VIMINAL (*)

VIrtual Model for Ip Network Architecture Lab

Maquette virtuelle de travaux pratiques pour architectures de réseaux IP

Jacques Landru, Jean-Philippe Vandeborre
GET / INT / ENIC Telecom Lille 1
{landru, vandeborre} @enic.fr

Mots cléfs :

maquette virtuelle de TP réseaux, LiveCD, virtualisation, zéro installation, maquettage réseau, labo réseau virtuel.

Résumé :

La montée en puissance continue des ordinateurs (loi de Moore), associée au développement de diverses méthodes de virtualisation de systèmes, permet aujourd'hui d'envisager la mise en œuvre de plate-formes et de maquettes virtuelles de systèmes réseaux sur de simples postes de travail. VIMINAL expérimente le maquettage par virtualisation tout en réduisant les contraintes de déploiement. L'objectif est de mettre à disposition des étudiants, des environnements systèmes et réseaux relativement complets sur lesquels ils puissent agir avec des droits étendus sans remettre en cause les protections que les équipes systèmes et réseaux ont déployées pour assurer la stabilité des machines des salles de travaux pratiques (TP). L'arrivée de systèmes auto-configurables disponibles grâce à la banalisation des CD auto-bootables (LiveCD) permet d'utiliser les ressources banalisées des salles informatiques pour des séances spécifiques de TP, tout en restituant les machines dans l'état dans lequel elles étaient avant de débuter la séance de travaux pratiques.*

1 Introduction

Le syndrome Iznogoud : ce populaire personnage de bande dessinée, qui « veut être Calife à la place du Calife », symbolise une frange importante de la population étudiante qui fréquente les salles de TP informatiques. Les tentatives de contournement des protections, patiemment élaborées par les équipes systèmes et réseaux, pour « être super-utilisateur à la place du super-utilisateur » sont en effet devenues un sport national dans nos environnements informatiques pédagogiques. La tâche des administrateurs, pour conserver un parc homogène et stable de machines tout en assurant à chaque enseignant qu'il disposera bien des environnements et outils spécifiques pour ses séances de travaux pratiques, est un véritable défi. Dans le domaine de l'enseignement des systèmes et réseaux, la tâche devient particulièrement ardue. En effet, pour ce type de travaux pratiques il y a, bien souvent, besoin d'accorder aux étudiants des droits étendus sur les plate-formes. Les outils sensibles, comme les analyseurs de protocoles, tels Tcpdump [1] ou Ethereal [2], nécessitent des droits super-utilisateurs. Activer ces droits, spécifiquement sur ces outils, avant chaque séance de TP, alourdit le travail des administrateurs. L'oubli de l'inactivation de ces droits spécifiques à l'issue des séances de TP peut également devenir problématique.

L'approche laboratoire dédié couramment mise en œuvre dans les disciplines nécessitant un accès réel aux équipements (biologie, électronique, mécanique, etc.) offre l'avantage de mettre les étudiants en situation réelle. Le domaine des réseaux, ne fait pas exception, le fait de manipuler concrètement les équipements demeure nécessaire. Toutefois les labos dédiés ont des limites :

- au niveau économique : coût des équipements, immobilisation de l'espace des ateliers et des matériels pour une utilisation limitée dans le temps ;
- au niveau de la gestion : l'enseignant et les personnels techniques qualifiés doivent s'assurer de l'état opérationnel de l'ensemble des équipements avant chaque séance de travail, ce qui, avec la multiplication des groupes, peut devenir lourd ;

*VIMINAL : La colline Viminal (Latin : Collis Viminalis,, Italien : Viminale) est la plus petite des sept collines sur lesquelles fut construite la ville antique de Rome. Elle doit son nom aux saules osier (vimen) qui y poussaient originellement.

http://en.wikipedia.org/wiki/Viminal
http://penelope.uchicago.edu/Thayer/E/Gazetteer/Places/Europe/Italy/Lazio/Roma/Rome/_Texts/PLATOP*/Viminalis.html

- dans le domaine des réseaux, chaque binôme d'étudiants ne travaille, à un moment donné, que sur une position de travail limitée, composée de quelques équipements. Il n'a pas la possibilité de gérer ou d'administrer une architecture complète, il lui manque bien souvent la vision d'ensemble ;
- l'alternative aux laboratoires réels peut être la simulation. Les possibilités de la simulation sont importantes. Bien que la manipulation concrète des équipements soit absente, les outils disposent en général d'interfaces évoluées et d'outils annexes qui permettent de monter des plate-formes pédagogiques vraiment intéressantes. Toutefois les environnements de simulation sont dans bien des cas lourds et difficiles à appréhender dans un contexte purement pédagogique. Ils peuvent également s'avérer sur-dimensionnés pour bien des travaux pratiques. Dans le domaine des réseaux, la plate-forme *Opnet* d'OPNET Technologies, Inc. [3], offrant des fonctionnalités très étendues, fait office de référence. Son coût et sa complexité peuvent rebuter bien des enseignants à l'utiliser pour leurs séances de travaux pratiques et les administrateurs système à la mettre en place.

Dans cet article, nous présentons une voie intermédiaire, basée sur la virtualisation des systèmes associée aux environnements auto-configurables que constituent les *LiveCD*. L'objectif initial est de pouvoir réaliser les TP systèmes et réseaux dans les salles informatiques banalisées en minimisant l'impact sur les configurations de ces dernières. Cette approche a été étudiée dans un contexte de pédagogie des systèmes et des réseaux. Elle peut également être mise en œuvre pour l'expérimentation, lors des périodes de projets où chaque groupe ou binôme d'étudiants nécessite sa propre plate-forme. Elle permet la mise à disposition des maquettes d'environnements informatiques qui ne nécessitent pas d'équipements ou de dispositifs matériels dédiés. Ces projets peuvent dès lors se dérouler dans les salles informatiques banalisées.

Après une introduction des systèmes GNU/Linux auto-configurables dits *LiveCD*, nous abordons la virtualisation des systèmes et plus spécifiquement User-Mode Linux qui est la technique de virtualisation sur laquelle s'appuie Virtual Network User-Mode Linux (VNUML). Le projet VIMINAL intègre les contraintes systèmes de ces différents environnements pour constituer une plate-forme homogène et autonome. Nous présentons ensuite les choix qui ont été faits par le *LiveCD* VIMINAL. Enfin, les limitations de notre système et ses évolutions futures sont décrites avant de conclure.

2 Environnements systèmes auto-configurables : *LiveCD*

Le succès des distributions auto-configurables embarquées sur un CDrom, dites *LiveCD*, participe à la popularisation du système GNU/Linux. Le fait de pouvoir démarrer un système depuis un CDrom sans se soucier de sa configuration matérielle, ni même de ce qui est déjà installé sur le disque de la machine ouvre des perspectives intéressantes. Avec l'augmentation des capacités de stockage des clés USB, il devient possible d'emmener avec soi sa propre configuration pour l'utiliser sur des machines d'emprunt sans impacter la configuration de ces dernières. On laisse la machine dans l'état où on l'a trouvée avant d'introduire le CDrom ou la clé USB. Bien que n'étant pas le premier projet permettant d'utiliser un système GNU/Linux directement depuis un CDrom, le projet DémoLinux [4] avait déjà ouvert la voie, il faut bien reconnaître que le projet de Klaus Knopper, plus connu sous le vocable de Knoppix [5], a fait bien des émules et a fédéré tout un ensemble d'outils d'auto-configuration qui peuvent simplifier grandement la vie des administrateurs système. La plupart des grandes distributions disposent maintenant de leurs *LiveCD* facilitant l'installation, et on ne compte plus les kits et les boites à outils à copier sur des CDrom ou des clés USB pour venir au secours de machines dont le système est hors-service. En automatisant la détection du matériel, au démarrage du système d'exploitation, la dépendance au matériel est réduite. Il devient possible pour les configurations courantes de stations de travail, ne nécessitant pas d'extensions matérielles spécifiques ou exotiques, d'utiliser les postes banalisés des salles de TP informatique quand bien même le parc de celles ci serait hétérogène. De plus, l'ensemble du système et de sa configuration étant sur un système de fichiers en lecture seule, le CDrom, il est durci dans la mesure où un changement malheureux de configuration est neutralisé par un simple redémarrage. La stabilité et la maintenance des postes de travail s'en trouvent de fait améliorées. De même, la remise en état initial de la plate-forme de TP entre chaque groupe ne nécessite plus qu'un simple redémarrage des stations. L'usage courtois des salles TP permettant de laisser, après la séance de TP, la salle dans l'état où on l'a trouvée en entrant, devrait dès lors être facilité.

3 Virtualisation des systèmes

La virtualisation des systèmes n'est pas une notion nouvelle. IBM avec son système VM/CMS [6] l'a largement déployée à l'époque de l'informatique centralisée où les mainframes étaient dominants. Cette technique qui permet de faire tourner plusieurs systèmes, éventuellement différents, sur un seul matériel, a ces derniers mois pris une importance croissante dans l'actualité informatique. La réussite économique d'outils propriétaires tel que VMware [7], l'intégration du code User-Mode Linux [8] dans les dernières versions du noyau GNU/Linux, les constructeurs de processeurs qui envisagent de l'intégrer au coeur des prochaines générations de puces à savoir l'annonce d'Intel et de son projet Vanderpool/Silverdale [9] et la réplique d'AMD avec Pacifica [10], l'activité soutenue des projets libres ambitieux tels que XEN [11], Qemu [12], PearPC [13], Adeos [14], Bochs [15],Virtual-server [16],Vserver [17], colinux [18], etc. nous confirment l'intérêt que prend aujourd'hui la virtualisation informatique. Il ne s'agit pas ici de comparer les mérites des différentes approches, mais d'expérimenter l'usage de l'une d'entre elles dans un environnement pédagogique.

4 User-Mode Linux

Dans le cadre de VIMINAL, nous nous intéressons à GNU/Linux en mode utilisateur connu sous le terme de User-Mode Linux [8] et abusivement dénommé UML, qu'il ne faut pas confondre avec l'Unified Modeling Language utilisé en génie logiciel pour la modélisation objet. VIMINAL intégrant VNUML [19] s'appuie donc naturellement sur User-Mode Linux.

4.1 Principes de fonctionnement

User-Mode Linux permet de faire tourner le noyau GNU/Linux en mode utilisateur comme n'importe quel processus. Utilisé à l'origine à des fins de débogage pour les développements du noyau, il permet de faire tourner des systèmes GNU/Linux gigognes. Le développeur peut alors tester les versions instables, inspecter le code lors de l'exécution sans remettre en cause la stabilité de sa station de développement. Divers outils et optimisations ont ensuite été développés pour en faire un véritable environnement de virtualisation GNU/Linux. La machine virtuelle ainsi créée est vue comme un bac à sable (*sandbox*) étanche, dans lequel les événements logiciels à destination du matériel sont interceptés et contrôlés. Ainsi le dysfonctionnement de la machine virtuelle ne remet pas en cause la stabilité de la machine réelle. User-Mode Linux ne permet que « GNU/Linux sur GNU/Linux », contrairement à d'autres systèmes de virtualisation basés sur l'émulation de processeur (QEMU [12], PearPC [13], etc.) qui autorisent la virtualisation d'autres systèmes d'exploitation au dessus du système réel gérant les composants matériels. La notion de bac à sable introduite par ces mécanismes de virtualisation est une propriété intéressante pour nos environnements pédagogiques dans la mesure où elle autorise l'octroi des droits étendus du super-utilisateur sur la machine virtuelle tout en conservant des droit restreints sur la machine réelle. La stabilité de l'environnement de cette dernière s'en trouve dès lors améliorée.

4.2 *Root-fs* et fichiers *COW*

Chaque machine virtuelle dispose de son système de fichiers, contenant l'ensemble des fichiers de la distribution GNU/Linux propre à la machine virtuelle. Pour la machine réelle, c'est à dire l'hôte, ce système de fichiers de la machine virtuelle se présente sous la forme d'un simple fichier, couramment dénommé système de fichiers racine ou *root-fs* en anglais. Par commodité, nous utilisons cette dénomination anglo-saxonne dans la suite de cet article. Comme il contient un système de fichiers GNU/Linux complet, la taille du fichier *root-fs* d'une machine virtuelle peut être importante. User-Mode Linux permet à plusieurs machines virtuelles de se partager un *root-fs* commun en lecture seule. Les opérations d'écriture de chacune des machines virtuelles sont déportées dans des fichiers séparés propres à chaque machine virtuelle. Ces fichiers ne contenant que les différences avec le *root-fs*, sont dénommés fichiers *COW* (abréviation de Copy On Write). Ils sont liés au fichier *root-fs* et sont de taille modeste. L'utilisation des fichiers *COW* permet donc de personnaliser un ensemble de machines virtuelles, partageant une base système commune. Les machines virtuelles 1 et 2 de la Figure 1 disposent ainsi de leur propre système de fichiers ne contenant que les différences avec le système de fichier de référence qu'est le *root-fs*.

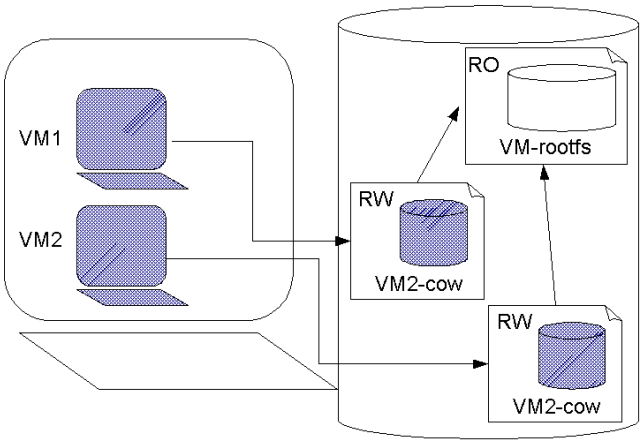

Figure 1 : fichiers *COW*.

4.3 Utilisation de User-Mode Linux dans un environnement pédagogique

Dès 2001, William McEwan [20] a montré comment User-Mode Linux rend possible la création de maquettes pédagogiques virtuelles de réseaux, en inter-connectant plusieurs machines virtuelles au moyen d'interfaces *ethertap*. Un poste dont les ressources peuvent paraître modestes aujourd'hui, à savoir un Pentium III 1Ghz, 384 Mo de RAM et 512 Mo de swap, supportait un réseau virtuel composé d'un routeur firewall interconnectant trois sous réseaux de deux postes virtuels chacun. Une des machines virtuelles, configurée en routeur firewall, assurait le lien entre la machine réelle et l'ensemble du réseau virtuel. Dès lors un poste de travail peut mettre à la disposition d'un étudiant un réseau complet sur lequel il peut effectuer toute manipulation sans perturber le réseau réel de la salle de TP.

En 2003 un premier projet d'étudiant nous avait montré la faisabilité de la transposition du réseau virtuel de McEwan sur un *LiveCD*.

5 VNUML maquettage virtuel de plate-forme réseaux IP

Dans le cadre du projet Euro6IX, pour des évaluations et des expérimentations Ipv6, le Telematics Engineering Department (DIT) de la Technical University of Madrid (UPM) a développé un ensemble de spécifications et d'outils permettant la construction de maquettes réseau, bâties sur l'interconnexion de machines virtuelles User-Mode Linux. L'ensemble, dénommé Virtual Network User Mode Linux (VNUML) [19] [21], fournit une spécification

XML, sous forme de DTD, décrivant le langage de description et de configuration des maquettes et un « parser » se chargeant de l'interprétation de la description de la maquette, de la configuration et du lancement de chacun de ses éléments. Le fichier XML de VNUML décrivant la maquette constitue également les scénarios de création, de démarrage, d'arrêt de simulation. VNUML apporte l'automatisation de la création de maquettes. La production de maquettes ou de configurations multiples est aisément envisageable, car elle se résume à l'écriture de fichiers XML.

L'exemple de la Figure 2 est une adaptation pour VIMINAL d'un scénario fourni en guise de tutoriel par le projet VNUML. Il décrit une maquette constituée de 4 réseaux (Net0 à Net3) inter-connectant 5 machines virtuelles (uml1 à uml5) à l'hôte. Ce dernier héberge la maquette est assure l'inter-connexion avec le réseau Internet.

La Figure 3 donne le code XML correspondant à la maquette de la Figure 2. Pour des raisons de concision, le code XML de description des machines uml4 et uml5 a été omis. Le scénario original et complet est disponible sur le site du projet VNUML [19].

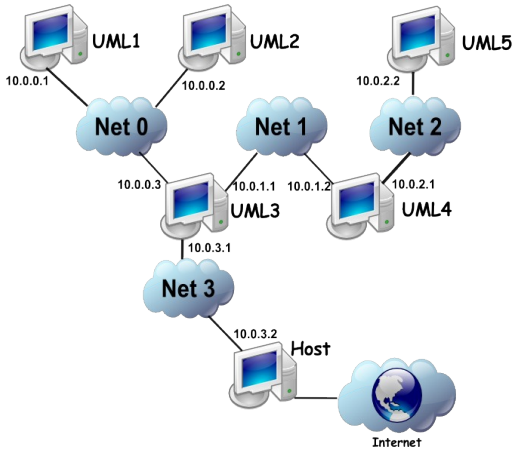

Figure 2 : exemple de maquette.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE vnuml SYSTEM
"/usr/local/share/xml/vnuml/vnuml.dtd">

<!--
VNUML Limited User Scenario adapted for VIMINAL
LiveCD
J. Landru ENIC Telecom Lille 1
- changes from original VNUML scenario :
 use uml-root-fs-viminal instead of VNUML root-fs
    modified con0 statement
-->

<vnuml>
 <global>
  <version>1.6</version>
  <simulation_name>tutorial-lu</simulation_name>
  <automac/>
  <vm_mgmt type="none" />
  <default_filesystem
type="cow">/usr/local/share/vnuml/filesystems/uml
-root-fs-viminal-02</default_filesystem>
  <default_kernel>/usr/local/bin/linux</default_k
ernel>
 </global>
 <net name="Net0" mode="uml_switch" />
 <net name="Net1" mode="uml_switch" />
 <net name="Net2" mode="uml_switch" />
 <vm name="uml1">
  <boot>
   <con0>xterm con1=xterm</con0>
   <!--xterm>gnome-terminal,-t,-x</xterm-->
  </boot>
  <if id="1" net="Net0">
   <ipv4>10.0.0.1</ipv4>
  </if>
  <route type="inet"
gw="10.0.0.3">default</route>
 </vm>
 <vm name="uml2">
   <boot>
    <con0>xterm con1=xterm</con0>
    <!--xterm>gnome-terminal,-t,-x</xterm-->
   </boot>
   <if id="1" net="Net0">
    <ipv4>10.0.0.2</ipv4>
   </if>
   <route type="inet"
gw="10.0.0.3">default</route>
 </vm>
 <vm name="uml3">
  <mem>64M</mem>
  <boot>
   <con0>xterm con1=xterm</con0>
   <!--xterm>gnome-terminal,-t,-x</xterm-->
  </boot>
  <if id="1" net="Net0">
   <ipv4>10.0.0.3</ipv4>
  </if>
  <if id="2" net="Net1">
   <ipv4>10.0.1.1</ipv4>
  </if>
  <route type="inet"
gw="10.0.1.2">10.0.2.0/24</route>
  <forwarding type="ip" />
 </vm>
<!--
...
Le code xml des machines virtuelles uml4 et uml5
est omis pour limiter la place de cet exemple
...
-->
</vnuml>
```

Figure 3 : exemple de scénario VNUML.

Un fichier XML de description de maquette comporte une section globale, encadrée entre les étiquettes `<global>`

</global>, suivie d'une ou plusieurs sections réseau, d'étiquette <net> et une ou plusieurs sections machine virtuelle d'étiquette <vm>. La section globale définit certains paramètres et options dont la validité s'étend à l'ensemble du scénario. On y trouve notamment la référence au *root-fs* par défaut et l'activation du mode COW avec l'attribut type=« cow », ainsi que la référence au noyau GNU/Linux à lancer en mode User-Mode. Les réseaux virtuels sont définis au moyen de l'étiquette <net>. Chaque réseau est identifié par un nom, qui sera utilisé dans la connexion des machines virtuelles. Les machines virtuelles sont ensuite décrites une par une au moyen de l'étiquette <vm>. Chaque section machine virtuelle est composée d'un ensemble d'étiquettes XML, telles que <con0> pour la console, <if> pour la ou les interfaces réseau, <route> pour le routage, etc. La liste complète des étiquettes et leur syntaxe sont référencées dans le guide de référence du langage disponible sur le site de VNUML [19].

Bien que l'étudiant ne manipule pas d'équipements réels, le maquettage offre l'avantage, sur les environnements de simulation, de manipuler les mêmes versions des systèmes et les mêmes configurations que celles qui sont déployées sur des machines réelles. Toutefois à l'instar du modélisme, le maquettage réseau introduit un facteur d'échelle. Ici il ne s'agit pas d'un facteur de taille, l'environnement modélisé peut avoir le même nombre de noeuds qu'un réseau réel, mais d'un facteur de puissance de calcul. Chaque machine virtuelle, bien qu'ayant le même système et le même comportement qu'une machine réelle, dispose d'une capacité de calcul et d'une capacité mémoire réduites par rapport à une machine réelle. L'ensemble des machines virtuelles de la maquette se partage les capacités du poste de travail. Le maquettage VNUML permet donc la manipulation et l'expérimentation, mais il ne permet pas les tests de performance.

6 Les choix pour le *LiveCD* VIMINAL

La mise au point de VIMINAL nécessite de faire plusieurs choix techniques que nous présentons dans ce paragraphe. Tout d'abord, VIMINAL s'appuyant sur GNU/Linux, il faut faire le choix d'une distribution GNU/Linux puis d'une interface graphique utilisateur respectant certaines contraintes (taille, prise en main, etc.). Sur le *LiveCD*, l'utilisation des différentes machines virtuelles User-Mode Linux implique également la configuration des différents systèmes de fichiers utilisés. Enfin, même si la majorité des manipulations faites par les étudiants ne nécessite pas d'autres droits que ceux d'un utilisateur ordinaire, il faut également se pencher sur la gestion du super-utilisateur tant au niveau de la machine hôte qu'au niveau des machines virtuelles.

6.1 Distributions GNU/Linux et outils de génération du *LiveCD*

Le choix d'une distribution GNU/Linux est en général un sujet de discussions animées dans la communauté des supporters du système d'exploitation au pingouin. Une documentation Internet abondante de création de *LiveCD* personnalisés et plusieurs distributions offrent des facilités pour la construction du *LiveCD* VIMINAL. Parmi celles-ci nous avons retenu la distribution Gentoo [24] et son outil Catalyst [25] de création automatisée de *LiveCD*. Ce choix arbitraire pour les supporters d'autres distributions, se justifie par une utilisation familière de cette distribution et le fait qu'une bonne maîtrise de l'outil Catalyst nous permettra de créer facilement de nouveaux *LiveCD* de maquettes pour différents types de TP. La première contrepartie est qu'il nous a fallu initialement adapter VNUML à la distribution Gentoo, VNUML ayant été développé et adapté pour d'autres distributions. Le résultat de cette adaptation a permis une modeste contribution au projet VNUML sous la forme d'un *how-to* [26]. La seconde contrepartie est qu'il a fallu maîtriser l'outil Catalyst qui, bien qu'offrant des fonctionnalités avancées, est en cours de développement et souffre d'une documentation non finalisée et d'une évolution de ses spécifications de configuration lors du changement de version. Il n'en demeure pas moins que la maturité de l'outil progresse rapidement.

Pour les systèmes de fichiers des machines virtuelles. On peut très bien envisager de créer un *root-fs* avec n'importe quelle distribution et notamment celle qu'apprécie le plus l'enseignant responsable de la définition du TP. Nous avons cependant utilisé le même couple d'outils Gentoo/Catalyst. Ce choix allonge quelque peu la durée de génération du *root-fs*, en effet Gentoo est une distribution en mode source, tout le système est donc recompilé de manière automatique. Mais en contrepartie, cela nous permet de conserver la configuration des paquetages constituant le *root-fs* sous forme de simple fichier de spécifications Catalyst, ce qui facilite l'actualisation des *root-fs* avec les dernières versions du système et de ses outils. Mais surtout nous bénéficions des procédures de nettoyage du système de fichiers intégrées à Catalyst afin de minimiser la taille du fichier *root-fs*.

6.2 Choix des environnements graphiques

Les maquettes réseau des séances de TP ne sont pas toutes destinées à des utilisateurs aguerris d'Unix qui maîtrisent toutes les subtilités du mode commande du shell. Le *LiveCD*, ainsi que les distributions des machines virtuelles, offrent les commodités d'un bureau graphique. Un environnement graphique limité est donc embarqué à la fois dans le système du *LiveCD*, le choix s'est porté sur XFCE et dans le système des machines virtuelles où là nous avons choisi Fluxbox. Les environnements de bureau sont différents pour faciliter la distinction entre le bureau de l'hôte et les bureaux des machines virtuelles. De plus, Fluxbox demeure plus léger que XFCE. L'accès aux machines virtuelles se fait donc soit en mode texte sous forme d'une console SSH, soit en mode graphique par l'intermédiaire d'un client VNC. Pour le *LiveCD*, cet environnement graphique permet l'affichage de cartes de la maquette réseau dans un navigateur web, facilitant ainsi la compréhension de l'architecture de la maquette et l'accès aux machines virtuelles. Pour les machines virtuelles, le

bureau graphique permet l'usage d'outils avancés tels qu'un analyseur de protocoles de type Ethereal [2]. Le choix de ces environnements de bureau graphiques doit rester modeste car ils alourdissent de manière non négligeable le système de fichiers du *LiveCD* et le *root-fs* des machines virtuelles. Quand bien même un *LiveCD* peut facilement être remplacé par un *LiveDVD* d'une capacité plus confortable, conserver une taille raisonnable reste important. En effet, n'oublions pas que le verrouillage du *boot* CDrom sur le BIOS des machines des salles de TP nous imposera de trouver le moyen de *booter* le *LiveCD* depuis le réseau. La taille de ce *LiveCD* sera alors un facteur important.

6.3 Imbrications des systèmes de fichiers

Les propriétés des fichiers *COW* sont particulièrement intéressantes dans le contexte de notre *LiveCD*. En effet, celui ci doit supporter l'imbrication de plusieurs systèmes de fichiers GNU/Linux complets : le système de fichiers de la machine réelle (*host-fs*) permettant le démarrage de celle-ci, ainsi que le ou les *root-fs* des machines virtuelles. Avec le système *COW*, on peut se contenter d'un *root-fs* par type de machine virtuelle : un *root-fs* pour les machines et serveurs virtuels qui partagent la même base système ou la même distribution GNU/Linux et un *root-fs* pour les machines virtuelles de type routeur, qui s'appuieront sur un système de type Zebra [22] ou Quagga [23]. De plus, la sauvegarde des fichiers *COW* de chaque machine virtuelle autorisera la conservation de l'état de configuration de la maquette entre deux séances de TP. De même, la destruction d'un fichier *COW* remet la configuration d'une machine virtuelle dans son état initial, l'état de configuration tel qu'il se trouve dans le *root-fs*.

La Figure 4 indique l'imbrication des différents systèmes de fichiers : CDrom, *host-fs*, *root-fs*. Le CDrom est constitué de trois niveaux de systèmes de fichiers imbriqués les uns dans les autres. Au premier niveau, on trouve le système de fichiers du CDrom au format ISO 9660 : il contient l'ensemble des outils de démarrage de GNU/Linux propre à un *LiveCD*, dont le noyau et le système de fichiers de l'hôte dénommé *host-fs*. Le *host-fs* constitue le deuxième niveau d'empilement des systèmes de fichiers. Il est constitué d'un fichier compressé au format *squash-fs*. Ce format permet de créer des systèmes de fichiers en lecture seule avec un taux de compression remarquable, il est particulièrement apprécié dans le contexte des *LiveCD*. Enfin le *host-fs* contient le ou les systèmes de fichiers des machines virtuelles, c'est à dire les *root-fs*.

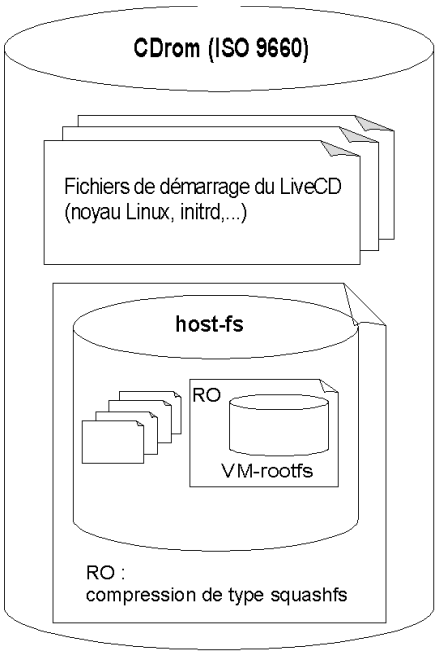

Figure 4 : systèmes de fichiers gigognes.

6.4 Gestion des mots de passe

L'objectif de VIMINAL est de permettre la création de *LiveCD* dédiés à une maquette réseau servant de base à un TP ou une famille de TP. Le *LiveCD* est conçu pour démarrer sur un ensemble le plus large possible de machines éventuellement hétérogènes, en faisant abstraction de leur configuration matérielle. L'outil universel d'auto-configuration n'existe probablement pas, mais le panel couvert par les *LiveCD* d'installation ou par la Knoppix est relativement large. Il doit également démarrer en n'autorisant qu'une session utilisateur sans privilège particulier. La plupart des *LiveCD* tels Knoppix ou les *LiveCD* d'installation des distributions GNU/Linux démarrent automatiquement une session super-utilisateur. Dans notre contexte, de salle de TP, l'utilisateur ne doit pas pouvoir bénéficier des droits étendus lui permettant l'accès privilégié au disque de la machine. Le *liveCD* démarre donc une session pour l'utilisateur viminal. Ce dernier ne dispose pas de droits étendus, par commodité il ne dispose pas de mot de passe. Le super-utilisateur (*root*) du *LiveCD* dispose quant à lui d'un mot de passe inconnu, généré aléatoirement à chaque démarrage du *LiveCD*. L'accès à l'utilisation du compte du super-utilisateur de la machine réelle, c'est à dire l'hôte, est donc verrouillé. L'éventuelle découverte frauduleuse de cette information sensible serait toute façon limitée dans le temps dans la mesure où un redémarrage du *LiveCD*, affectera un nouveau mot de passe au compte root.

Les machines virtuelles démarrent une session super-utilisateur. Par commodité, le super-utilisateur n'a pas de mot de passe. Ce choix peut sembler irresponsable, pour tout administrateur digne de ce nom, mais n'oublions pas que la machine virtuelle est un processus utilisateur vu de l'hôte, elle se comporte comme un bac à sable. L'absence de mot de passe facilite la connexion aux machines

virtuelles. L'alternative d'un mot de passe générique, annoncé dans le sujet de TP, n'est pas plus élégante. Quant à appliquer aux machines virtuelles la solution du mot de passe aléatoire, mise en œuvre pour le *LiveCD,* elle obligerait à initier une console en session super-utilisateur au démarrage de chaque machine virtuelle. De plus, elle imposerait un changement de mot de passe immédiat pour autoriser l'accès à d'autres consoles ou au bureau graphique de la machine virtuelle. Bien que cette attitude de changement systématique de mot de passe ait un intérêt didactique en sensibilisant l'étudiant à l'importance de cette information sensible, elle aurait tendance à alourdir le démarrage des séances de TP.

6.5 Identification des opérations nécessitant des droits étendus

L'utilisation des premières versions de VNUML nécessitait les droits super-utilisateur. Cette restriction a été partiellement levée dans les versions les plus récentes. Le nombre d'opérations nécessitant les droits super-utilisateur a été réduit et bien identifié. Certaines opérations privilégiées restent toutefois nécessaires pour permettre les communications entre l'hôte et les machines virtuelles ou pour permettre aux machines virtuelles d'accéder au réseau de la salle de TP. VNUML permet en effet de construire un réseau virtuel de commandes pour piloter les machines virtuelles. Ce réseau de commandes est distinct des réseaux de la maquette. L'avantage est de permettre une communication directe entre l'hôte et les machines virtuelles pour configurer ces dernières. Séparer le réseau de commande des réseaux de la maquette, permet également de ne pas polluer ces derniers avec les dialogues de pilotage des machines virtuelle. Toutefois ce réseau de commandes nécessite la connexion d'une interface virtuelle de l'hôte. Pour créer et activer cette interface, les droits privilégiés sont nécessaires. Pour le *LiveCD* VIMINAL, ces opérations s'effectuent à l'aide de scripts de démarrage avant que ne démarre la session de l'utilisateur viminal.

7 Limitations

Les machines virtuelles User-Mode Linux ne peuvent pas interagir directement avec les dispositifs matériels du poste de travail. Dès lors, les manipulations induisant le pilotage de tels dispositifs sont difficilement concevables pour ne pas dire inaccessibles. Toutefois il reste possible de mixer une plate-forme réelle reliée au poste hébergeant le réseau de machines virtuelles [21]. Ainsi, par exemple, la connexion de postes téléphoniques IP réels au travers d'une maquette réseau est tout à fait envisageable.

La solution des *LiveCD*, nécessite d'autoriser le démarrage du PC sur le CDrom. Si cela est possibible dans les salles ou labos dédiés et surveillés, elle n'est pas supportable dans les salles informatiques banalisées dans lesquelles l'accès est libre. En effet il suffit dès lors de démarrer la machine depuis un simple CDrom Knoppix pour devenir le super-utilisateur et prendre le contrôle total du poste et de son disque. Une solution de démarrage distant du *LiveCD* devra donc être étudiée. La mise à disposition des *LiveCD* VIMINAL sur un serveur permettra un démarrage distant depuis les salles de TP informatique tout en offrant l'avantage de centraliser les différentes versions, d'éviter la duplication des CDrom avant les séances de TP et d'autoriser le téléchargement de la maquette pour que les étudiants puissent travailler les TP chez eux sur leur machine personnelle.

Le *LiveCD* ne détecte pas et n'active pas pour le moment les éventuelles partitions de *swap* du poste de travail. La taille des maquettes est donc limitée par la taille de la mémoire de la machine hôte. La détection et l'activation automatique d'un espace de *swap* sont à envisager. On s'inspirera pour cela du *LiveCD* Knoppix qui active automatiquement les partitions de swap découvertes sur les disques de la machine.

8 Perspectives d'évolutions

VNUML ne permet aujourd'hui que les machines virtuelles User-Mode Linux. Bien que les possibilités de configurations de telles machines soient larges, depuis les postes de travail, les serveurs de toutes sortes et un panel de routeurs et de firewalls, l'ensemble reste homogène. Des machines GNU/Linux restent interconnectées entre elles. D'autres environnements de virtualisation sont conçus pour lancer n'importe quel système d'exploitation. La reconnaissance de ces environnements par le VNUML permettrait de bâtir des maquettes hétérogènes dans lesquelles cohabiteraient des machines virtuelles GNU/Linux, Free/Net/Open/BSD, Opendarwin, ReactOS voire, si l'on en possède les licences, des OS propriétaires. L'émulateur de processeur QEMU [12] semble être un bon candidat. Il est d'une efficacité certaine, il reconnaît les systèmes de fichiers *COW* et dans le cadre de VNUML pourrait avoir un comportement très proche de User-Mode Linux, ce qui faciliterait son intégration. Une « Feature Request » (RFE) a été déposée sur le projet VNUML, il n'est pas interdit d'espérer qu'à terme on puisse disposer de réseaux virtuels hétérogènes.

La puissance toujours croissante des ordinateurs d'aujourd'hui permet de réaliser des maquettes dont le nombre de noeuds est déjà relativement important. Le lecteur se référera à la maquette intitulée « OSPF Network Laboratory » du site VNUML reproduisant le réseau du laboratoire DIT de l'UPM [27]. Cette maquette met en oeuvre pas moins de 51 machines virtuelles et 45 réseaux virtuels. Les projets de cluster GNU/Linux tels OpenMosix ou OpenSSI, s'ils permettaient l'utilisation transparente de processus User-Mode Linux ou QEMU permettraient probablement de concevoir des maquettes comportant un nombre très importants de noeuds.

9 Conclusion

VIMINAL est un projet d'intégration de systèmes mêlant les caractéristiques et contraintes des CDrom auto-bootables de type *LiveCD* et les machines virtuelles User-Mode Linux. Avec VIMINAL, nous disposons d'une base

fonctionnelle pour développer des plate-formes virtuelles spécifiques à différentes familles de TP système et réseau. L'objectif initial de mise à disposition d'environnements système disposant de droits étendus sans remettre en cause les protections des postes de travail est atteint. Il reste à poursuivre le travail par divers améliorations, notamment dans un premier temps l'activation d'éventuels espaces de mémoire virtuelle (*swap*) pour permettre la construction de maquettes plus importantes.

Références

[1] tcpdump
http://www.tcpdump.org/

[2] Ethereal
http://www.ethereal.com/

[3] OPNET Technologies, Inc.
http://www.opnet.com/

[4] Démolinux :
http://www.demolinux.org/

[5] Knoppix :
http://www.knoppix.org/

[6] IBM VM :
http://en.wikipedia.org/wiki/VM_%28Operating_system%29

[7] VMware
http://www.vmware.com/

[8] User Mode Linux,
http://user-mode-linux.sourceforge.net/
http://usermodelinux.org/

[9] Vanderpool
http://www.intel.com/technology/computing/vptech/
http://www.dancewithshadows.com/vanderpool-virtualization-technology.asp

[10] Pacifica :
http://www.pcinpact.com/actu/news/Pacifica_le_VanderpoolSilverdale_version_AMD.htm

[11] XEN
http://www.cl.cam.ac.uk/Research/SRG/netos/xen/

[12] QEMU
http://fabrice.bellard.free.fr/qemu/

[13] PearPC
http://pearpc.sourceforge.net/

[14] Adeos
http://home.gna.org/adeos/

[15] Bochs
http://bochs.sourceforge.net/

[16] Virtual server
http://www.linuxvirtualserver.org/

[17] Vserver
http://linux-vserver.org/

[18] Colinux
http://www.colinux.org/

[19] VNUML
http://www.dit.upm.es/vnuml/

[20] McEwan, W. (2001) "Using Academic Research Methodologies to Improve the Quality of Teaching: A Case Study". In Proc. Fourteenth Annual Conference of the NACCQ, Napier, New Zealand: 83-93
http://user-mode-linux.sourceforge.net/case-studies.html
http://user-mode-linux.sourceforge.net/cpit.html

[21] Fermín Galán, David Fernández, Javier Rúiz, Omar Walid, Tomás de Miguel. "A Virtualization Tool in Computer Network Laboratories", 5th International Conference on Information Technology Based Higher Education and Training (ITHET'04), Instanbul, May 2004. ISBN: 0-7803-8596-9. IEEE Catalog Number: 04EX898.

[22] Zebra
http://www.zebra.org/

[23] Quagga
http://www.quagga.net/

[24] Gentoo
http://www.gentoo.org/

[25] Catalyst
http://www.gentoo.org/proj/en/releng/catalyst/

[26] Jacques Landru "VNUML on Gentoo Guide"
http://www.enic.fr/people/landru/viminal/vnuml.gentoo/how-to/vnuml-gentoo-guide.html

[27] OSPF Networking Labaratory
http://jungla.dit.upm.es/~vnuml/doc/1.3/examples/ospf_lab/ospf_lab.html