PROJETO DE REDES
www.projetoderedes.com.br

Projeto, implementação e operação de um laboratório para o ensino de redes convergentes

Carlos Marcelo Pedroso , Ricardo Nabhen

[1] Pontifícia Universidade Católica do Paraná
Centro de Ciências Exatas e Tecnologia
Rua Imaculada Conceição, 1155 - Prado Velho,
Curitiba, Paraná, Brasil

c.pedroso@pucpr.br, rcnabhen@ppgia.pucpr.br

Abstract. *The efficient utilization of communication networks is a very important subject. The integration of voice, data and image transmission proposed by the convergent networking leads to lower communication costs and simplifies the network management. Studies foresee that 95% of the operating computer networks will be based on this convergence in 2010. In this context, the convergent network teaching becomes one of the most important issues for the networking and telecommunications area professionals. This paper presents the experience of the project and operation of the convergent network laboratory through the years of 2003 and 2004 at the Pontifical University Catholic of Paraná, PUCPR. The main strategies used in the conception and assembly of this laboratory as well as some of the scenarios successfully developed during the classes and experiments are presented.*

Resumo. *A eficiência no uso das redes de comunicação é de fundamental importância. A integração da transmissão de voz, dados e imagem proposta pelas redes convergentes abrem as portas para custos de comunicação mais baixos e para simplificação no gerenciamento de rede. Estimativas prevêem que 95% das redes de computadores em operação serão baseadas nesta convergência em 2010. Neste contexto, o ensino de redes convergentes tornou-se um dos aspectos fundamentais na formação do profissional da área de redes e telecomunicações. Este artigo apresenta a experiência do projeto e da operação do laboratório de redes convergentes ao longo dos anos de 2003 e 2004 na Pontifícia Universidade Católica do Paraná, PUCPR. Serão apresentadas as principais estratégias utilizadas na concepção e montagem do laboratório bem como alguns dos cenários desenvolvidos com sucesso durante as aulas e experimentos.*

1. Introdução

A utilização da rede de computadores para transmissão de voz, dados e imagem em uma infra-estrutura flexível com possibilidade de configuração de diversos tipos de aplicativos com diferentes níveis de qualidade serviço originou o termo *redes convergentes*.

O mercado mostra-se cada vez mais favorável ao uso de redes convergentes por duas causas principais. A primeira é econômica: a manutenção de uma infra-estrutura única para voz e dados representa uma economia de recursos financeiros com enlaces de transmissão, compra de equipamentos e pessoal. Um dos benefícios diretos desta tendência é a economia com as chamadas telefônicas de longa distância, uma vez que

permite a realização de chamadas sem o uso da rede de telefonia convencional das operadoras de telecomunicações. Um fato que também deve ser citado é que grande parte das empresas já dispõe de um enlace de dados que permite o acesso dos usuários de sua rede interna à Internet. É comum observar que este enlace já é utilizado para a interligação da rede de dados de duas ou mais unidades, muitas vezes com disponibilidade de banda suficiente para a integração almejada. A segunda causa que justifica o uso das redes convergentes é técnica: a utilização de uma rede convergente apresenta novas possibilidades de comunicação dentro da empresa, como a integração entre aplicativos de voz e dados (ex. correio eletrônico e telefonia) ou a implementação de estações de trabalho móveis.

O ensino de redes convergentes tornou-se um dos aspectos fundamentais na formação do profissional da área. A formação desejada para tal profissional engloba questões como sistema de cabeamento estruturado, redes locais Ethernet, protocolo IP, redes ATM, até qualidade de serviço e voz sobre IP. A qualidade de serviço refere-se a disponibilidade de um conjunto de recursos percebida por um determinado aplicativo. Estes recursos podem ser: disponibilidade de banda, atraso máximo de propagação, variação do atraso (*jitter*), perda de pacotes, etc.

Para suportar o ensino de redes convergentes, é necessário que a Universidade esteja equipada com laboratórios específicos para o ensino nesta área. Laboratórios de informática não são suficientes: é necessário que o estudante possa atuar como projetista e administrador da rede, criando topologias, configurando e testando cenários de utilização. Através dos experimentos realizados nestes cenários, o estudante poderá identificar as vantagens e implicações de se possuir uma rede convergente, utilizando as principais tecnologias disponíveis no mercado para dar o suporte às aplicações e compreendendo os parâmetros que devem ser considerados na sua implantação e operação.

Este artigo relata a experiência do projeto e da operação do laboratório de redes convergentes ao longo dos anos de 2003 e 2004 na Pontifícia Universidade Católica do Paraná, PUCPR. Serão apresentadas as principais estratégias utilizadas na concepção e montagem do laboratório bem como alguns dos cenários possíveis desenvolvidos com sucesso durante as aulas e experimentos. Este artigo está estruturado como segue. A seção 2 mostra como foi realizado o projeto da infra-estrutura física do laboratório, apresentando os equipamentos disponíveis e descrevendo os sistemas operacionais escolhidos para o uso. A seção 3 apresenta as configurações de cenários de uso que se mostraram mais adequadas para o ensino de redes convergentes. A seção 4 conclui o artigo.

2. Infra-estrutura física

O ensino redes convergentes requer a disponibilidade de recursos que permitam a construção de topologias e cenários dos mais diversos possíveis. Neste contexto, a montagem do laboratório de redes convergentes da PUCPR teve como principais requisitos:

- Flexibilidade na montagem de cenários de utilização da rede;
- Utilização de multi-plataformas de sistemas operacionais de rede e software livre;
- Liberdade de configuração e acesso aos equipamentos sem risco de danos físicos;
- Situar-se no estado da arte da tecnologia disponível, incluindo qualidade de serviço e voz sobre IP.

Para o alcance destes objetivos, foi realizado um projeto físico utilizando o conceito de cabeamento estruturado, de acordo com a norma brasileira NBR 14565 [ABNT, 2002]. Desta forma, obteve-se flexibilidade e segurança física dos equipamentos, tornando possível produzir virtualmente qualquer configuração desejada sem que seja necessário manipular o equipamento diretamente.

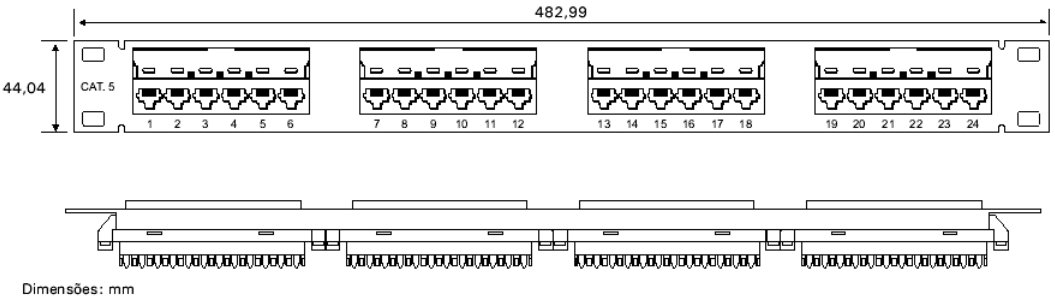

Figura 1: Painel de manobra

Foi estabelecida uma parceria com uma empresa líder de mercado na área de redes convergentes, onde a universidade foi equipada com dispositivos desta área, que a permitiram se posicionar no estado da arte da tecnologia. Por outro lado, a empresa pôde utilizar os recursos da universidade para treinamento e capacitação de pessoal, além de contar com uma vitrine de grande alcance para seus produtos.

O laboratório dispõe de 4 bancadas com 5 computadores em cada uma delas. Em cada bancada existem 6 tomadas de telecomunicações, conectadas a um painel de manobra localizado em um armário de conexões. A Figura 1 mostra um diagrama esquemático de um painel de manobra. Cada tomada de telecomunicações corresponde a um conector fêmea na parte frontal do painel.

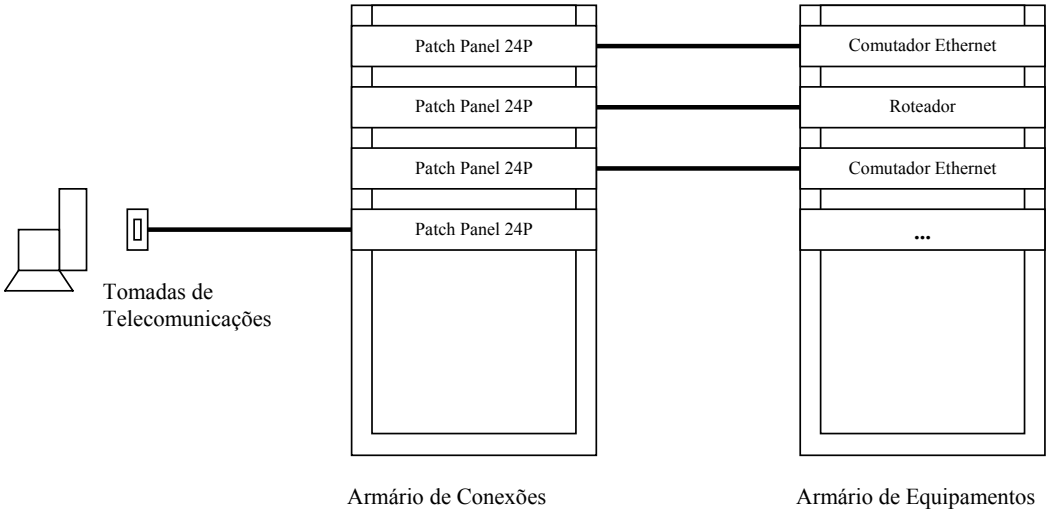

Figura 2: Topologia física de conexões

Os cabos que conectam as tomadas de telecomunicações ao armário de conexões são chamados de *cabeamento horizontal* e neste caso consistem de cabos *UTP (Unshielded Twisted Pair)* categoria 5, suportando taxas de transmissão de até 100Mbps.

A Figura 2 mostra a topologia física de conexões do laboratório. Um armário de equipamentos, normalmente mantido fechado, contém os equipamentos ativos: comutadores ethernet, roteadores, entre outros.

As interfaces dos equipamentos ativos foram mapeadas em painéis de manobra no armário de conexões cruzadas. Os equipamentos foram conectados de modo a agrupar no mesmo painel de manobra os equipamentos que normalmente seriam utilizados em uma pequena rede ou em um departamento de uma grande empresa. Em cada painel de manobra foram conectados: comutador Ethernet (24 portas), roteador IP (4 portas), *fire-*

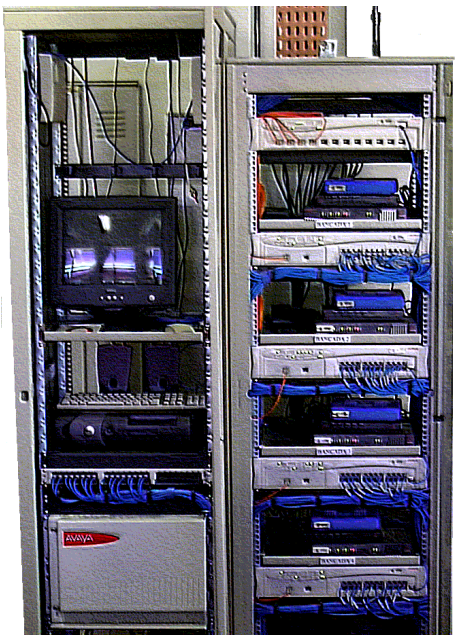

Figura 3: Armário de equipamentos

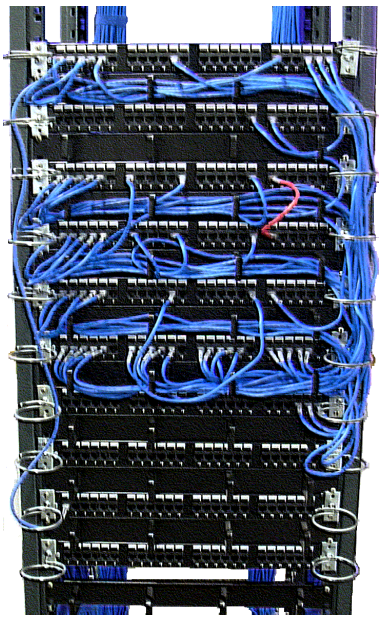

Figura 4: Armário de conexões

wall (4 portas), hardware para *VPN - Virtual Private Network* (2 portas), em um total de 4 conjuntos de painéis. As interfaces de um *PABX Voz sobre IP (VoIP)*, com 16 portas de telefonia analógica e 2 interfaces de rede Ethernet, suportando a tecnologia H.323 [Hassan et al., 2000] também foram mapeadas no armário de conexões cruzadas.

A Figura 3 mostra a disposição dos equipamentos no armário de telecomunicações. Foram necessários dois armários para acomodar todos os equipamentos. No armário ao lado esquerdo, pode observar-se o *PABX VoIP* e um servidor utilizado em seu gerenciamento. Ao lado direito, o armário contendo 5 comutadores Ethernet, 4 roteadores, 4 caixas *firewall*, 4 caixas *VPN*.

A configuração da topologia é feita realizando-se a conexão cruzada entre as portas dos painéis de manobra na parte frontal do armário de conexões. A Figura 4 mostra um exemplo de configuração para um dos cenários utilizados. O aluno fica encarregado de realizar a configuração do cenário, sem que seja necessária a manipulação do equipamento, apenas realizando interligações no armário de conexões cruzadas.

Durante o desenvolvimento das atividades práticas no laboratório, o estudante é confrontado com problemas típicos da operação de redes convergentes, devendo propor e implementar possíveis soluções para tais problemas. Posteriormente, em função da flexibilidade permitida, ele poderá avaliar o desempenho de sua solução.

Quando o estudante configura a topologia de conexões físicas do laboratório para a experiência prática, ele estará indiretamente sendo treinado no conceito de cabeamento estruturado. Ao longo das aulas, tornam-se evidentes para os alunos os benefícios obtidos com a utilização de um projeto baseado na norma. Quando o profissional formado confrontar-se com problemas práticos de projetos de cabeamento, ele certamente irá lembrar-se da metodologia de trabalho utilizada.

Para facilitar a configuração inicial dos equipamentos, todas as interfaces de console foram conectadas a um painel de manobra localizado no armário de conexões cruzadas. Desta forma, será possível de realizar a configuração inicial do equipamento a partir de qualquer computador situado ao longo das bancadas.

Também, estão disponíveis câmeras para realização de vídeo-conferências e telefones IP. O laboratório permite experiências com redes sem fio utilizando o padrão *IEEE802.11b* [IEEE802.11, 2004] e integração com a rede através de pontes *802.11* para *802.3*, conhecidos pela sigla *AP - Access Point*.

O grande benefício da estrutura física montada é a possibilidade de configuração de *qualquer* topologia de rede apenas através da interligação dos pontos do armário de conexões através de cabos de manobra. Não existe a necessidade de operação direta sobre os equipamentos ativos ou sobre o cabeamento da rede horizontal.

2.1. Equipamentos Disponíveis

Os equipamentos ativos foram especificados para equipar quatro ambientes de rede local. Os equipamentos são:

- Comutadores Ethernet: Suportam o padrão *IEEE 802.1Q e p* [IEEE802.1Q, 1998] para marcação de *VLAN* e priorização de tráfego para qualidade de serviço. Estão disponíveis 4 comutadores de 24 portas 10/100BaseTx e duas portas 1000BaseSx. Também está disponível um comutador com 12 portas 1000BaseSx camada 3;
- Roteadores IP: Suportam o roteamento IP e a configuração de qualidade de serviço utilizado o *CBQ (Class Based queue* [Floyd and Jacobson, 1995]). Os roteadores também suportam o protocolo de sinalização *RSVP (Resource Reservation Protocol*, algoritmos para distribuição de rotas *RIP (Routing Information Protocol)* [Malkin, 1998] e *OSPF (Open Shortest Path First)* [Moy, 1998], além de filtros de tráfego e *NAT (Network Address Translation) [Egevang and Francis, 1994]*. Estão disponíveis 4 roteadores com duas portas Ethernet 10/100BaseTx e duas portas seriais síncronas;
- *Firewall* IP: Estão disponíveis 4 sistemas de firewall por hardware, com 3 portas Ethernet 10/100BaseTX;
- Wireless: Estão disponíveis 2 *Access Point* com um canal cada e uma interface Ethernet e 2 *Access Points* operando com dois canais simultaneamente. O padrão suportado é o *IEEE 802.11b* [IEEE802.11, 2004]. Estão disponíveis também cartões de rede *wireless* para os computadores;
- Voz sobre IP: Um *PABX VoIP* implementa o padrão H.323. O *PABX* disponibiliza 16 ramais analógicos, cujos pontos foram mapeados no armário de conexões. Existem telefones IP disponíveis e a possibilidade de utilizar os computadores como telefones via software.

A configuração do sistema foi planejada para suportar o *ensino* para os diversos níveis de cursos de graduação e pós-graduação, sendo possível a configuração de cenários para o ensino de redes convergentes com ênfase para utilização de sistemas baseados em redes Ethernet.

Os equipamentos utilizados são típicos de uso comercial e não é possível realizar a inclusão ou modificação do software do equipamento nas camadas física, enlace e rede.

2.2. Sistema Operacional

Estão sendo utilizados computadores com inicialização dual para o sistema operacional. O aluno pode escolher entre os sistemas operacionais Linux e Windows 2000. A escolha destes sistemas operacionais fundamenta-se pela grande utilização destes no ambiente das organizações.

O sistema operacional Linux é um sistema Unix compatível que possui código fonte aberto e um grande número de aplicativos disponibilizados gratuitamente, da mesma forma, com código fonte aberto. É um sistema ideal para área de pesquisa e para

exploração de recursos. Particularmente, a formação obtida com o sistema Linux capacita o aluno a atuar como um administrador de sistemas Unix e oferece oportunidades de atuação com sistemas operacionais de diferentes fornecedores: Solaris, Aix, Irix, entre outros, além de estar recebendo formação básica que permite a atuação na área de sistemas abertos. Atualmente o mercado carece de mão de obra técnica especializada, o que pode atrasar a implantação de projetos de sistemas abertos por parte de agências de governo e empresas; a formação técnica oferecida por parte da Universidade irá contribuir para o esforço nesta área, revertendo-se em ganhos para a sociedade como um todo.

A importância do sistema operacional Windows 2000 deve-se a sua grande utilização no ambiente comercial. A formação de um bom engenheiro de redes convergentes deve contemplar o conhecimento dos sistemas mais utilizados no mercado.

Utilizando-se os sistemas operacionais são desenvolvidas experiências de configuração dos serviços de rede mais importantes: compartilhamento de arquivos, resolução de nomes, gerência de redes, servidores Web, chamada a procedimentos remotos, autenticação em ambientes heterogêneos e correio eletrônico. A disponibilidade do Linux e Windows permite ao aluno o contato com sistemas heterogêneos e as possíveis soluções de integração disponíveis, bem como a visualização de problemas gerados a partir de protocolos proprietários.

3. Cenários possíveis

Esta seção apresenta quatro cenários tipicamente utilizados durante os experimentos efetuados no laboratório de redes convergentes. A subseção 3.1 apresenta dois cenários básicos, que servem de base para a maioria dos experimentos efetuados, enquanto a subseção 3.2 apresenta um cenário usado comumente no estudo da transmissão de voz sobre IP e outro cenário abordando o tópico de segurança de redes, no qual é utilizado software livre para a construção de arquiteturas de *firewalls* e *proxies*.

3.1. Cenários Básicos

3.1.1. Redes Ethernet

Este cenário mostra as possibilidades de configuração de uma rede Ethernet comutada. Os estudantes são colocados diante de uma rede corporativa que já possui uma rede local para dados e deseja-se implantar uma rede de telefonia IP.

Supõe-se que cada bancada constitui um departamento ou um andar de um prédio que possui equipamentos de dados e voz em uma rede Ethernet com topologia estrela, onde os equipamentos de cada departamento ou andar são conectados com um comutador ethernet utilizando cabos *UTP* em uma taxa de transmissão de 100Mbps. Os comutadores são conectados a um comutador central utilizando fibras ópticas a uma taxa de transmissão de 1Gbps. A topologia resultante é mostrada na Figura 5.

Naturalmente, é preciso que os equipamentos de dados das diversas bancadas possam comunicar entre si, o mesmo valendo para os equipamentos de voz (tipicamente, uma pessoa utilizando um telefone IP em uma bancada fazendo uma chamada a outra pessoa em outra bancada). Neste caso, é solicitado aos alunos que façam a caracterização do tráfego da rede, normalmente utilizando analisadores de protocolos como o *Ethereal* [Orebaugh and Ramirez, 2004] e o *Analyzer* [Degioanni et al., 2004]. Em seguida, são configuradas uma *VLAN* (*Virtual LAN* [IEEE802.1Q, 1998] para o tráfego de dados e uma outra *VLAN* para o tráfego de voz. As *VLANs* representam um importante instrumento no gerenciamento de tráfego de redes locais, possibilitando que vários computadores passem

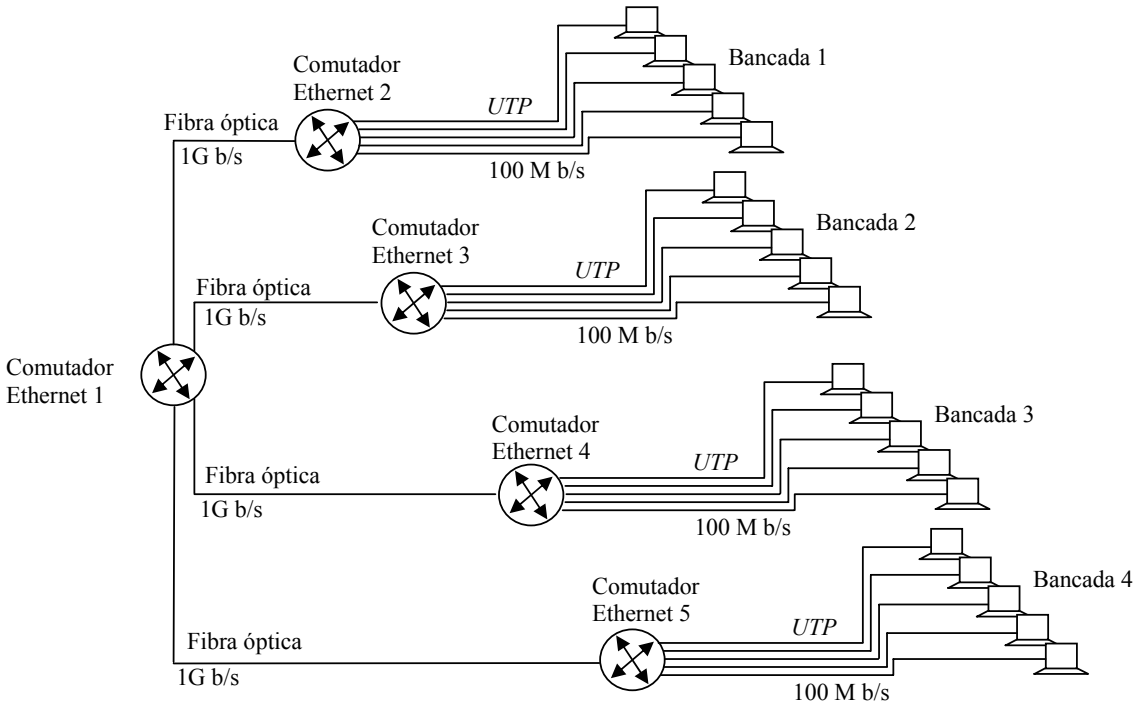

Figura 5: Cenário para o ensino de redes Ethernet

a pertencer a uma mesma rede local virtual independentemente do comutador físico que estejam conectados.

Após esta configuração inicial, é solicitado que o tráfego de voz seja priorizado em relação ao tráfego de dados utilizando os níveis de prioridade de quadros definidos na norma 802.1Q [IEEE802.1Q, 1998]. Para implementação deste cenário, os estudantes configuram o modo *entroncamento* entre interligações entre comutadores ethernet, uma vez que nestes segmentos irão trafegar pacotes provenientes das duas *VLANs* (dados e voz). Finalmente, os alunos realizam novamente uma análise do tráfego da rede utilizando os analisadores de protocolo, agora dando ênfase à observação do tráfego das *VLANs* de forma isolada e aos benefícios alcançados com esse isolamento e com a política de prioridade estabelecida.

Posteriormente, a topologia da Figura 5 é alterada de modo a produzir conexões redundantes entre os comutadores, permitindo a realização de testes com o algoritmo *spanning tree* [IEEE802.1D, 2004], que realiza o bloqueio de portas objetivando eliminar caminhos redundantes em uma rede Ethernet comutada.

3.1.2. Roteamento e endereçamento

Este cenário mostra a utilização do laboratório para o aprendizado de roteamento estático e dinâmico. O cenário é mostrado na Figura 6. Inicialmente, é necessário que os estudantes realizem um projeto de endereçamento IP e roteamento estático. Supõe-se, por exemplo, que cada bancada constitui uma rede distinta, portanto, tornando necessário a utilização de comutadores IP para a interligação destas redes. Neste caso, deve ser proposto um esquema de endereçamento IP para cada rede, inclusive para a interligação dos roteadores IP 2 e 3. O esquema de endereçamento é projetado utilizando-se duas situações típicas: A primeira empregando-se endereços de redes IP independentes e a outra empregando-se um único endereço base, quando é discutido o uso de sub-redes e de máscaras [Comer, 2002].

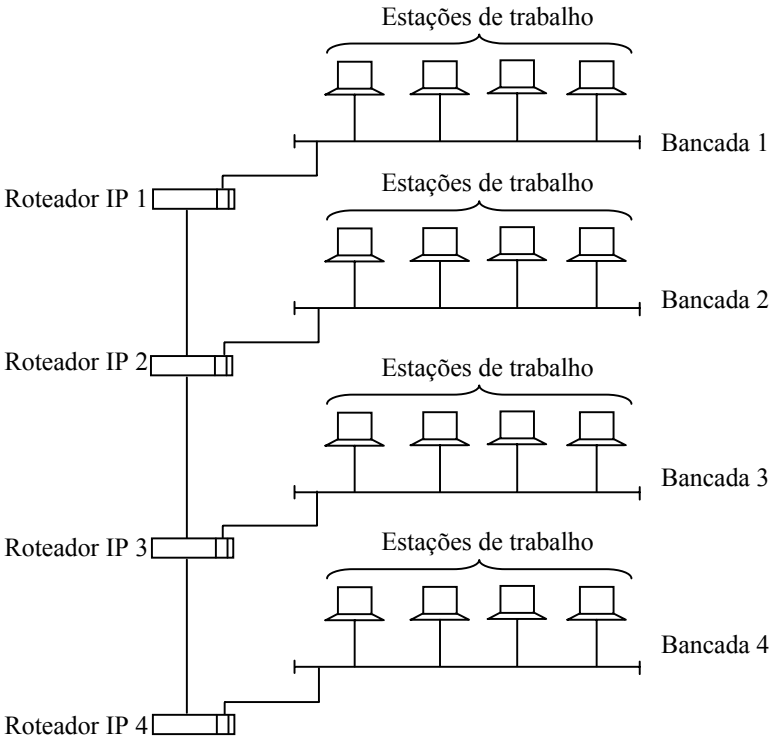

Figura 6: Cenário para o ensino de roteamento

Após o projeto de endereçamento, os estudantes aplicam as configurações IP em cada equipamento da rede, inclusive nas interfaces dos roteadores. Mesmo com a aplicação de forma apropriada do esquema de endereçamento, não existirá conectividade entre as máquinas das diferentes sub-redes (ver Figura 5. Este problema mostra a necessidade da realização de um outro procedimento vital para as redes IP: a definição das tabelas de roteamento [Tanenbaum, 2003] dos roteadores IP que interligam as sub-redes. Neste momento é realizado o planejamento das rotas necessárias para a comunicação entre as quatro sub-redes e a aplicação destas configurações aos roteadores, finalizando o processo de configuração estática de rotas. A conectividade é testada novamente para que os estudantes verifiquem o número de saltos que os pacotes gerados em uma sub-rede realizam até chegarem ao seu destino, questão fundamental que deve ser compreendida no processo de comutação IP.

Como experimento final, as rotas são excluídas e a comunicação entre as sub-redes será interrompida. Em seguida, é solicitado que seja habilitado o protocolo para a descoberta automática de rotas (*RIP - Routing Information Protocol* [Malkin, 1998]) nas interfaces dos roteadores, protocolo que permite que os comutadores, e outros dispositivos (disponível também nas plataformas Windows e Linux), troquem informações de roteamento. Desta forma, os estudantes observam que o comutador de sua bancada adicionou em sua tabela de roteamento as rotas necessárias para as redes das outras bancadas, concluindo a importância vital do processo de roteamento dinâmico no ambiente das redes IP. Utilizando analisadores de protocolo, os estudantes compreendem o processo de troca de mensagens utilizada pelo protocolo *RIP* e suas limitações.

3.2. Cenários Avançados

3.2.1. Voz sobre IP

Um dos cenários mais importantes para o estudo das redes convergentes é o da transmissão de voz sobre IP. Este cenário tem como base os dois cenários apresentados na

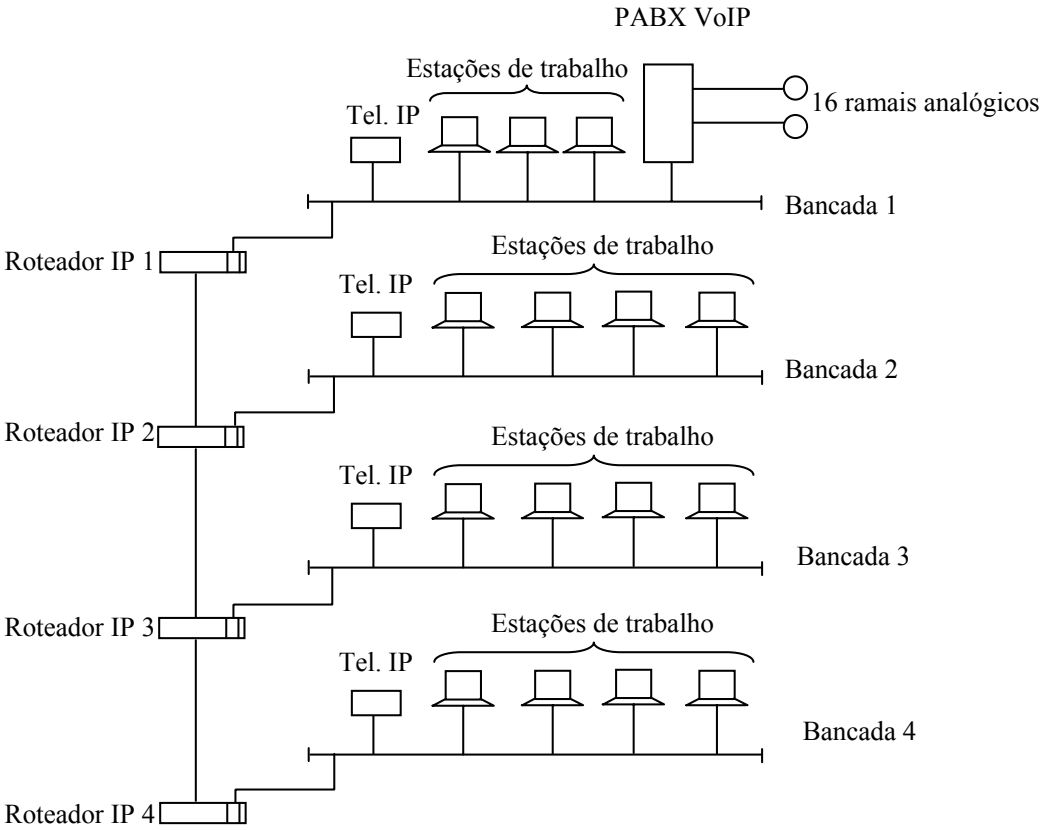

Figura 7: Cenário para o ensino de voz sobre IP

subseção 3.1.

A configuração do cenário é apresentada na Figura 7. Como pode ser observado nesta figura, o dispositivo *gatekeeper*, que é responsável pelo controle da operação da rede de telefonia na arquitetura H.323, é instalado na rede da bancada 1. Além disso, este equipamento também atua como dispositivo *gateway*, realizando a interligação entre os telefones IP e os telefones analógicos. Vale a pena citar que este dispositivo ainda permite a interligação com centrais de comutação telefônicas convencionais, permitindo que a rede de telefonia IP da organização esteja totalmente integrada à rede pública de telefonia. Neste experimento, os estudantes instalam e testam telefones IP nas sub-redes de cada bancada.

Uma das questões fundamentais relacionadas com o tráfego de telefonia IP é o uso de protocolos de sinalização e controle. Como citado anteriormente, os telefones IP e o equipamento *gatekeeper* disponível no laboratório interagem através do H.323, conjunto de protocolos e padrões que regulam o tráfego de telefonia, dispondo de protocolos para, por exemplo, que os telefones IP se anunciem ao *gatekeeper* e para iniciar e terminar uma chamada.

Durante a realização dos experimentos, os alunos estudam o tráfego gerado pela rede de telefonia através dos analisadores de protocolos, observando o uso dos protocolos durante a realização de chamadas. Um outro aspecto fundamental neste estudo é a análise dos sistemas de codificação (conhecidos como *codecs*) utilizados para codificar e comprimir a voz durante uma conversação. Os estudantes também avaliam o consumo de banda requerido pelos diferentes *codecs* (como G.711 [ITUG.711, 1988] ou G.723 [ITUG.723, 1988], por exemplo) e o impacto no tráfego da rede. Posteriormente, observam a operação do protocolo de transmissão em tempo real (*RTP - Real Time Protocol* [Audio-Video Transport Working Group et al., 2003]), que é o protocolo de aplicação

utilizado para transportar o tráfego de telefonia durante uma conversação.

Finalmente, é solicitado aos estudantes que realizem a geração de tráfego na rede e avaliem a o impacto sobre a qualidade percebida na transmissão de voz. São utilizadas ferramentas de geração de tráfego desenvolvidas pelos próprios alunos em linguagem C e Java. Assim, é observado que o tráfego de telefonia torna-se sofrível quando a rede está sobrecarregada, situação que os alunos resolvem com a adoção de políticas de qualidade de serviço, realizando a reserva de recursos para o tráfego de telefonia através do *CBQ* [Floyd and Jacobson, 1995]. Este experimento mostra a influência do tráfego de dados sobre o tráfego de telefonia e que é de fundamental importância a adoção de mecanismos de qualidade de serviço para diferenciar o tráfego de aplicações sensíveis à disponibilidade de banda, atrasos de transmissão e variações do atraso.

3.2.2. Segurança de Redes

O uso de software livre tem crescido de maneira importante no ambiente das redes de computadores corporativas. Em função da facilidade de obtenção, do baixo custo de propriedade e da flexibilidade na sua utilização, cada vez mais as organizações estão adotando este tipo de software para prover serviços aos seus usuários. Desta forma, a habilidade de instalar, configurar e manter serviços em cenários como este é fundamental para o profissional da área de redes.

Esta subseção mostra um dos cenários utilizados no treinamento dos estudantes na área de segurança de redes utilizando software livre. O cenário está apresentado na Figura 8. Note que este cenário tem como base o cenário apresentado na subseção3.1.2. Neste cenário supõe-se que cada bancada seja uma rede independente de uma empresa, onde é preciso permitir que o servidor Web de cada bancada seja acessado por usuários externos.

Como primeira tarefa, os alunos devem estabelecer o esquema de endereçamento IP para cada rede. Da mesma forma, devem configurar adequadamente a informação de roteamento. Em seguida, selecionam três máquinas com sistema operacional Linux em cada rede para desempenhar os seguintes papéis:

- *Firewall*: Tem como objetivo proteger a rede interna dos acessos provenientes da rede externa por meio da filtragem de pacotes;
- *Proxy*: Tem como objetivo fazer *caching* de páginas para otimizar o acesso Web relativo aos usuários da rede interna;
- Servidor Web: Tem como objetivo disponibilizar o serviço Web para os usuários das redes interna e externa.

Todos os aplicativos são obtidos a partir de pacotes de software livre. Após a instalação destes aplicativos, os alunos passam à fase de configuração, que envolve os seguintes procedimentos:

- Configurar e ativar o servidor Web disponibilizando páginas para acesso;
- Configurar os navegadores (*browsers*) para utilizarem o serviço de *proxy*;
- Configurar o servidor de *proxy* e uma lista de controle de acesso determinando quem poderá usar o serviço. Também são criadas regras de filtragem de conteúdo;
- Configurar o *firewall* adicionando regras que implementam a política de segurança citada anteriormente.

Com o cenário configurado, é solicitado que os alunos de uma bancada passem a agir como invasores, atacando serviços e computadores das redes das demais bancadas.

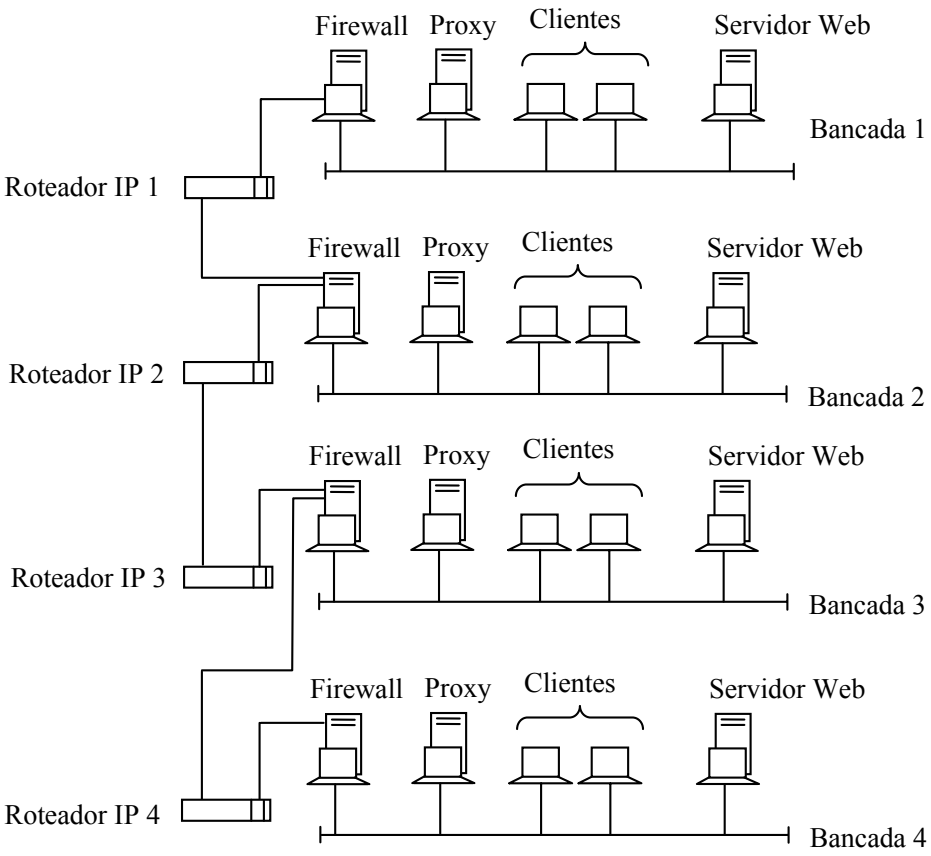

Figura 8: Cenário para o ensino de segurança em redes convergentes

Esta experiência deve mostrar a eficácia da operação do *firewall* e do *proxy*. Apesar da simplicidade das regras e acessos configurados, ao final deste roteiro, o estudante observa a importância do uso de arquiteturas de *firewalls* e *proxies* em uma rede, além da competência adquirida na instalação e configuração dos aplicativos.

4. Conclusões

Este artigo apresentou a experiência no projeto e na operação do laboratório de redes convergentes da Pontifícia Universidade Católica do Paraná, PUCPR, adquirida ao longo dos anos de 2003 e 2004. Este laboratório tem sido utilizado na formação dos profissionais da área de redes e telecomunicações dos diversos cursos de graduação e pós-graduação da Universidade. Foram apresentadas as estratégias utilizadas na montagem e concepção do laboratório, cujo objetivo principal foi a flexibilidade de operação, permitindo que os alunos durante as aulas realizem o projeto e a implementação dos mais variados cenários, dentro os quais foram apresentados o projeto da infra-estrutura usando a norma de cabeamento estruturado, a montagem e configuração de redes ethernet, o projeto de endereçamento e roteamento IP, projeto e implementação de Telefonia IP e, finalmente, o projeto e implementação de segurança de redes utilizando software livre.

Um estudo comparativo realizado junto aos professores dos cursos e disciplinas que utilizam este laboratório confirma a importância de seu uso. Os dados apontam para uma redução média da ordem de 20% no número de repetências nas disciplinas relacionadas e, conseqüentemente, para um aumento da ordem de 15% na nota média destas mesmas disciplinas. Além disso, observa-se com facilidade o nível de satisfação dos alunos em usar o laboratório, o que propiciou o maior envolvimento dos alunos durante as aulas e a nítida redução no número de ausências.

Referências

ABNT (2002). ABNT/NBR 14565. procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada. Associação Brasileira de Normas Técnicas.

Audio-Video Transport Working Group, Schulzrinne, H., Casner, S., Frederick, R., and Jacobson, V. (2003). RFC 3550: RTP: A transport protocol for real-time applications. Status: PROPOSED STANDARD.

Comer, D. (2002). *Redes de Computadores e Internet*. Bookman, Rio de Janeiro, 1^a edition.

Degioanni, L., Politano, P., Risso, F., and Viano, P. (2004). Analyzer: a public domain protocol analyzer. http://analyzer.polito.it/.

Egevang, K. and Francis, P. (1994). RFC 1631: The IP network address translator (NAT). Status: INFORMATIONAL.

Floyd, S. and Jacobson, V. (1995). Link-sharing and resource management models for packet networks. *IEEE/ACM Transactions on Networking*, 3(4):365–386.

Hassan, M., Nayandoro, A., and Atiquzzaman, M. (2000). Internet telephony: Services, technical challenges, and products. *IEEE Communications Magazine*, 38(4):96–103.

IEEE802.11 (2004). Wireless local area networks. IEEE Std 802.11.

IEEE802.1D (2004). Standard for local and metropolitan area networks: Media access control (MAC) bridges. IEEE Std 802.1D.

IEEE802.1Q (1998). 802.1q - virtual lans. IEEE Std 802.1Q.

ITUG.711 (1988). ITU recommendation G.711 (11/88). Pulse code modulation (PCM) of voice frequencies.

ITUG.723 (1988). ITU recommendation G.723 (11/88). Extensions of Recommendation G.721 adaptive differential pulse code modulation to 24 and 40 kbit/s for digital circuit multiplication equipment application.

Malkin, G. (1998). RFC 2453: RIP version 2.

Moy, J. (1998). RFC 2328: OSPF version 2.

Orebaugh, A. D. and Ramirez, G. (2004). *Ethereal Packet Sniffing*. Syngress Publishing, 1st edition.

Tanenbaum, A. S. (2003). *Computer Networks*. Prentice Hall, New York, 4th edition.