Experiências no uso de máquinas virtuais para o ensino de Redes de Computadores

Ricardo Nabhen [1], **Carlos Maziero**[1]

[1] Pontifícia Universidade Católica do Paraná
Centro de Ciências Exatas e Tecnologia - Curitiba, Paraná, Brasil

{rcnabhen,maziero}@ppgia.pucpr.br

Abstract. *Laboratory practice is a fundamental aspect of computer network learning. Experiments usually demand changes in the local network topology and privileged access to the operating system. These features impose a specific and exclusive laboratory for network teaching experiments. This problem can be alleviated by the use of virtual machines, allowing each student to build its own network experiment, using the appropriate topology, and not disturbing the other activities running in the lab. This paper presents some experiences in using virtual machines to teach advanced aspects of computer networks, like IPSec, firewalls and network services. Also, some key points are highlighted which show the benefits achieved in the learning process.*

Resumo. *A prática em laboratório é uma componente fundamental do ensino de redes de computadores. Os experimentos geralmente exigem a adequação da topologia da rede e o acesso privilegiado às configurações do sistema operacional de cada máquina, que impõe a disponibilidade de um laboratório específico e exclusivo. Esse problema pode ser contornado através do uso de máquinas virtuais, permitindo a cada aluno construir sua própria rede de computadores, com a topologia adequada para cada experimento, sem interferir com a estrutura física do laboratório e as atividades dos demais alunos. Este artigo apresenta algumas experiências no uso de máquinas virtuais para o ensino de aspectos avançados de redes de computadores, como IPSec, firewalls e serviços de rede, onde são destacados alguns pontos importantes que indicam os benefícios para a prática pedagógica.*

1. Introdução

A prática em laboratório é uma componente fundamental do ensino de redes de computadores. Em experimentos mais complexos, muitas vezes torna-se necessário adequar a topologia da rede do laboratório a cada experimento e alterar as configurações do sistema operacional de cada máquina. Por exemplo, para se realizar um experimento de construção de uma arquitetura de *firewall*, é necessário a) organizar a topologia do laboratório, dispondo computadores nas redes externa, interna e *DMZ* (*demilitarized zone*), b) instalar interfaces de rede adicionais nas máquinas que farão o roteamento e filtragem dos pacotes entre as redes, c) configurar as respectivas tabelas de roteamento, e d) configurar os endereços de rede e demais atributos das máquinas das três regiões.

Essa característica não-convencional das atividades práticas da disciplina de redes de computadores (que aparece também em algumas outras disciplinas da área de sistemas, como sistemas operacionais) exige a disponibilidade de um laboratório específico e exclusivo para as atividades dos alunos nessa disciplina. Todavia, nem sempre isso é possível; a realidade da maioria da instituições de ensino impõe o uso de laboratórios compartilhados com diversas turmas e disciplinas, o que inviabiliza a realização de experimentos mais elaborados, que exijam exclusividade no uso do laboratório. Esse problema pode ser contornado através do uso de máquinas virtuais. Essa tecnologia permite a cada aluno construir sua própria rede de computadores virtuais, interligando-os de acordo com a topologia adequada para cada experimento, sem interferir com a estrutura física do laboratório e as atividades dos demais alunos. O uso de máquinas virtuais para o ensino de disciplinas na área de sistemas não é novidade, ele vem sendo proposto desde os anos 80 [Donaldson 1987]; no entanto, os recentes desenvolvimentos na área de máquinas virtuais [Rosenblum and Garfinkel 2005] justificam a retomada dessa tecnologia como facilitador do processo de aprendizagem. Hoje um aluno geralmente tem poder computacional suficiente em seu computador doméstico para executar várias máquinas virtuais e reproduzir os experimentos realizados em sala.

Este artigo apresenta algumas experiências no uso de máquinas virtuais para o ensino de aspectos avançados de redes de computadores, como *IPSec*, *firewalls* e serviços de rede. O artigo está estruturado da seguinte forma: a seção 2 apresenta a tecnologia de máquinas virtuais, enumerando as possibilidades, vantagens e limitações decorrentes de seu uso; a seção 3 discute as possibilidades de uso de máquinas virtuais no ensino de redes; a seção 4 apresenta o contexto no qual os experimentos aqui descritos foi desenvolvidos; a seção 5 ilustra alguns dos experimentos realizados; a seção 6 discute trabalhos correlatos e finalmente a seção 7 conclui o trabalho.

2. A tecnologia de máquinas virtuais

Uma máquina virtual (*Virtual Machine - VM*) é definida em [Popek and Goldberg 1974] como sendo uma duplicata isolada de uma máquina real. Um ambiente de máquina virtual é criado por um monitor de máquinas virtuais (*Virtual Machine Monitor - VMM*), o qual cria uma ou mais máquinas virtuais sobre uma mesma máquina real. Cada máquina virtual provê as funcionalidades necessárias para um sistema operacional convidado que acredita estar executando sobre uma plataforma convencional de hardware. Usos típicos de máquinas virtuais incluem o desenvolvimento e teste de novos sistemas operacionais e a consolidação de servidores.

Existem duas arquiteturas clássicas para sistemas de máquinas virtuais: nos sistemas de tipo I, o monitor é implementado entre o hardware e os sistemas convidados; os ambientes de máquinas virtuais *Xen* [Barham et al. 2003] e *VMWare ESX Server* [VMware 1999] são exemplos desta arquitetura. Nos sistemas de tipo II o monitor é implementado como um processo de um sistema operacional convencional subjacente, denominado sistema hospedeiro; os sistemas *VMWare Workstation* [VMware 1999] e *User-Mode Linux* [Dike 2000] usam esta arquitetura.

O ambiente de maquinas virtuais adotado nas experiências descritas neste trabalho é o UML - User-Mode Linux [Dike 2000], um monitor de maquinas virtuais de tipo II que permite executar sistemas convidados Linux sobre um sistema hospedeiro Linux.

Esse monitor foi escolhido por ser *open source*, leve e bastante flexível.

3. Máquinas virtuais no ensino de redes

A tecnologia de máquinas virtuais pode ser adotada com benefícios concretos nas práticas de laboratórios das disciplinas de sistema, como redes de computadores e sistemas operacionais. Entre esses benefícios podem ser citados [Davoli 2004] [Kneale et al. 2004]:

- pode-se criar mais hosts virtuais que o número de computadores físicos disponíveis no laboratório, permitindo que cada aluno crie sistemas complexos, envolvendo vários hosts;
- o número de interfaces de rede de cada host e a interligação entre as mesmas é feita no plano virtual, sem restrições vinculadas à topologia física do laboratório ou à configuração de suas máquinas;
- o aluno é o administrador de seus hosts virtuais, podendo alterar suas configurações e instalar os softwares necessários a cada experimento;
- o aluno pode salvar na máquina real o estado de cada máquina virtual, permitindo assim desenvolver experimentos mais demorados, ou de caráter incremental;
- o aluno pode reproduzir o experimento em casa, se possuir um computador mediano e os softwares necessários.

Uma primeira abordagem para o uso de máquinas virtuais no ensino de redes seria dispor de um laboratório específico, no qual cada computador teria instalado um monitor de máquinas virtuais local, como o *UML* [Dike 2000] ou o *VMWare Workstation* [VMware 1999]. O sistema pode ser configurado para permitir que máquinas interajam com as máquinas reais do laboratório, ou com máquinas virtuais em outros computadores. Essa abordagem, utilizada por [Stockman 2003], [Adams and Laverell 2005] e [Kneale et al. 2004], é simples de implementar, mas pouco flexível, pois ainda exige a implantação de um laboratório específico (embora não necessariamente exclusivo). Outra abordagem consiste em instalar o monitor de máquinas virtuais em um servidor central, como proposto em [Davoli 2004]. Neste caso, o aluno se conecta ao servidor, lança as máquinas virtuais que precisar para seu experimento e interage com elas localmente (dentro do servidor) ou através de máquinas reais na rede local. Embora seja mais flexível, essa abordagem exige um um servidor de maior porte para a execução das máquinas virtuais, que podem demandar recursos significativos de processamento, memória e espaço em disco.

Um aspecto importante a discutir é a adequação dos diferentes tipos de máquinas virtuais às necessidades de ensino. Um monitor de máquinas virtuais de tipo I executa diretamente sobre o hardware (ou está embutido no sistema operacional hospedeiro). Neste contexto, a criação de uma máquina virtual é uma operação privilegiada, reservada ao administrador, o que inviabiliza a criação de máquinas virtuais sob demanda. Além disso, normalmente o acesso aos recursos de baixo nível (drivers) e às configurações de rede também são operações privilegiadas, o que limita as possibilidade de configuração. Exemplos de uso de monitores de tipo I como apoio ao ensino são apresentados em [Norton 2002] e [Villanueva and Cook 2005]. Um monitor de máquinas virtuais de tipo II é visto pelo sistema hospedeiro como um processo de usuário. Assim, a criação de máquinas virtuais sob demanda só é restrita pela quantidade de recursos (memória, espaço em disco) disponíveis ao usuário. Além disso, o aluno tem total controle sobre a configuração de

hardware e software de cada máquina virtual, permitindo experimentos mais complexos e de nível mais baixo. Os trabalhos [Stockman 2003], [Davoli 2004], [Kneale et al. 2004] e [Adams and Laverell 2005] usam monitores de tipo II e exploram a possibilidade de criação de máquinas virtuais sob demanda.

4. O Ambiente de ensino implantado

Em nossa instituição, o ensino de redes é feito usando prioritariamente um Laboratório de Redes construído especificamente para esse fim. Esse laboratório, que também é utilizado com sucesso no ensino das redes convergentes [Nabhen and Pedroso 2005], é composto por 25 computadores divididos em 5 bancadas e interligados por redes locais. Além das máquinas, estão disponíveis *hubs, switches*, roteadores, adaptadores de rede sem fio, patch panels e outros equipamentos de conectividade. A motivação para o uso de máquinas virtuais surgiu das seguintes constatações:

- os alunos têm de vir até a universidade para realizar os trabalhos extra-classe; como o uso do laboratório está saturado, alunos que precisam fazer trabalhos fora de horário têm dificuldade em encontrá-lo livre;
- as mudanças freqüentes nas configurações das máquinas são fonte de transtornos na realização dos experimentos.

Com base nessas constatações, foi delineada uma solução usando máquinas virtuais, que permitisse resolver os problemas encontrados e oferecer outras facilidades, como a possibilidade de realizar experimentos remotos, mesmo que exigissem clientes gráficos (*browsers*, clientes de *e-mail*, etc) e a preservação do trabalho de cada aluno, sem risco de deleção de trabalhos em andamento por outros alunos.

A solução encontrada foi disponibilizar um sistema de máquinas virtuais de tipo II através de um servidor de médio porte, a ser acessado pelos alunos remotamente, usando terminais textuais e/ou gráficos. Cada aluno possui uma conta no servidor e pode lançar máquinas virtuais sob demanda, configuradas para atender as necessidades de cada experimento. A Figura 1 ilustra a arquitetura do sistema desenvolvido.

Além disponibilizar a criação de máquinas virtuais sob demanda, o ambiente implantado traz os seguintes benefícios:

- como o servidor está integrado ao laboratório de rede, as máquinas virtuais podem se comunicar com os computadores reais do laboratório, permitindo trazer um maior realismo aos experimentos;
- o servidor oferece acesso às contas através de *SSH* (terminal texto) e *VNC* (terminal gráfico). Este último é essencial para que o aluno possa testar remotamente os serviços implementados usando clientes gráficos (browsers);
- as imagens de disco e demais configurações de cada aluno ficam armazenadas em sua conta no servidor, permitindo a execução de experimentos de longa duração e/ou incrementais;
- imagens pré-definidas, com configurações e/ou softwares específicos, são disponibilizadas em um diretório público, facilitando a realização dos experimentos;
- aplicações gráficas, como analisadores de protocolos e clientes de e-mail, podem ser lançadas *dentro* das máquinas virtuais (as janelas dessas aplicações são desviadas para a sessão gráfica do respectivo usuário usando a rede virtual 0).

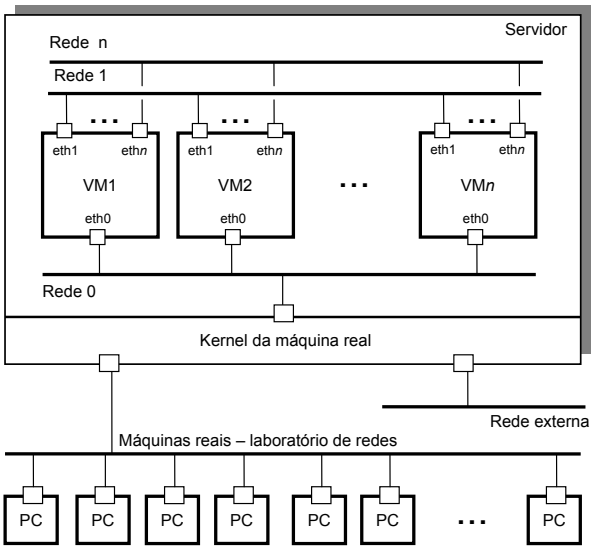

Figura 1. Ambiente de ensino implantado

O servidor utilizado é um computador *Dell PowerEdge* 1500, com dois processadores PIII de 1.1 GHz, 2 GBytes de memória RAM e 100 GBytes de espaço em disco. Como software, foi instalado o sistema *Linux Fedora Core 3* no sistema hospedeiro e *Linux RedHat 9* nos sistemas convidados. Com essa configuração, o servidor atende sem sobrecarga cerca de 40 usuários; é freqüente observar 40-50 máquinas virtuais ativas simultaneamente.

5. Experimentos realizados

A flexibilidade dada pelo uso das máquinas virtuais tem possibilitado o desenvolvimento de uma série de experimentos que de outra forma seriam inviáveis. Estes procedimentos vão desde tarefas básicas de configuração de máquinas até as mais complexas, envolvendo a instalação, a configuração e a operação de serviços. Com o uso das máquinas virtuais, diversos cenários podem ser implementados pelos alunos de forma individual ou coletiva, possibilitando, também, um ambiente com uma melhor interação e colaboração. Nesta seção serão apresentados dois experimentos utilizados no ensino das redes de computadores abordando cenários usualmente empregados nas soluções relacionadas com a segurança de redes.

5.1. Arquiteturas de *Firewalls* - Rede *DMZ*

As redes *DMZ - Demilitarized Zone* - se apresentam como uma das soluções mais usuais das arquiteturas de *firewalls*. O princípio básico de sua implementação se baseia no isolamento da rede interna de uma determinada empresa da área onde são colocados os *hosts* acessíveis à rede externa. No desenvolvimento deste experimento, os alunos devem propor uma solução para um cenário onde há a necessidade da implementação desta arquitetura de *firewall*. Por exemplo, seja o seguinte cenário: ”Determinada empresa disponibiliza uma certa aplicação aos seus clientes. Esta aplicação é executada em um servidor

WEB presente em suas instalações. Também, a empresa possui uma rede local para seus colaboradores internos, os quais podem acessar a Internet e os serviços disponibilizados nos servidores da empresa. A empresa ainda possui um servidor *DNS* que mantém seu serviço de nomes."

A partir do cenário proposto, os alunos realizam o planejamento da topologia da rede. Em seguida, definem os esquemas de roteamento e endereçamento IP. Posteriormente, passam à implementação do cenário utilizando a estrutura disponibilizada pelas máquinas virtuais. A Figura 2 apresenta uma topologia possível para implementação do cenário descrito.

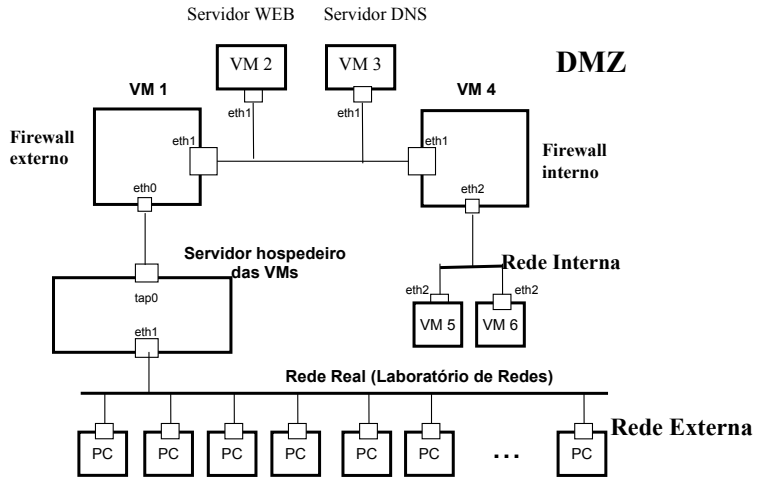

Figura 2. Cenário 1: Rede *DMZ* com uso das *VMs*

A Figura 2 mostra a utilização de seis máquinas virtuais (VM_1 a VM_6). Cabe ressaltar dois aspectos importantes que reforçam o benefício didático alcançado pelo uso das máquinas virtuais. Em primeiro lugar, este cenário pode ser implementado por um aluno ou por um grupo, dando condições para que todos tenham acesso aos recursos que estão sendo trabalhados. Esta é uma questão-chave para o bom aprendizado da prática desenvolvida, muitas vezes limitada pela indisponibilidade de equipamentos. Em segundo lugar, a montagem de um cenário complexo como este em um laboratório de comum é inviável, pois seria necessário um grande número de máquinas disponíveis e, ainda, que elas estivessem com configurações adequadas para tal. Neste cenário devem ser instalados e ativados os serviços *HTTP*, *DNS* e a filtragem de pacotes. Pela utilização da *DMZ*, os servidores [1] *HTTP* e *DNS* são implantados, respectivamente, nas máquinas VM_2 e VM_3. Por sua vez, os mecanismos de filtragem de pacotes são configurados nas máquinas VM_1 e VM_4. Finalmente, VM_5 e VM_6 representam as máquinas dos colaboradores internos da empresa. Após a instalação dos serviços citados em cada uma das máquinas virtuais definidas, a tarefa seguinte passa a ser a aplicação das regras de filtragem [2] nas máquinas VM_1 e VM_4. A seguir, são apresentadas algumas regras[3] como exemplo:

[1]Normalmente, são instalados os pacotes *Apache* e *Named* disponibilizados de forma gratuita para o ambiente *Linux*.

[2]Normalmente, é utilizado o sistema *iptables* que está presente nas versões do *kernel* do *Linux* mais recentes.

[3]As regras associadas ao tráfego de resposta não estão sendo apresentadas.

- **VM**$_1$: Autorizar o tráfego destinado à máquina VM$_2$ na porta 80/TCP no sentido eth$_0$ $\Rightarrow$ eth$_1$;
- **VM**$_1$: Autorizar o tráfego destinado à máquina VM$_3$ na porta 53/UDP no sentido eth$_0$ $\Rightarrow$ eth$_1$;
- **VM**$_4$: Autorizar o tráfego destinado a servidores externos na porta 80/TCP provenientes de máquinas com endereços *IP* pertencentes à faixa de endereçamento da rede interna no sentido eth$_2$ $\Rightarrow$ eth$_1$;
- **VM**$_4$: Autorizar o tráfego destinado à máquina VM$_3$ na porta 53/UDP no sentido eth$_2$ $\Rightarrow$ eth$_1$.

O cenário da Figura 2 permite algumas avaliações interessantes. Por exemplo, as máquinas reais localizadas no laboratório de redes podem ser configuradas para acessar a rede formada pelas máquinas virtuais. Neste caso, os alunos podem simular o acesso de clientes externos à rede, onde possíveis ataques e vulnerabilidades das configurações são avaliados. Da mesma forma, utilizando o serviço *VNC*, acessos via *browser* ao serviço *HTTP* da máquina VM$_2$ podem ser realizados a partir das máquinas VM$_5$ e VM$_6$, onde ocorre a simulação de um acesso de um cliente pertencente à rede interna. Note que todas estas possibilidades permitem uma avaliação ampla das atividades realizadas durante o experimento.

5.2. Redes Virtuais Privadas - *VPN* - com *IPsec*

As redes virtuais privadas (*VPNs*) são redes que se baseiam no uso de um meio compartilhado, como a infra-estrutura da própria Internet, para a interligação de redes. Elas se apresentam como alternativa mais econômica quanto à utilização de serviços de telecomunicações, uma vez que uma rede privada é "construída" sobre uma rede pública, sem que seus usuários tenham que contratar novos serviços de comunicação. Na realidade, esta rede privada é construída utilizando técnicas associadas ao tunelamento de pacotes, criptografia e autenticação.

Dentre as soluções utilizadas na implementação das redes virtuais privadas, o *IPSec* [Kent and Atkinson 1998] tem tido maior destaque, estando hoje disponível nos principais sistemas operacionais modernos e suas distribuições. As políticas *IPSec* são definidas a partir de regras que especificam listas de condições e suas respectivas listas de ações a serem executadas. As ações definidas nas políticas envolvem, normalmente, a especificação da forma como a conexão deve ser realizada entre as entidades que compõem a *VPN*. Por exemplo, abaixo são apresentadas duas regras para ilustrar a sistemática da definição de políticas *IPSec*:

- **Regra 1**: Se o tráfego utilizar o protocolo TCP e for destinado à porta 80 do servidor WEB, exija criptografia dos dados, caso contrário negue o estabelecimento da *VPN*;
- **Regra 2**: Se o tráfego for proveniente da rede 10.0.0.0/8, exija autenticação dos pacotes, caso contrário negue o estabelecimento da *VPN*.

O *IPSec* define dois protocolos para serem utilizados durante uma conexão *VPN*. O primeiro, o *AH(Authentication Header)* define um mecanismo para a autenticação de pacotes, enquanto o segundo, o *ESP(Encapsulating Security Payload)*, permite a criptografia dos dados, objetivando a confidencialidade das informações. O cenário tipicamente utilizado nos experimentos com as máquinas virtuais para a implementação de *VPNs* é

mostrado na Figura 3. O cenário apresentado é o de uma *VPN NET-TO-NET*. Pretende-se, com isto, criar um canal seguro de informações entre as redes internas dos dois *sites* de uma empresa hipotética, a *Rede Local 1* e a *Rede Local 2*.

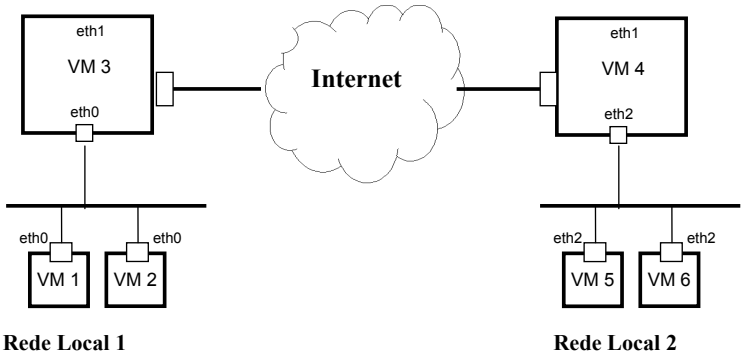

Figura 3. Cenário 2: Rede Virtual Privada com uso das *VMs*

No cenário da Figura 3 foram utilizadas seis máquinas virtuais. Os pares [VM_1, VM_2] e [VM_5, VM_6] representam as máquinas dos usuários das duas redes locais. As máquinas VM_3 e VM_4 desempenham o papel de *gateways* da *VPN*. Neste caso, os alunos instalam pacotes de soluções *IPSec* [4] e aplicam as políticas necessárias ao estabelecimento do canal seguro de comunicação entre as duas redes, o qual é assumido no *link* que interliga as interfaces eth_1 destes dois *gateways*. Por exemplo, as políticas usuais deste cenário são definidas pelas seguintes regras:

- **VM_3:** Todo o tráfego da Rede Local 1 destinado à Rede Local 2 deve ser transportado pela *VPN NET-TO-NET* estabelecida entre as interfaces eth_1 dos *gateways*. Essa *VPN* deve utilizar *ESP*;
- **VM_4:** Todo o tráfego da Rede Local 2 destinado à Rede Local 1 deve ser transportado pela *VPN NET-TO-NET* estabelecida entre as interfaces eth_1 dos *gateways*. Essa *VPN* deve utilizar *ESP*.

Após esta configuração, os alunos avaliam a eficácia do experimento pela análise do tráfego capturado entre as duas redes locais, quando observam o tunelamento e a criptografia conseguidos com a *VPN*. Assim, confirmam a operação do canal seguro de comunicação entre os *sites*. O tráfego capturado é obtido a partir da comunicação entre as máquinas virtuais pertecentes às redes internas distintas.

6. Trabalhos Correlatos

Diversos trabalhos na literatura apresentam experiências de uso de máquinas virtuais no ensino das disciplinas ditas "de sistema", como sistemas operacionais, redes de computadores e sistemas distribuídos. A seguir apresentamos alguns que se assemelham em objetivo e estratégia ao estudo apresentado neste trabalho.

Em [Davoli 2004], o autor ilustra as possibilidades de uso o ambiente *UML* no ensino de administração de servidores *UNIX*, dando como exemplos a configuração de serviços de *DNS* para *Ipv4* e *Ipv6*, *LDAP* e configurações de roteamento. Um conjunto

[4] Por exemplo, o conjunto de ferramentas disponível em http://ipsec-tools.sourceforge.net/

de três servidores abriga as máquinas virtuais dos alunos, que podem ser criadas sob demanda. O acesso aos servidores reais é feito por *SSH* (Secure Shell), o que pode limitar o uso de clientes gráficos por alunos iniciantes. O trabalho [Kneale et al. 2004] implementa um ambiente denominado *Velnet* para o ensino de redes de computadores. Esse ambiente consiste de um conjunto de máquinas virtuais (usando *VMware*) executando em cada um dos computadores dos alunos. As máquinas virtuais interagem entre si através de redes virtuais, sem possibilidade de interação entre máquinas virtuais e máquinas reais da rede. Foi construída uma ferramenta gráfica para auxiliar os alunos a compor suas redes virtuais com máquinas virtuais pré-configuradas: roteadores, servidores de arquivos, servidores web, etc. Uma experiência um pouco diferente foi relatada em [Norton 2002], na qual é usado um servidor *IBM S/390* para executar centenas de servidores virtuais Linux, um para cada aluno distinto. Esses servidores são acessíveis através da Internet e servem como base para o desenvolvimento dos trabalhos acadêmicos nas disciplinas de sistema e de programação para a Web. Uma solução similar a esta foi apresentada em [Villanueva and Cook 2005]. O artigo [Adams and Laverell 2005] realiza um estudo comparativo entre as plataformas *UML* e *VMWare* para o ensino de disciplinas de sistema. A configuração usada no estudo difere daquela aqui apresentada, pois os autores usam instalações locais dos ambientes de máquinas virtuais em cada uma das máquinas do laboratório, que é exclusivo para essas disciplinas e não pode ser acessado externamente.

Os monitores isolam as máquinas virtuais entre si e em relação à máquina real, o que permite ver cada máquina virtual como um *host* autônomo. Entretanto, há outras formas de atingir esse objetivo, ao menos parcialmente. Um conceito conhecido como virtualização do espaço usuário permite criar contextos isolados entre si e autônomos, operando sobre um mesmo sistema operacional. Implementações conhecidas desse conceito são as *Solaris Zones* [Tucker and Comay 2004], as *FreeBSD Jails* [McKusick and Neville-Neil 2004] e os *Virtual Servers* do *Linux* [VServer-Project 2004]. O artigo [Armitage 2003] explora as possibilidades de uso da funcionalidade *Jails* do ambiente *FreeBSD*, que permite a criação de réplicas isoladas do espaço de usuário do sistema operacional, cada réplica com seu próprio endereço IP. Essa abordagem tem um melhor desempenho que as máquinas virtuais, mas restringe os alunos ao espaço de usuário das réplicas: a pilha de rede e os drivers do sistema operacional não podem ser modificados, pois estão no núcleo da máquina real, o que impede experimentos de roteamento e filtragem de pacotes, por exemplo.

7. Conclusão

Este artigo apresentou algumas experiências no uso de máquinas virtuais para o ensino de aspectos avançados de redes de computadores. Foram apresentados os cenários envolvendo a criação de Redes Virtuais Privadas com o *IPSec* e de uma das arquiteturas de *firewalls* mais comuns, as Redes *DMZ*. Os resultados observados após o emprego das máquinas virtuais nos experimentos desenvolvidos ao longo dos cursos são extremamente satisfatórios, onde destacam-se a motivação e o maior envolvimento dos alunos, bem como a melhora do nível de aproveitamento do período destinado à execução dos procedimentos práticos. É comum os alunos iniciarem alguns experimentos em aula, continuarem em casa e retomarem sua execução no encontro seguinte. Também, a maioria das limitações existentes foram eliminadas devido à flexibilidade dada pelo uso das máquinas virtuais, observada pela possibilidade da criação dos mais variados cenários envolvendo

a instalação, configuração e operação de serviços e aplicações de redes.

Referências

Adams, J. and Laverell, W. (2005). Configuring a multi-course lab for system-level projects. *ACM Technical Symposium on Computer Science Education*.

Armitage, G. (2003). Maximising student exposure to networking using FreeBSD virtual hosts. *ACM SIGCOMM Computer Communications Review*, 33(3).

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, X. A. (2003). Xen and the art of virtualization. *Proceedings of the ACM Symposium on Operating Systems Principles - SOSP*.

Davoli, R. (2004). Teaching operating system administration with user mode linux. *Proceedings ACM Annual Conference on Innovation and Technology in Computer Science*.

Dike, J. (2000). A user-mode port of the linux kernel. *Proceedings of the 4th Annual Linux Showcase and Conference*.

Donaldson, J. (1987). Teaching operating systems in a virtual machine environment. *Proceedings 18th SIGCSE Technical Symposium on Computer Science Education*.

Kent, S. and Atkinson, R. (1998). Security architecture for the internet protocol. *Request for Comments - RFC 2401*.

Kneale, B., Horta, A., and Box, I. (2004). Velnet - virtual environment for learning networking. *Proceedings 6th Australasian Computing Education Conference*.

McKusick, M. and Neville-Neil, G. (2004). The design and implementation of the FreeBSD operating system. addison-wesley professional. *Addison-Wesley Professional*.

Nabhen, R. and Pedroso, C. (2005). Projeto, implementação e operação de um laboratório para o ensino de redes convergentes. *XIII Workshop sobre Educação em Computação - WEI - Sociedade Brasileira de Computação*.

Norton, R. (2002). Using virtual linux servers. *IEEE Computer*.

Popek, G. and Goldberg, R. (1974). Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, 17(7).

Rosenblum, M. and Garfinkel, T. (2005). Virtual machine monitors: Current technology and future trends. *IEEE Computer*.

Stockman, M. (2003). Creating remotely accessible virtual networks on a single PC to teach computer networking and operating systems. *ACM Conference On Information Technology Education*.

Tucker, A. and Comay, D. (2004). Solaris zones: Operating system support for server consolidation. *3rd USENIX Virtual Machine Research and Technology Symposium*.

Villanueva, B. and Cook, B. (2005). Providing students 24/7 virtual access and hands-on training using VMware GSX server. *ACM SIG on University and College Computing Services Conference*.

VMware (1999). VMware technical white paper. *VMware Inc*.

VServer-Project (2004). Linux VServer project. *http://www.linux-vserver.org*.