnement de simulation développé à l'Université de Fribourg [9]. D'autres tests de performances sont en cours à l'EPFL. L'approche proposée a été testée puis mise en service sur le réseau WLAN de l'EIA-FR. Sur ce réseau de 16 APs, le RME adapte automatiquement la répartition des canaux radio. les principes impliqués dans le RME sont protégés par le brevet n° 03405356.1 [13]. Ce papier contient une brève description du RME et de ces tests.

Le problème d'allocation des fréquences WLAN

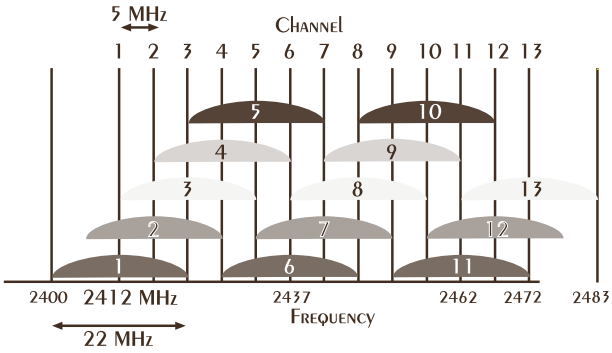


fig. 1 – spectre du WLAN

Les 83.5 MHz de la bande ISM utilisée par les équipements WLAN est partagée en 13 canaux se chevauchant selon la figure 1. Un canal WLAN pour le Wi-Fi /802.11b occupe une largeur de bande d'environ 22 MHz. Cette largeur de bande est utilisée pour transmettre des débits de 1, 2, 5.5 ou 11 Mb/s en utilisant une technique d'étalement du spectre (Direct Sequence Spread Spectrum). Comme l'indique la figure 1, seul les trois canaux 1,6 et 11 ne s'interfèrent pas parmi les 11 premiers canaux qui sont utilisables dans pratiquement le monde entier. Il est donc nécessaire de séparer d'au moins cinq canaux les APs dont les couvertures radio se superposent. Ainsi, les canaux 1, 6, et 11 sont les plus souvent utilisés. De plus, il est très difficile en pratique d'utiliser les autres canaux de manière efficace car les interférences dépendent entre autre des équipements (APs et clients) et du trafic.

Examinons un scénario concret comme celui décrit dans la figure 2 pour illustrer le problème de l'allocation des canaux Wi-Fi.

Admettons une allocation manuelle initiale sur les trois premiers APs : soit AP1, AP2 et AP3 avec les canaux 1, 11, et 6. Ainsi: freq(AP1)=1, freq(AP2)=11 et freq(AP3)=6. Cette solution permet d'offrir un maximum de QoS (Quality Of Service). Elle n'est pas unique mais a été choisie comme exemple. Considérons maintenant qu'un 4ème AP (AP4) est installé à l'image de la figure 2. Quel canal faut-il attribuer à AP4 pour obtenir un minimum d'interférences afin d'offrir un maximum de QoS ? Il est impossible d'attribuer un canal sans créer de perturbations. Mais en changeant l'allocation des fréquences sur AP2 et AP3, il est possible

de disposer d'un canal presque libre de toute perturbation car les couvertures des AP2 et AP4 ne se chevauchent que très peu. Ainsi, une nouvelle attribution sur les APs 2 et 3: freq(AP2)=6 et freq(AP3)=1 permet d'attribuer le canal 11 à l'AP4 en minimisant les interférences.

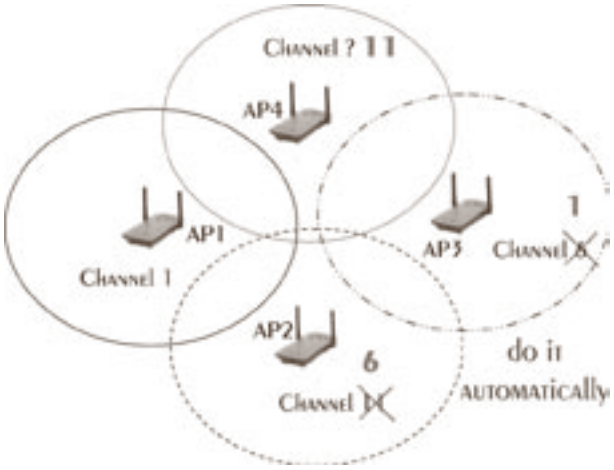


fig. 2 – illustration d'une solution au problème de la superposition des couvertures radio dans un exemple simple

En pratique, dans le réseau WLAN de l'EIA-FR décrit dans la figure 2 par exemple, les couvertures et les interférences sont beaucoup plus complexes et dépendent aussi de la charge de trafic sur chaque AP. Ainsi la répartition optimale des canaux peut être non seulement difficile à obtenir manuellement, mais elle varie dans le temps en fonction de la charge du réseau par les utilisateurs. C'est pourquoi le RME a été réalisé pour effectuer les allocations de canaux d'une manière adaptative, automatique et optimale. Une mise en oeuvre distribuée du RME a été choisie au lieu d'une solution centralisée afin de faciliter son utilisation sur un grand nombre d'APs. Le RME est décrit dans les sections suivantes en considérant sa mise en œuvre dans un réseau WLAN fonctionnel.

L'infrastructure de test pour le RME

La figure 3 décrit le réseau WLAN de l'EIA-FR et la mise en œuvre du RME dans cet environnement.

L'EIA-FR est composée de plusieurs bâtiments dont 4 sont équipés du WLAN pour un total de 16 APs. Tous les APs sont reliés sur le même sous réseau. D'un point de vu logique, chaque agent logiciel du RME gère un AP. Comme il s'agit d'un système distribué, le choix fut d'attribuer un PC par bâtiment. Chaque PC supporte l'environnement nécessaire aux agents logiciels [6]. En résumé, le RME se trouvent sur un sous-réseau interne à l'EIA-FR (VLAN30) et pilote le réseau WLAN (VLAN160) en utilisant le protocole SNMP.

La section suivante donne plus de détails sur le RME.

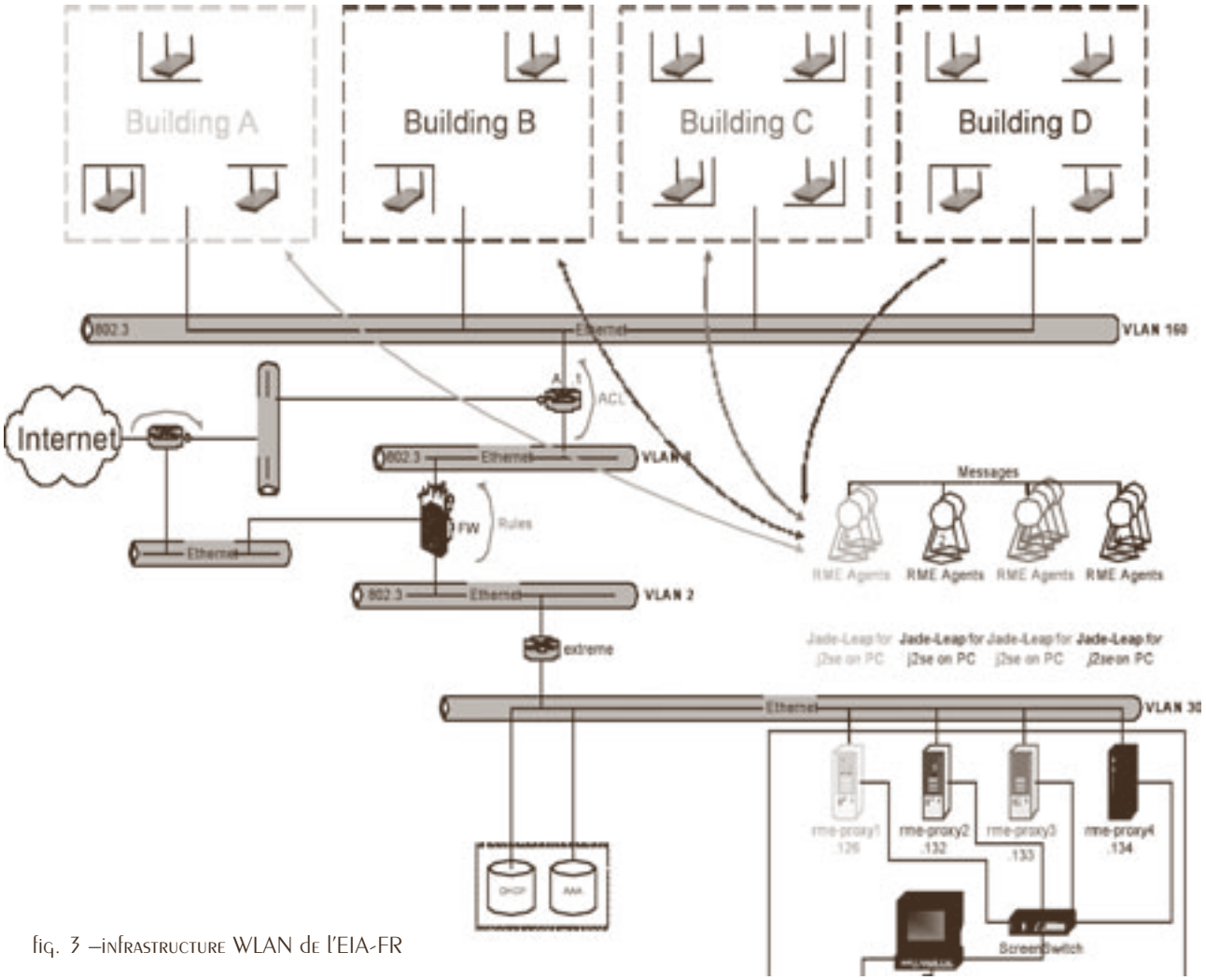


fig. 3 –infrastructure WLAN de l'EIA-FR

L'approche agent

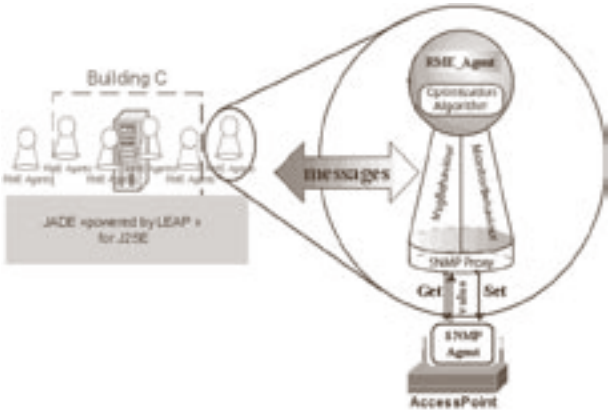


fig. 4 – l'agent RME

Le système RME est basé sur des agents logiciels afin d'assurer un déploiement simple quelle que soit l'échelle du réseau WLAN. La plate-forme logicielle pour les agents RME a été choisie sur la base d'expériences et de projets réalisés à Swisscom et à l'EIA-FR. Ainsi, le choix pour supporter les agents RME s'est dirigé vers JADE[1] [6]. Cette plate-forme est issue d'une organisation *open source* et écrite entièrement en JAVA. JADE est conforme au standard FIPA[2]. La plate-forme multi agents JADE dispose de plusieurs mécanismes pour l'échange de messages asynchrones entre agents. Classiquement, nous définissons un agent comme un logiciel exécutant des tâches spécifiques et possédant un degré d'intelligence qui lui permet de gérer ces tâches de manière autonome et d'interagir avec son environnement de façon appropriée. Les agents logiciels possèdent un ou plusieurs comportements (*Behaviours*) simultanés dont la concurrence est gérée grâce aux *JAVA Threads* dont JADE est issue. Les agents RME possèdent deux comportements exécutés en parallèles : le *MonitorBehaviour* et le *MsgBehaviour*. Le *MonitorBehaviour* lit continuellement les données de l'AP qu'il contrôle pour évaluer l'environnement dans lequel l'AP évolue.

Le *MsgBehaviour* lit les messages reçus des autres agents RME. Ces messages sont de deux types :

- *inform*: annonce de changements par un autre AP, ou
- *management*: pour la gestion des agents par la plate-forme JADE.

L'agent RME, grâce aux données fournies par ces deux comportements, détermine le canal le plus approprié suivant un algorithme d'optimisation et affecte ce canal à l'AP qu'il gère. Pour diminuer la place mémoire requise en vue d'une implémentation sur du matériel embarqué ou d'une intégration dans le progiciel de l'AP, la plate-forme JADE-LEAP[3] a été utilisée. JADE-LEAP offre un noyau qui a été adapté pour différents environnements [6]: J2SE pour des ordinateurs de bureau, des stations de travail ou certains systèmes embarqués (TINI [12] par exemple), J2ME-PJava[4] pour des systèmes plus limités comme des petits ordinateurs (PDA par exemple), et J2ME-MIDP/CLDC[5] pour d'autres systèmes embarqués (SNAP [11] par exemple avec modifications car il ne supporte pas MIDP) ou des téléphones mobiles (smartphone par exemple).

L'algorithme d'optimisation [13] et son paramétrage ne sont pas décrits ici afin de garder une vue d'ensemble du RME. Les concepts de bases de l'algorithme d'optimisation sont les fruits de discussions avec l'EPFL et Swisscom Innovations. Le développement de cet algorithme est la contribution principale de l'EPFL et de Sacha Varone en particulier. La première phase d'évaluations de l'algorithme d'optimisation sera terminée à fin 2003. Une mise en œuvre et certains paramétrages pratiques ont été réalisés sur la base de simulations, décrites dans la section suivante, et d'expériences réalisées à Swisscom Innovations, puis à l'EIA-FR.

Simulations du RME

Pour tester la mise en œuvre et la stabilité de l'algorithme d'optimisation[6], le Generic Network Management Tool (GNMT [9]) a été utilisé. Les interfaces conviviales du GNMT et son extension réalisée par Daniel Rossier (Swisscom Innovations) pour la couche du WLAN ont permis de rapidement procéder aux tests décrits brièvement ci-dessous (figure 5).

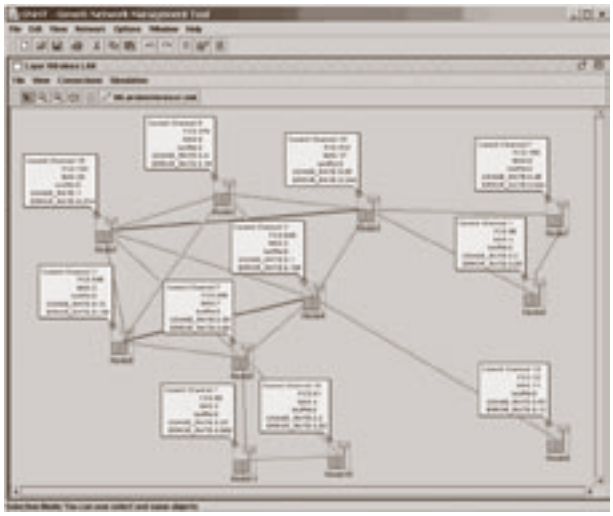


fig. 5 –simulation avec le GNMT (Generic Network Management Tool)

Dans la figure 6, les liens entre 2 nœuds (APs) du réseau représentent l'existence des interférences qu'il pourrait y avoir si les canaux de ces 2 APs étaient trop proches l'un de l'autre. La couleur du lien (niveau de gris dan les figs 5-10) indique le degré d'interférences entre les 2 APs. Chaque lien possède un poids, normalisé entre 0 et 1, qui définit le niveau de perturbations dû à la proximité géographique des 2 APs. Par exemple: si 2 APs sont en ligne de vue, le poids est de 1 mais si les APs sont séparés par un mur, le poids serait de 0.5. La mise en place des poids se réalise aisément pour les simulations grâce au GNMT.

1 JADE : Java Agent DEvelopment Framework for multi-agent systems (compliance with FIPA)
2 FIPA : Foundation for Intelligent & Physical Agents
3 LEAP : Lightweight Extensible Agent Platform
4 J2ME-Pjava : Java 2 Micro Edition for Personal Java
5 J2ME-MIDP/CLDC : Java 2 Micro Edition for Mobile Information Device Profile/Connected Limited Device Configuration
6 devisé par Sacha Varone et modifié par Frédéric Aviolat (EPFL) dans le cadre du projet CTI/KTI.

Le GNMT avec sa couche WLAN facilite aussi l'utilisation des agents logiciels et nous avons pu y intégrer les agents RME. Ainsi des tests fonctionnels ont pu être validés sur plusieurs réseaux WLAN simulés.

Une des limitations actuelles du GNMT est l'adaptation des données (MIBs)[8] lors de modifications des canaux radio par les agents du RME. Ces données sont accessibles en pratique grâce au protocole SNMP [4-5]mais ces valeurs sont simulées dans le GNMT. La section suivante décrit ces aspects de la gestion d'un réseau WLAN par le RME.

Le management de réseau

Le SNMP (Simple Network Management Protocol) est devenu le standard de facto pour la gestion des équipements sur réseau *IP*. Le SNMP se base sur le modèle client - serveur entre le manager, ici l'agent RME, et l'agent SNMP[7] qui se trouve dans l'AP. La terminologie *agent* est source de confusion mais c'est celle qui est officiellement utilisée. Les données lues par le *MonitorBehaviour* sont des informations contenues dans les objets d'une MIB[8] [7]-[8]. Les MIBs peuvent être considérées comme des bases de données, dans lesquelles les caractéristiques d'un équipement, ici un AP, sont stockées dans une structure en arbre.

Les deux opérations effectuées par l'agent RME sur la MIB de son AP sont le *GET* et le *SET*. L'opération *GET* permet à l'agent RME de récupérer une valeur contenue dans la base de données de l'AP. L'opération *SET* permet d'assigner un canal radio particulier. Dans ce dernier exemple, c'est l'élément *dot11CurrentChannel* de la MIB standard des équipements Wi-Fi (IEEE 802.11b) qui est utilisé. On remarquera la description quasi-intuitive de cet élément. Ce n'est malheureusement pas toujours aussi clair pour d'autres données nécessaires au fonctionnement du RME. Ainsi des adaptations doivent être réalisées pour configurer un agent RME aux spécificités d'un constructeur ou d'un type d'AP particulier.

Le Resource Management Engine (RME)

Les sections précédentes ont décrit le RME. Un agent RME, représenté dans la figure 4, comporte 3 parties principales (voir la section **L'approche agent** en page 11 pour les définitions) :

- le *MonitorBehaviour*,
- le *MsgBehaviour*, et
- l'algorithme d'optimisation.

Le système RME a été testé en simulation. Les résultats étant satisfaisants, une mise en pratique dans le réseau WLAN de l'EIA-FR a été réalisée. Les sections suivantes décrivent cette réalisation.

7 Agent SNMP : progiciel mis en oeuvre par les constructeurs d'équipements réseaux pour la gestion à distance de ces équipements.

8 MIB : Management Information Base

Description du réseau WLAN EIA-FR pour les tests du RME

La figure 6 présente précisément les 16 APs du réseau WLAN de l'EIA-FR, la répartition de ces APs dans les bâtiments nommés A, B, C et D et les différents étages (axe vertical). Dans le bâtiment A, il y a 4 APs, 2 dans le B, 6 dans le C et 4 dans le D. Dans la figure 6, chaque nœud (*Node* ou AP) indique son canal (*Current Channel*), le nombre de stations associées (*NAS*) et l'activité de l'AP (*Activity*). L'activité de l'AP a été définie par une fonction tenant compte du taux d'erreurs, du taux d'utilisation et du nombre de stations associées.

La visualisation des résultats pratiques du RME représentée dans la figure 6 a été accomplie en modifiant l'interface graphique du GNMT ce qui explique la similarité avec la figure 5 qui décrit une simulation.

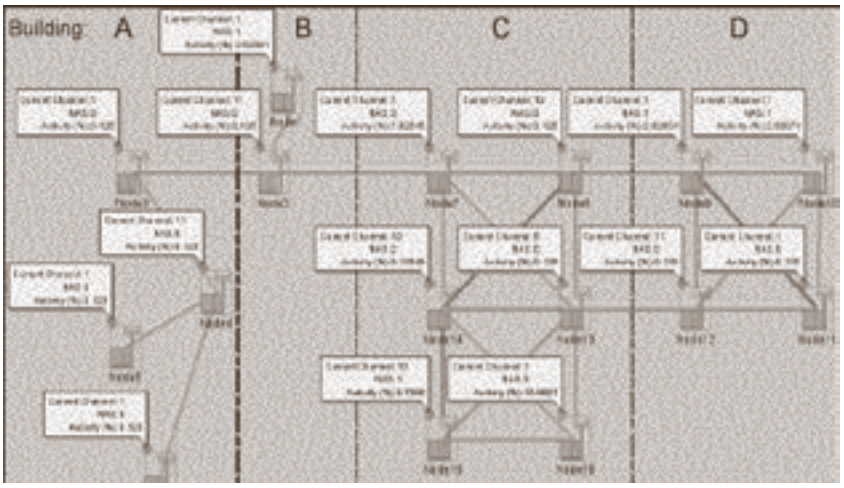


fig. 6 –visualisation du réseau WLAN de l'EIA-FR et des liens d'interférence entre APs

Afin de démontrer le bon fonctionnement du RME, nous avons documenté les tests suivants :

Démonstration : initialisation

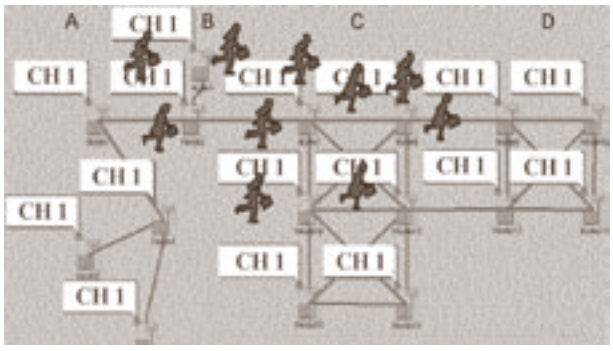


fig. 7– état initial du réseau WLAN

Grâce à une commande de gestion spéciale du RME, les canaux des APs sont tous initialisés avec le canal 1 et les changements de canaux sont inhibés. Cet état permet aux agents RME de mettre à jour leurs données qui varient en fonction du voisinage de chaque AP, mais interdit toute modification des canaux. Le réseau WLAN est fonctionnel mais de nombreuses interférences diminuent l'efficacité. Une

mesure de débit sur 2 PC portables associés à 2 APs différents (reliés par un lien d'interférence) donne par exemple 1 et 2 Mbps.

Le processus d'optimisation est ensuite libéré. Ce processus entraîne des modifications dans l'attribution des canaux. Après quelques dizaines de secondes un état stable est obtenu, lequel est visualisé dans la figure 8. L'optimisation du RME permet, par exemple, d'augmenter à 4 et 5.5 Mbps les débits mesurés ci-dessus. La configuration de la figure 8 dépend de la charge du réseau et, d'une manière aléatoire, de l'agent qui a commencé l'optimisation. Cet état est optimal mais n'est pas unique. En effet, plusieurs configurations optimales sont possibles comme dans le cas des 4 APs de la figure 2. D'autre part, la répartition optimale dépend de la charge et du trafic sur chaque AP. Ainsi une autre répartition optimale est obtenue une heure après, comme le montre la figure 9.

Démonstration : utilisateurs nomades

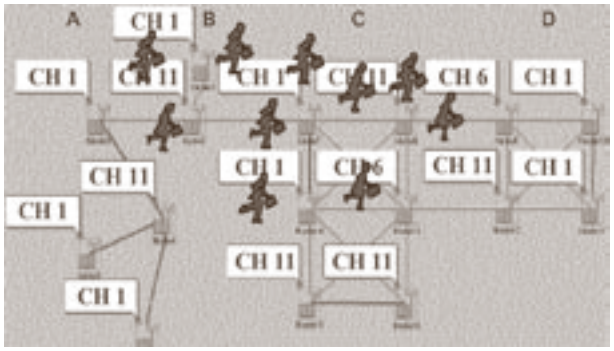


fig. 8– état stable (à 9H00)

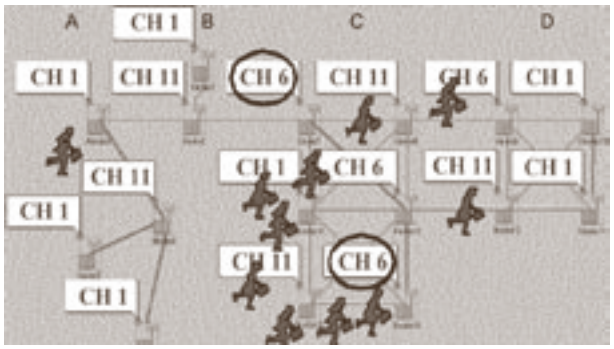


fig. 9– état stable (à 10H00)

Comme exemple, analysons le bâtiment C, qui offre une vue concrète de la distribution des fréquences en fonction de la charge. Les deux APs de l'étage inférieur du bâtiment C (en bas dans les figures 8 et 9) ont obtenus le canal 11 (figure 8) car ils n'ont pas encore de stations associées alors que les autres APs obtiennent des canaux espacés les uns des autres là où il y a le plus de charge (voir les canaux 1, 6 et 11).

La figure 9 reflète l'état du réseau une heure plus tard, alors que les personnes se sont déplacées vers les étages inférieurs.

Ainsi, à 10h, les deux APs de l'étage inférieur (qui, à 9h00, avaient le canal 11) ont dû *s'éloigner l'un de l'autre* pour diminuer leurs interférences mutuelles et offrir une meilleure bande passante. Les cercles indiquent les changements et la valeur obtenue par l'algorithme d'optimisation. Par rapport à une configuration statique, le RME permet une adaptation aux conditions de charge du réseau WLAN.

Les mesures ont montré qu'un utilisateur ne s'aperçoit pas des changements de canaux des APs, en particulier si la personne utilise Windows 2000 ou XP et que les APs permettent de commuter d'une fréquence à une autre en quelques millisecondes comme c'est le cas pour les APs *Cisco Aironet 1100*.

Démonstration: opérateur concurrent

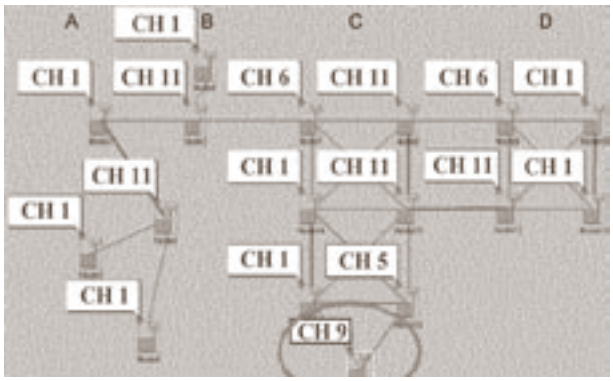


fig. 10 – un opérateur concurrent se place à proximité de notre réseau WLAN

Une autre illustration de l'avantage du RME dans un réseau WLAN est la prise en compte d'un opérateur externe ou concurrent venant perturber le réseau WLAN sous contrôle de RME. Considérons par exemple qu'un AP concurrent avec le canal 9 (voir AP encerclé dans la figure 10) est installé près des deux APs de l'étage inférieur. Cet AP concurrent n'a pas d'agent RME qui puisse le contrôler. Le problème de la découverte automatique d'un tel AP (concurrent ou non) n'étant pas encore résolu dans le projet, ce nouvel AP a été annoncé au réseau WLAN de l'EIA-FR par le biais du GNMT. Dès lors, une reconfiguration des canaux sur les deux APs interférés a pu s'opérer. La situation de la figure 10 présente le résultat de l'adaptation par le RME. L'AP qui avait le canal 11 a pris le canal 1 et l'autre AP est passé au canal 5. Les APs contrôlés par les agents RME se sont reconfigurés pour éviter les perturbations provoquées par l'AP concurrent. A noter que les liens d'interférences entre l'AP concurrent et les APs contrôlés par le RME ont été définis avec le poids maximal de 1 étant donné l'ignorance du degré de la perturbation. Ce dernier exemple montre l'avantage du RME dans le cas d'interférences non contrôlables. Actuellement, l'annonce manuelle des APs concurrents reste un inconvénient.

Conclusions

La faisabilité d'un système distribué et autonome permettant une répartition optimale et adaptée aux conditions de trafic et d'interférences dans un réseau WLAN a été démontrée. Le système appelé Resource Management Engine (RME) a été développé en JAVA sur une plate-forme distribuée d'agents logiciels JADE-LEAP.

L'efficacité des agents logiciels RME est établie par l'adaptation automatique à la charge du réseau WLAN,

par la stabilité obtenue suite au processus d'optimisation, par la capacité de prendre en compte un AP concurrent et par la diminution observable des interférences. Des mesures de débit utile réalisées avec le scénario de l'AP concurrent montre une augmentation d'un facteur 5 pour les débits obtenus grâce au RME[9].

Au vu des expériences accumulées dans ce projet, deux améliorations ont été identifiées. La première amélioration, indispensable pour le gestionnaire d'un réseau WLAN, concerne la supervision des agents et leurs déploiements. La deuxième amélioration, concerne la découverte automatique du voisinage par les agents RME afin de réduire encore toute intervention manuelle.

fig. 11 – Le démonstrateur RME pour le WLAN de l 'EIA-FR

Remerciements

Les auteurs n'auraient pas pu accomplir le système présenté ici sans les contributions de :

- Daniel Rossier, chef du projet RME à Swisscom Innovations.
- François Buntschu, collaborateur scientifique EIA-FR, et WLAN manager.
- Fiorenzo Gamba, collaborateur scientifique EIA-FR, pour son suivi lors du projet de diplôme.

D'autre part les contributions d'Eric Demierre, Mohamed Mokdad, Ferran Moreno Blanca, et Sacha Varone (Swisscom Innovations), de Roger Lagadec (Swisscom Mobile) et récemment, de Frédéric Aviolat (EPFL) ont été fortement appréciées.

Références

[1] Standard pour réseau sans fil : 802.11, Daniel Trezentos, Ecole nationale supérieure des Télécommunications de Bretagne, ***http://www.techniques-ingenieur.fr/affichage/DispIntro.asp?nGcmId=TE7375***

[2] A Technical Tutorial on the IEEE 802.11 Protocol, Pablo Brenner, Breezecom Wireless Communications, ***http://www.sss-mag.com/pdf/802_11tut.pdf***

[3] IEEE Std 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, including ieee802.11-mib, edition 1999 (***http://ieee802.org/11/***)

[4] Architecture SNMP, mémoire de Laurent Frank, Laurent Frank, Université libre de Bruxelles, 1998, ***http://www.f4dwu.net/download/memoire2.pdf***

[5] RFC 1157, Simple Network Management Protocol (SNMP), May 1990

[6] Jade-LEAP (3.0b1, 19th March 2003), ***http://www.jade.cselt.it***, Fabio Bellifemine, Giovanni Caire, Tiziana Trucco, TILab S.p.A., Giovanni Rimassa, Università di Parma

[7] RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II

[8] Cisco Systems, ***http://www.cisco.com***

[9] A Description of the Generic Network Management Tool (GNMT), Daniel Rossier, Université de Fribourg et Swisscom Innovations, ***http://diuf.unifr.ch/pai/publications/2002/technical_report/ros_1002.pdf***

[10] NLANR/DAST Projects, Ajay Tirumala, Feng Qin, Jon Dugan, Jim Ferguson, Kevin Gibbs, version 1.7.0, March 2003, ***http://dast.nlanr.net/Projects/Iperf/***

[11] SNAP (Simple Network Application Platform), ***http://www.imsys.se*** , IMSYS AB, Sweden

[12] TINI(TinyInterNetInterface),***http://www.ibutton.com/TINI/*** , Dallas Semiconductor Corporation, Tex

[13] Brevet Nr. 03405356.1, System für die dynamische Zuweisung von Trägerfrequenzen zu Zugriffspunkten eines lokalen Funknetzes, Daniel Rossier, Sacha Varone, Swisscom Innovations, Jean-Frédéric Wagen, Vincenzo Inguscio, Eric Marchon, Fiorenzo Gamba, Ecole d'ingénieurs et d'architectes de Fribourg. ■

9 Mesure de référence: tous les canaux à 1 et le canal 2 pour l'AP concurrent. Mesure avec RME : voir figure 10. Les mesures de la bande passante sur TCP/IP ont été réalisées avec les logiciels « IPERF » [10].

Programme des cours

organisés par le Domaine IT de l'EPFL

Ces cours sont ouverts à tous, membres ou non de l'EPFL.
Pour le personnel de l'EPFL, le DIT se charge des frais de cours.
Les descriptifs des cours sont sur Internet: ***http://dit.epfl.ch/formation***

Renseignements
(les matins des lu, me & ve)
Daniele.Gonzalez@epfl.ch
✆ 021/69 353 14
Fax: 021/69 322 20

Renseignements
(tous les matins)
Josiane.Scalfo@epfl.ch
✆ 021/69 322 44
Fax: 021/69 322 20

CONDITIONS D'INSCRIPTION

En cas d'empêchement à suivre le(s) cours, l'élève avertira le Domaine IT au minimum une semaine à l'avance (sauf cas exceptionnel), faute de quoi le DIT se réserve le droit de facturer à son unité les frais occasionnés pour le cours.

Une confirmation parviendra à l'élève environ deux semaines avant le(s) cours. S'il est déjà complet, l'élève sera informé de suite et son nom placé en liste d'attente. Dès qu'un cours identique sera fixé, il recevra un nouveau formulaire d'inscription.

Le DIT se réserve le droit d'annuler un cours si le nombre minimum de 4 participants n'est pas atteint ou pour des raisons indépendantes de sa volonté. Aucune compensation ne sera due par le DIT.

INTRODUCTION AU POSTE DE TRAVAIL

OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
Mac	Internet & Entourage	04-0086	1	12.02.2004	08:30 - 12:00
Win	Internet & Outlook express	04-0095	1	09.02.2004	13:30 - 17:00
Mac	Macintosh, le système X	04-0084	1	03.02.2004	13:30 - 17:00
Mac	Macintosh, le système X	04-0085	1	23.03.2004	08:30 - 12:00
Win	Windows XP, votre machine en pratique	04-0087	1	02.02.2004	13:30 - 17:00
Win	Windows XP, votre machine en pratique	04-0088	1	11.03.2004	08:30 - 12:00

ACQUISITION ET TRAITEMENT DE DONNÉES

	OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
	Win	LabVIEW Basics 1	04-0009	6	16 au 18.02.2004	08:30 - 17:00
	Win	LabVIEW Basics 1	04-0011	6	15 au 17.03.2004	08:30 - 17:00
	Win	LabVIEW Basics 2	04-0010	4	19 & 20.02.2004	08:30 - 17:00
	Win	LabVIEW DAQ	04-0013	6	05 au 07.04.2004	08:30 - 17:00
Nouveau	Win	LabVIEW Intermediate 2	04-0023	4	24 & 25.06.2004	08:30 - 17:00
	Win	LabVIEW Real-Time	04-0012	4	18 & 19.03.2004	08:30 - 17:00
	Win	LabVIEW Vision IMAQ	04-0017	4	22 & 23.04.2004	08:30 - 17:00

BASE DE DONNÉES

OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
Win	Access, 1-introduction	04-0098	4	27.01, 03, 10 & 12.2.2004	08:30 - 12:00
Win	Access, 2-avancé	04-0099	4	16, 23, 25 & 30.03.2004	08:30 - 12:00
Win	FileMaker Pro, 1-introduction	04-0060	1	20.01.2004	08:30 - 12:00
Mac	FileMaker Pro, 1-introduction	04-0061	1	05.02.2004	13:30 - 17:00
Win	FileMaker Pro, 2-perfect.: modèles	04-0062	1	10.02.2004	13:30 - 17:00
Win	FileMaker Pro, 3-perfect.: liste de valeurs et options	04-0063	1	12.02.2004	13:30 - 17:00
Win	FileMaker Pro, 4-perfect.: scripts et boutons	04-0064	1	17.02.2004	13:30 - 17:00
Win	FileMaker Pro, 5-avancé : développement d'une base de données	04-0065	3	02, 04 & 09.03.2004	08:30 - 12:00

DESSIN - IMAGE

OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
Mac	Illustrator, introduction	04-0081	2	26 & 28.01.2004	13:30 - 17:00
Win	Illustrator, introduction	04-0082	2	02 & 04.03.2004	13:30 - 17:00
Win	Illustrator, niveau avancé	04-0083	2	15 & 17.03.2004	08:30 - 12:00
Win	PhotoShop: saisie, retouche, impression	04-0100	4	27, 28.01, 03 & 04.02.2004	13:30 - 17:00
Mac	PhotoShop: saisie, retouche, impression	04-0101	4	08, 10, 15 & 17.03.2004	13:30 - 17:00

ÉDITION

OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
Mac	FrameMaker, 1-mise en forme	04-0053	3	27, 29.01 & 03.02.2004	08:30 - 12:00
Win	FrameMaker, 1-mise en forme	04-0055	3	09, 11 & 16.03.2004	13:30 - 17:00
Mac	FrameMaker, 2-livre et EndNote	04-0054	1	10.02.2004	08:30 - 12:00
Win	FrameMaker, 2-livre et EndNote	04-0056	1	23.03.2004	13:30 - 17:00
Mac	In-Design	04-0079	3	26, 28.01 & 02.02.2004	08:30 - 12:00
Mac	In-Design	04-0080	3	30.03, 01 & 06.04.2004	13:30 - 17:00
Mac	Word, gestion des automatismes	04-0069	1	27.01.2004	13:30 - 17:00
Win	Word, gestion des automatismes	04-0074	1	16.02.2004	08:30 - 12:00
Win	Word, gestion des automatismes	04-0093	1	29.03.2004	08:30 - 12:00
Mac	Word, images et colonnes	04-0068	1	22.01.2004	13:30 - 17:00
Win	Word, images et colonnes	04-0073	1	11.02.2004	08:30 - 12:00
Win	Word, images et colonnes	04-0078	1	24.03.2004	08:30 - 12:00
Mac	Word, mise en forme et styles	04-0066	2	13 & 15.01.2004	13:30 - 17:00
Win	Word, mise en forme et styles	04-0071	2	02 & 04.02.2004	08:30 - 12:00
Win	Word, mise en forme et styles	04-0076	2	15 & 18.03.2004	13:30 - 17:00
Mac	Word, modèles et publipostage (mailing)	04-0070	1	29.01.2004	13:30 - 17:00
Win	Word, modèles et publipostage (mailing)	04-0075	1	18.02.2004	08:30 - 12:00
Win	Word, modèles et publipostage (mailing)	04-0094	1	31.03.2004	08:30 - 12:00
Mac	Word, tableaux	04-0067	1	20.01.2004	13:30 - 17:00
Win	Word, tableaux	04-0072	1	09.02.2004	08:30 - 12:00
Win	Word, tableaux	04-0077	1	22.03.2004	08:30 - 12:00

OUTLOOK

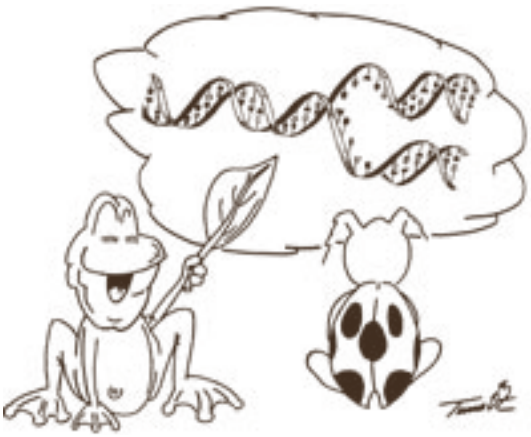
	OS	Nom du cours	N°	1/2 jour(s)	Date(s)	Horaire
	Win	Outlook XP	04-0048	2	19 & 23.01.2004	08:30 - 12:00
	Win	Outlook XP	04-0049	2	03 & 05.03.2004	08:30 - 12:00

PRÉSENTATION

	OS	Nom du cours	N°	1/2 jour(s)	Date(s)	Horaire
	Win	PowerPoint, les présentations	04-0050	2	19 & 22.01.2004	13:30 - 17:00
	Mac	PowerPoint, les présentations	04-0051	2	16 & 20.02.2004	08:30 - 12:00
	Win	PowerPoint, les présentations	04-0052	2	22 & 24.03.2004	13:30 - 17:00

PROGRAMMATION

	OS	Nom du cours	N°	1/2 jour(s)	Date(s)	Horaire
Nouveau	Win	Développement d'Applications Web avec J2EE	04-0109	4	25 & 26.03.2004	08:30 - 17:00
Nouveau	Win	Développement d'Enterprise JavaBeans (EJB) avec J2EE	04-0107	6	15 au 17.03.2004	08:30 - 17:00
	Win	Java	04-0106	10	08 au 12.03.2004	08:30 - 17:00
	Win	Langage C	04-0103	10	09 au 13.02.2004	08:30 - 17:00
	Linux	MPI, Introduction à la programmation parallèle	04-0026	8	19 au 22.01.2004	08:30 - 17:00
	Win	PHP	04-0104	6	16 au 18.02.2004	08:30 - 17:00
	Win	SQL - My SQL	04-0105	4	19 & 20.02.2004	08:30 - 17:00
	Win	XML et technologies associées	04-0108	6	22 au 24.03.2004	08:30 - 17:00



SYSTÈME

	OS	Nom du cours	N°	1/2 jour(s)	Date(s)	Horaire
	Linux	Linux, administration et réseau	04-0102	8	26 au 29.01.2004	08:30 - 17:00
	Linux	Linux, débutant	04-0111	6	02 au 04.02.2004	08:30 - 17:00
Nouveau	Win	Windows 2003, administration et maintenance d'une infrastructure réseau	04-0030	8	26 au 29.01.2004	08:30 - 17:00
Nouveau	Win	Windows 2003, administration, droits d'accès et ressources	04-0033	8	02 au 05.03.2004	08:30 - 17:00
Nouveau	Win	Windows 2003, implémentation de Windows Server 2003 Active Directory	04-0032	8	24 au 27.02.2004	08:30 - 17:00
Nouveau	Win	Windows 2003, implémentation de Windows Server 2003 Active Directory	04-0035	8	29.03 au 01.04.2004	08:30 - 17:00
Nouveau	Win	Windows 2003, maintenance et gestion	04-0034	4	23 & 24.03.2004	08:30 - 17:00
Nouveau	Win	Windows 2003, Upgrade Windows serveur 2000 à Windows serveur 2003	04-0031	10	02 au 06.02.2004	08:30 - 17:00
Nouveau	Win	Windows XP Pro, déploiement	04-0029	4	13 & 14.01.2004	08:30 - 17:00

TABLEUR

OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
Win	Excel, 1-introduction	04-0044	1	21.01.2004	08:30 - 12:00
Win	Excel, 2-feuille de calcul	04-0042	3	29, 30.01 & 05.02.2004	08:30 - 12:00
Mac	Excel, 2-feuille de calcul	04-0046	3	16, 18 & 23.03.2004	13:30 - 17:00
Win	Excel, base de données	04-0045	2	24 & 26.02.2004	13:30 - 17:00
Win	Excel, graphiques	04-0043	1	06.02.2004	08:30 - 12:00
Mac	Excel, graphiques	04-0047	1	25.03.2004	13:30 - 17:00

WWW - WEB

OS	*Nom du cours*	*N°*	*1/2 jour(s)*	*Date(s)*	*Horaire*
Mac	Dreamweaver, 1ère partie	04-0037	2	15 & 16.01.2004	08:30 - 12:00
Win	Dreamweaver, 1ère partie	04-0039	2	17 & 19.02.2004	08:30 - 12:00
Mac	Dreamweaver, 2ème partie	04-0038	2	22 & 23.01.2004	08:30 - 12:00
Win	Dreamweaver, 2ème partie	04-0040	2	24 & 26.02.2004	08:30 - 12:00
Win	Dreamweaver, avancé	04-0041	2	18 & 19.03.2004	08:30 - 12:00
Mac	Flash, 1ère partie	04-0057	3	10, 12 & 17.02.2004	13:30 - 17:00
Mac	Flash, 2ème partie	04-0058	2	02 & 04.03.2004	13:30 - 17:00
Mac	Flash, programmation	04-0059	4	16, 17, 25 & 30.03.2004	08:30 - 12:00
Mac	Jahia : création de sites web EPFL	04-0089	1	14.01.2004	08:30 - 12:00
Win	Jahia : création de sites web EPFL	04-0090	1	05.02.2004	13:30 - 17:00
Win	Jahia : création de sites web EPFL	04-0091	1	23.02.2004	08:30 - 12:00
Win	Jahia : création de sites web EPFL	04-0092	1	17.03.2004	13:30 - 17:00

INSCRIPTION POUR LES COURS ORGANISÉS PAR LE DIT

A retourner à Josiane Scalfo ou à Danièle Gonzalez, DIT-EPFL, CP 121, 1015 Lausanne

Je, soussigné(e) Nom: _____ Prénom: _____

Tél.: _____ E-Mail: _____ Fonction: _____

Institut: _____ Faculté: _____

Adresse: _____

m'engage à suivre le(s) cours dans son (leur) intégralité et à respecter l'horaire selon les conditions d'inscription:

Nom du cours N° du cours N° cours de remplacement Date du cours

_____

Date: Signature:

_____

Autorisation du chef hiérarchique: nom lisible: Signature:

_____

Intérêt et souhait pour d'autres cours

Description ou titre des cours que je souhaite voir organiser par le DIT:

_____

_____

AFS Login pour Mac OS X

Jacques.Menu@epfl.ch, Domaine IT

Cette mini-application bilingue français-anglais a été écrite pour permettre aux utilisateurs de Mac OS X d'accéder à leur dossier hébergé sur les serveurs OpenAFS de l'Ecole.

Elle ne fait que fournir une interface graphique devant les commandes **klog**, **unlog** et **tokens** dont on dispose par ailleurs depuis une fenêtre de Terminal lorsque le client OpenAFS est installé.

Figure 1 : fenêtre d'AFS Login, en version française

AFS Login consiste en une interface graphique composée d'une simple fenêtre, illustrée à la figure 1, dans laquelle on peut :

- fournir son nom d'utilisateur OpenAFS et le mot de passe associé;
- effectuer un login pour s'authentifier, ce qui donne un jeton (token) et l'accès à son dossier en cas de succès;
- effectuer un logout AFS, ce qui fait que le ou les jeton(s) détenus sont perdus.

Le nom d'utilisateur proposé dans l'interface au lancement est celui de l'utilisateur courant, mais on peut bien sûr en utiliser un autre.

La fenêtre contient deux autres champs montrant respectivement le résultat de la dernière authentification et les jetons AFS obtenus suite à un login réussi, ainsi que les informations nécessaires à l'emploi de l'application.

La figure 2 montre le dossier OpenAFS tel qu'il est visible après un login réussi. On a tiré l'icône du dossier /afs/j/jmenu en bas à gauche de la fenêtre pour l'avoir toujours à disposition dans les dialogues d'ouverture de fichiers.

Figure 2 : montage réussi du dossier utilisateur OpenAFS

La page ***http://dit.epfl.ch/SE/AFS/AFS_client_install_mac.html*** décrit comment installer et configurer le client OpenAFS sur Mac OS X, et renvoie à ***http://dit.epfl.ch/SE/AFS/AFSLoginInstall.html*** qui indique où et comment installer AFS Login lui même.

Pour les esprits curieux, mentionnons que nous avons utilisé AppleScript pour écrire cette application, en nous inspirant d'un exemple fourni par Apple.

Toute suggestion d'amélioration est à transmettre directement au soussigné. ■

Prochaines parutions

	délai rédaction	parution
1	22.01.04	03.02.04
2	12.02.04	02.03.04
3	11.03.04	30.03.04
4	08.04.04	27.04.04
5	13.05.04	01.06.04
6	10.06.04	29.06.04
7	26.08.04	14.09.04
8	30.09.04	19.10.04
9	28.10.04	16.11.04
10	02.12.04	21.12.04

Sommaire FI 10/2003

Calendrier

LU	12.01.04	17^{15}	INM202	Séminaire I&C —Where is the «Net Economy» going ? Technologies and Markets at the Dawn of the XXI century par Prof. Dominico Ferrari
MA	**20.01.04**	**08^{30}**	**Polydôme EPFL**	**Journée de présentation de la technologie DSP (lire en page 8)**
ME	28.01.04	08^{45}	Salle Polyvalente DIT	**Comité de rédaction du FI** J. Dousson, +41 21 69 32246, courriel: Jacqueline.Dousson@epfl.ch
JE	29.01.04	14^{00}	Salle Wavre	DIS – **Direction informatique stratégique** J.-Cl. Berney, +41 21 69 32590, courriel: jean-claude.berney@epfl.ch
MA	24.02.04	08^{45}	Salle Polyvalente DIT	**Comité de rédaction du FI** J. Dousson, +41 21 69 32246, courriel: Jacqueline.Dousson@epfl.ch
ME	24.03.04	08^{45}	Salle Polyvalente DIT	**Comité de rédaction du FI**

ISSN 1420-7192