

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

**BALANCEAMENTO DE CARGA E REDUNDÂNCIA USANDO MÚLTIPLOS
LINKS DE INTERNET E SUA VIABILIDADE ECONÔMICA**

**BALANCEAMENTO DE CARGA E REDUNDÂNCIA USANDO MÚLTIPLOS
LINKS DE INTERNET E SUA VIABILIDADE ECONÔMICA**

Monografia apresentada ao curso de
Bacharelado em Sistemas de
Informação da Faculdade Natalense
para o Desenvolvimento do Rio
Grande do Norte como requisito
parcial para a obtenção do título de
Bacharel em Sistemas de Informação.

Orientador: **George Henrique Bezerra**

Aluna: **Ferreira da Silva, Nely**

**NATAL/RN
2004**

LIGA FARN
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
CURSO DE BACHARELADO EM SISTEMA DE INFORMAÇÃO

BALANCEAMENTO DE CARGA E REDUNDÂNCIA USANDO MÚLTIPLOS
LINKS DE INTERNET E SUA VIABILIDADE ECONÔMICA
**BALANCEAMENTO DE CARGA E REDUNDÂNCIA USANDO MÚLTIPLOS
LINKS DE INTERNET E SUA VIABILIDADE ECONÔMICA**

George Henrique Bezerra

Monografia apresentada ao curso de
Bacharelado em Sistemas de
Informação da Faculdade Natalense
para o Desenvolvimento do Rio
Grande do Norte como requisito
parcial para a obtenção do título de
Bacharel em Sistemas de Informação.

Orientador:

Aluizio Ferreira da Rocha Neto

NATAL/RN
2004

Bezerra, George Henrique

Balanceamento de Carga e Redundância Usando Múltiplos *Links*
de Internet / George Henrique Bezerra. -- Natal: FARN, 2004.
63 p.

Monografia (Graduação em Sistemas de Informação) –
Faculdade Natalense para o Desenvolvimento do Rio Grande do
Norte.

Orientador: Aluizio Ferreira da Rocha Neto (M.sc)

1. Internet-Monografia. 2. Balanceamento de Links-Monografia.
3. Redes de Computadores I. Título

RN/FARN/BC

CDU 004.7

FARN

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
CURSO DE BACHARELADO EM SISTEMA DE INFORMAÇÃO**

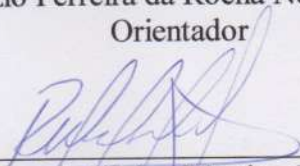
**BALANCEAMENTO DE CARGA E REDUNDÂNCIA USANDO MÚLTIPLOS
LINKS DE INTERNET E SUA VIABILIDADE ECONÔMICA**

George Henrique Bezerra

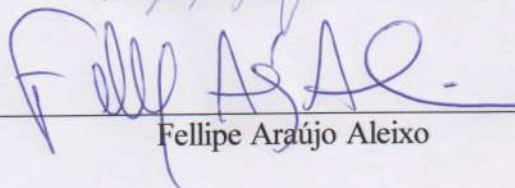
Monografia apresentada e aprovada em 15 de
DEZEMBRO de 2004 pela banca examinadora composta pelos
seguintes membros.



Aluizio Ferreira da Rocha Neto, Ms.C
Orientador

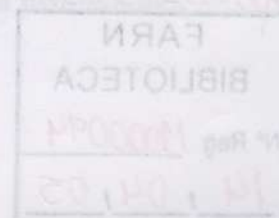


Ricardo Kleber Martins Galvão



Felipe Araújo Aleixo

Natal, 15 de DEZEMBRO de 2004



CURSO DE BACHARELADO EM SISTEMA DE INFORMAÇÃO
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
LIGA DE ENSINO DO RIO GRANDE DO NORTE

LINKS DE INTERNET E SUA VIABILIDADE ECONÔMICA
BALANCEAMENTO DE CARGA E REDUNDÂNCIA USANDO MÚLTIPLOS

George Henrique Bezerra

Monografia apresentada e aprovada em _____ de _____ de 2004 pela banca examinadora composta pelos seguintes membros:


Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador


Ricardo Kleber Martins Galvão


Felipe Araújo Aluizio

Natal, 12 de Setembro de 2004

88-21.375
FARN
BIBLIOTECA
Nº Reg M000094
14, 04, 05

M
004.738.5
B469L
2004

AGRADECIMENTOS

Principalmente a Deus por estar sempre me cercado e me auxiliando pelas melhores formas, aos meus pais João Batista Bezerra e Maria Margarida de Lira Bezerra (as avózinhas), que sempre me apoiaram e torceram por meu sucesso pessoal e profissional, e minha querida esposa Adriana Karla, pela paciência e incentivo ao longo da graduação.

Aos meus avós João Batista Ferreira e Maria de Lourdes de Oliveira Ferreira, por sempre estarem presentes ajudando no que fosse preciso.

Ao meu orientador, professor doutor Abílio Ferreira da Rocha Neto, pelo auxílio na orientação desta monografia.

Aos meus pais dedico este trabalho, pelo apoio e incentivo que deles recebi em toda minha vida.

A minha querida esposa, Adriana, pela compreensão e incentivo.

Ao meu filho Pedro Henrique, que é a maior razão de todo meu esforço de melhoria profissional.

AGRADECIMENTOS

Primeiramente a Deus por estar sempre me encaminhando pelos melhores rumos, aos meus pais João Batista Bezerra e Maria Margarete de Lima Bezerra (*in memoriam*), que sempre me apoiaram e torceram por meu sucesso pessoal e profissional, a minha querida esposa Adriana Karla, pela paciência e incentivo ao longo da graduação.

Aos meus sogros João Batista Ferreira e Maria de Lourdes de Oliveira Ferreira, por sempre estarem presentes ajudando no que fosse preciso.

Ao meu orientador, professor mestre Aluizio Ferreira da Rocha Neto, pelo auxílio na orientação desta monografia.

RESUMO

Este trabalho apresenta uma solução de balanceamento de *links*¹ de Internet, utilizando tecnologias de acesso à Internet de banda larga, bem como demonstra sua implementação através de software livre e as vantagens geradas por esta solução como: escalabilidade, redução de custo e redundância. Através do roteamento baseado na origem, pode ser feita a junção de *links* de prestadoras distintas, como por exemplo, um *link* dedicado com a TELEMAR e dois *links* de banda larga ADSL permitindo assim uma maior velocidade de acesso à Internet. Com a utilização de múltiplos *links* utilizados em paralelo, pôde-se constatar a grande vantagem obtida no aspecto de economia e de velocidade de acesso, não conseguido nas atuais tecnologias de banda larga, as quais são oferecidas com um limite baixo de velocidade.

Palavras-Chave: balanceamento de links, redundância entre conexões, viabilidade econômica, roteamento avançado, iproute2.

¹ Enlace para acesso a meios de telecomunicações

ABSTRACT

This work presents a solution of load balance of Internet links, using wide band access technologies to Internet, as well as to demonstrate your implementation through free software and the advantages generated by this solution, such as: scalability, cost reduction and redundancy. Through source based routing, it can be made the junction of links of different companies, as for instance, a link dedicated with TELEMAR and two links of wide band ADSL allowing a larger access speed to Internet. With the use of multiple links used in parallel, the great advantage could be verified obtained in the economy aspect and of access speed, not gotten in the current band technologies it releases, which are offered with a low limit of speed.

2.2	COMPARTILHAMENTO DE CONEXÃO	16
2.3	ROTEAMENTO	18
2.3.1	Roteamento Baseado em Origem	19
2.3.2	Política de Roteamento (Routing Policy Database)	20
2.3.3	Múltiplas Tabelas de Roteamento	22
2.4	IFTABLES	24
2.5	WEB PROXY CACHE	25
2.5.1	SQUID	25
2.6	ADSL	24
3	ANÁLISE DO PROBLEMA	26
3.1	ESTUDO DA VIABILIDADE ECONÔMICA DA SOLUÇÃO	27
3.1.1	Projeção de gastos e redução de custo	28
4	DESENVOLVIMENTO DA SOLUÇÃO PROPOSTA	31
4.1	CONFIGURAÇÃO DO AMBIENTE	32
4.2	COMPARTILHANDO A CONEXÃO COM O LINUX	33
4.3	IMPLEMENTANDO O BALANCEAMENTO DE LINHAS	35
4.4	PROBLEMAS NA IMPLEMENTAÇÃO	39
4.5	GARANTINDO A CONTINUIDADE DO SERVIÇO	41
5	ANÁLISE DOS RESULTADOS	42
6	CONCLUSÃO	46
	REFERÊNCIAS BIBLIOGRÁFICAS	47
	ANEXO I - RELATÓRIO GERADO PELO CALAMARIS	48
	ANEXO II - COMPILANDO O KERNEL	49
	APÊNDICE I - SCRIPT PARA COMPARTILHAMENTO DE CONEXÃO	54
	APÊNDICE II - SCRIPT PARA AUTENTICAÇÃO NA VELOX	57

SUMÁRIO

1	INTRODUÇÃO.....	12
1.1	OBJETIVOS	13
1.2	JUSTIFICATIVA.....	13
1.3	ORGANIZAÇÃO DO TRABALHO	15
2	REFERENCIAL TEÓRICO	16
2.1	INTERNET	16
2.2	COMPARTILHAMENTO DE CONEXÃO.....	16
2.3	ROTEAMENTO	19
2.3.1	Roteamento Baseado na Origem	19
2.3.2	Política de Roteamento (<i>Routing Policy Database</i>)	20
2.3.3	Múltiplas Tabelas de Roteamento	22
2.4	IPTABLES	22
2.5	WEB PROXY CACHE	23
2.5.1	SQUID	23
2.6	ADSL	24
3	ANÁLISE DO PROBLEMA	26
3.1	ESTUDO DA VIABILIDADE ECONÔMICA DA SOLUÇÃO	27
3.1.1	Projeção de gastos e redução de custo	28
4	DESENVOLVIMENTO DA SOLUÇÃO PROPOSTA	32
4.1	CONFIGURAÇÃO DO AMBIENTE	32
4.2	COMPARTILHANDO A CONEXÃO COM O LINUX.....	33
4.3	IMPLEMENTANDO O BALANCEAMENTO DE <i>LINKS</i>	35
4.4	PROBLEMAS NA IMPLEMENTAÇÃO	39
4.5	GARANTINDO A CONTINUIDADE DO SERVIÇO	41
5	ANÁLISE DOS RESULTADOS	42
6	CONCLUSÃO.....	46
	REFERÊNCIAS BIBLIOGRÁFICAS.....	47
	ANEXO I – RELATÓRIO GERADO PELO CALAMARIS	49
	ANEXO II - COMPILANDO O KERNEL.....	52
	APÊNDICE I - <i>SCRIPT</i> PARA COMPARTILHAMENTO DE CONEXÃO	54
	APÊNDICE II - <i>SCRIPT</i> PARA AUTENTICAÇÃO NA VELOX.....	57

LISTA DE FIGURAS

FIGURA 1 - EXEMPLO DE MÚLTIPLOS <i>LINKS</i> PARA ACESSO À INTERNET.....	14
FIGURA 2 - ESQUEMA DE NAT (<i>NETWORK ADDRESS TRANSLATOR</i>).....	17
FIGURA 3 – REPRESENTAÇÃO GRÁFICA DE COMPARTILHAMENTO DE CONEXÃO.....	18
FIGURA 4 - ESQUEMA DE <i>CACHE</i> DE PÁGINAS.....	24
FIGURA 5 - GRÁFICO GERADO PELO MRTG DE UTILIZAÇÃO DE UM LINK DE INTERNET	26
FIGURA 6 – GRÁFICO DE CUSTO MENSAL RELACIONADO À TABELA 3	29
FIGURA 7 – GRÁFICO DE CUSTO MENSAL RELACIONADO À TABELA 4	30
FIGURA 8 - GRÁFICO DE CUSTO MENSAL RELACIONADO À TABELA 5	31
FIGURA 9 - TOPOLOGIA LÓGICA DA REDE FARN	32
FIGURA 10 – TRÁFEGO DA INTERFACE ETH3	42
FIGURA 11 – TRÁFEGO DA INTERFACE ETH0	43
FIGURA 12 – TRÁFEGO DA INTERFACE ETH1	44
FIGURA 13- MEDIÇÃO DO TRÁFEGO DO LINK VELOX 1.....	45
FIGURA 14 - MEDIÇÃO DO TRÁFEGO DO LINK VELOX 2.....	45

LISTA DE TABELAS

TABELA 1 – ASSINATURA MENSAL DO SERVIÇO VELOX DA TELEMAR.....	28
TABELA 2 – ASSINATURA MENSAL DO SERVIÇO TC IP ACCESS CONNECT DA TELEMAR	28
TABELA 3 – DEMONSTRATIVO P/ REDUÇÃO DE UMA LP DE 512 KBPS P/ 128 KBPS.....	29
TABELA 4 – DEMONSTRATIVO P/ REDUÇÃO DE UMA LP DE 1 MBPS P/ 256 MBPS.....	29
TABELA 5 – DEMONSTRATIVO P/ REDUÇÃO DE UMA LP DE 2 MBPS P/ 512 KBPS	30
QUADRO 6 – EXIBINDO AS INTERFACES DE REDES	37
QUADRO 7 – VERIFICANDO AS ROTAS CRIADAS AUTOMATICAMENTE PELO SISTEMA	37
QUADRO 8 – VINCULANDO AS ROTAS ÀS TABELAS DE ROTAMENTO.....	38
QUADRO 9 – ADICIONANDO AS ROTAS ÀS TABELAS DE ROTAMENTO	38
QUADRO 10 – ADICIONANDO A ROTA PADRÃO PARA AS TABELAS DE ROTAMENTO	38
QUADRO 11 – CRIANDO O BALANÇAMENTO DE USUÁRIOS LINHAS	39
QUADRO 12 – HABILITANDO FRUIT TRANSPARENTE	39
QUADRO 13 – CONTROLANDO O ATRIBUTO IFCO-ETH0	40
QUADRO 14 – SCRIPT DE INICIALIZAÇÃO DO SERVIÇO.....	41

LISTA DE QUADROS

QUADRO 1 - COMANDO DE HABILITAÇÃO DE ROTEAMENTO	34
QUADRO 2 - COMANDOS PARA FAZER <i>MASQUERADING</i> NO FIREWALL.....	34
QUADRO 3 - CONTEÚDO DO ARQUIVO RT_TABLES	35
QUADRO 4 - COMANDO PARA LISTAR AS REGRAS DE ROTEAMENTO	36
QUADRO 5 - CRIANDO UMA NOVA TABELA DE ROTEAMENTO	36
QUADRO 6 - EXIBINDO AS INTERFACES DE REDES	37
QUADRO 7 - VERIFICANDO AS ROTAS CRIADAS AUTOMATICAMENTE PELO SISTEMA	37
QUADRO 8 - VINCULANDO AS ROTAS ÀS TABELAS DE ROTEAMENTO.....	38
QUADRO 9 - ADICIONANDO AS REGRAS ÀS TABELAS DE ROTEAMENTO	38
QUADRO 10 - ADICIONANDO A ROTA PADRÃO PARA AS TABELAS DE ROTEAMENTO.....	38
QUADRO 11 - CRIANDO O BALANCEAMENTO DE USO DOS LINKS.....	39
QUADRO 12 - HABILITANDO <i>PROXY</i> TRANSPARENTE	39
QUADRO 13 - CONTEÚDO DO ARQUIVO IFCFG-ETH0	40
QUADRO 14 - SCRIPT DE INICIALIZAÇÃO DO SERVIÇO.....	41

1 INTRODUÇÃO

Cada vez mais as empresas sentem necessidade de se conectarem à grande rede mundial de computadores, que é a Internet. Os motivos são bastante diversos, e os mais comuns são exploração comercial e necessidade de comunicação com o mundo.

No início as empresas somente podiam se ligar a provedores através de linhas discadas, com baixa velocidade de acesso ou através do que as operadoras de telefonia chamam de LP (linha privada), que é uma linha de dados dedicada, que não necessita de discagem para a conexão e se mantém ativa de forma ininterrupta. Normalmente, esta LP somente é oferecida pelas empresas de telecomunicações (Telecom). Agregado ao serviço de locação desta linha, a Telecom também oferece uma faixa de endereços de Internet (endereços IPs) públicos e fixos, permitindo assim que as empresas contratantes tenham condições de manter em sua estrutura, um conjunto de servidores para proverem os serviços disponíveis para a Internet (DNS, EMAIL, WEB, FTP, etc.).

Recentemente, foram disponibilizadas novas tecnologias para acesso à Internet, como por exemplo, as tecnologias de Internet banda larga, que é um serviço prestado a uma velocidade bem mais alta que via linha discada, mas com custos parecidos a esta última. As tecnologias mais utilizadas pela Internet banda larga são ADSL (*Asymmetric Digital Subscriber Line*) e Internet via TV a cabo, também conhecida como Internet a Cabo. Essas novas tecnologias possibilitam as empresas que possuem ligação à Internet através de LP, reduzirem a velocidade do *link* da LP, possibilitando assim uma queda no custo, e contratarem alternativas como, por exemplo, ADSL para que os usuários de sua rede interna passem a utilizar os serviços da Internet por meio deste *link* mais barato. Este esquema de ligação com a Internet traz um problema técnico, que é como fazer o roteamento do tráfego da rede utilizando dois ou mais *links*.

O roteamento é a principal forma utilizada na Internet para a entrega de pacotes de dados entre redes distintas. O modelo padrão de roteamento utilizado é o do salto-a-salto (*hop-by-hop*), onde cada roteador que recebe um pacote de dados, abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto, que é o roteador seguinte mais próximo do destino, e entrega-o como se o pacote desse um salto entre os roteadores.

Este processo se repete até o roteador mais próximo do destino, que é na verdade o *gateway*² de sua rede.

Quando se trata de *links* com a utilização de banda larga, ADSL ou Internet a Cabo, não é exigida a utilização de roteadores por parte do cliente, tendo em vista que os roteadores a serem utilizados ficam na operadora ou provedor de Internet.

Basicamente, um cliente da rede somente precisa saber quem é o seu *gateway*, que é a porta de saída para a Internet. Normalmente as redes são configuradas para acessarem por uma única saída. Caso haja uma perda de serviço desta saída, a rede inteira fica sem acesso. A idéia foi possibilitar que haja uma redundância entre múltiplos *links* e balanceamento entre eles, de forma que fique transparente para o usuário. Isto é, caso haja queda no serviço de acesso à Internet ou mesmo se um *link* estiver saturado, o sistema de forma automática faz o balanceamento.

Portanto, este trabalho demonstra a viabilidade da implantação desta solução, e mostra quais os benefícios que o uso do Balanceamento de *links* para o acesso à Internet pode proporcionar às diversas empresas que se utilizam da Internet via banda larga.

1.1 OBJETIVOS

O objetivo deste trabalho é apresentar a implementação de um esquema de balanceamento entre *links* para acesso à Internet, de forma automática e transparente para o usuário final. Além disso, é verificada a viabilidade econômica desta solução, haja visto que são utilizados vários *links* de baixo custo, como por exemplo, os utilizados com tecnologia ADSL ou Internet a Cabo.

1.2 JUSTIFICATIVA

O trabalho desenvolvido visa contribuir de forma significativa para comunidade e empresas que desejem baratear o custo de acesso à Internet. A solução criará uma nova possibilidade para empresas que procurem ligar-se à Internet.

² Ponte de saída da rede

Com a possibilidade de se criar um balanceamento entre *links* de acesso à Internet, o interessado poderá contratar vários *links* de baixo custo. Esse esquema possibilita uma velocidade maior para acesso à Internet, pois na medida em que o acesso fosse aumentando, o sistema distribuiria o acesso entre os vários *links*, mantendo assim os *links* balanceados, conforme apresentado na Figura 1.

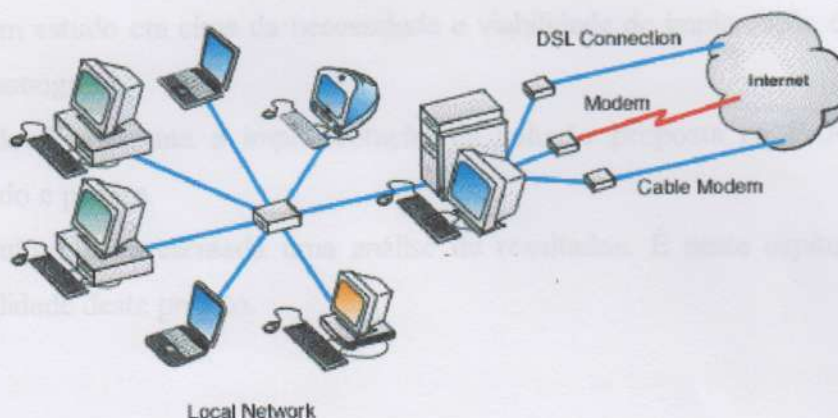


Figura 1 - Exemplo de múltiplos *links* para acesso à Internet

Outro ponto importante é a redundância entre os *links*, permitindo que a possibilidade de queda no acesso à Internet seja bem menor, pois quando houvesse falha em um dos *links*, os demais se manteriam em atividade. Além disso, no momento em que o sistema torne-se sobrecarregado, a empresa contrataria um novo *link* de acesso, que somado ao conjunto existente, diminuiria a sobrecarga.

Foi observado que existem inúmeras empresas que mantêm um *link* dedicado para prover serviços, mas que também permitem o acesso à Internet aos seus funcionários através deste mesmo *link*. Poderá ser observado em um capítulo mais adiante, um demonstrativo de preços dos *links* dedicados e de banda larga, permitindo uma real análise do gasto desnecessário com a utilização excessiva de linhas dedicadas. Com a implementação da solução proposta neste trabalho, busca-se garantir ganho de desempenho e redução de custo.

Assim, esta solução beneficia diversos segmentos de negócios, como por exemplo: *LAN Houses*, escolas, e quaisquer empresas que desejem aumentar o *link* de acesso à Internet a um baixo custo.

1.3 ORGANIZAÇÃO DO TRABALHO

Esta monografia está organizada da seguinte forma. O capítulo 2 apresenta o referencial teórico, abordando os conceitos e tecnologias utilizadas no desenvolvimento da solução aqui proposta.

O capítulo 3 é relativo ao início do desenvolvimento propriamente dito. Neste capítulo faz-se um estudo em cima da necessidade e viabilidade de implantação da solução proposta nesta monografia.

O capítulo 4 apresenta a implementação da solução proposta na FARN, como ambiente de estudo e prática.

No capítulo 5 é apresentada uma análise de resultados. É neste capítulo que se apresenta a viabilidade deste projeto.

Segundo Moura (1997, p.2), a Internet é uma coleção de redes interconectadas, e os pontos de ligação são os roteadores. Estes, por sua vez, estão organizados de forma hierárquica, onde alguns roteadores são utilizados apenas para trocar dados entre grupos de redes controlados pela mesma autoridade administrativa, enquanto outros roteadores também a comunicação entre as autoridades administrativas. A entidade que controla e administra um grupo de redes e roteadores chama-se Sistema Autônomo. O roteamento é o principal meio para que exista conectividade entre as diversas redes, que juntas formam a grande rede (Internet).

Apesar de a Internet ser uma rede onde a utilização de roteadores é de fundamental importância para o seu funcionamento, os usuários final ou empresas que não possuem rede dedicada, não necessitam adquirir roteadores para usufruir da Internet, podendo adquirir serviço de banda larga, que pode ser a tecnologia ADSL ou Internet a Cabo. (Moura, 1997).

1.2 COMPARTILHAMENTO DE CONEXÃO

Com a utilização de banda larga, se faz necessário compartilhar a conexão para que assim possa um maior número de usuários usufruir do acesso à Internet. Para tal, deve

2 REFERENCIAL TEÓRICO

O estudo realizado envolveu um conhecimento prévio do protocolo TCP/IP e roteamento, para a partir daí estudar e desenvolver uma solução envolvendo *softwares* livres como S.O. LINUX, e diversas ferramentas, tais como iptraf, mrtg, iproute2, netfilter, *softwares* baseados em licença GPL (licença pública geral). A seguir, são apresentados os conceitos que são necessários para que o leitor tenha um conhecimento básico dos assuntos envolvidos, a fim de obter um melhor entendimento do tema principal.

2.1 INTERNET

Segundo Moura (1997, p.2), a Internet é uma coleção de redes interconectadas, e os pontos de ligação são os roteadores. Estes, por sua vez, estão organizados de forma hierárquica, onde alguns roteadores são utilizados apenas para trocar dados entre grupos de redes controlados pela mesma autoridade administrativa, enquanto outros roteadores fazem também a comunicação entre as autoridades administrativas. A entidade que controla e administra um grupo de redes e roteadores chama-se Sistema Autônomo. O roteamento é o principal meio para que exista conectividade entre as diversas redes, que juntas formam a grande rede (Internet).

Apesar de a Internet ser uma rede onde a utilização de roteadores é de fundamental importância para o seu funcionamento, o usuário final ou empresas que não possuam *links* dedicados, não necessitam adquirir roteadores para usufruir da Internet, podendo adquirir serviço de banda larga, que pode ser a tecnologia ADSL ou Internet a Cabo. (Moura, 1997).

2.2 COMPARTILHAMENTO DE CONEXÃO

Com a utilização de banda larga, se faz necessário compartilhar sua conexão para que assim possa um maior número de usuários utilizar do acesso à Internet. Para tal, deve

ser utilizado algum equipamento conectado ao *modem cable/adsl*³, podendo ser um computador, que no caso deverá ter duas placas de rede, um modem que já venha com recursos de compartilhamento de conexão, ou um roteador, conforme representação da Figura 2. O equipamento utilizado deverá ter recurso de NAT (*Network Address Translator*). NAT é um esquema de tradução de endereços de rede que visa minimizar a escassez dos endereços IP, pois o crescimento da Internet tem sido grande e, para que uma máquina tenha acesso à rede, é preciso ter um endereço IP válido. O NAT está descrito na RFC⁴ 1631. (MOGUL, 2004).

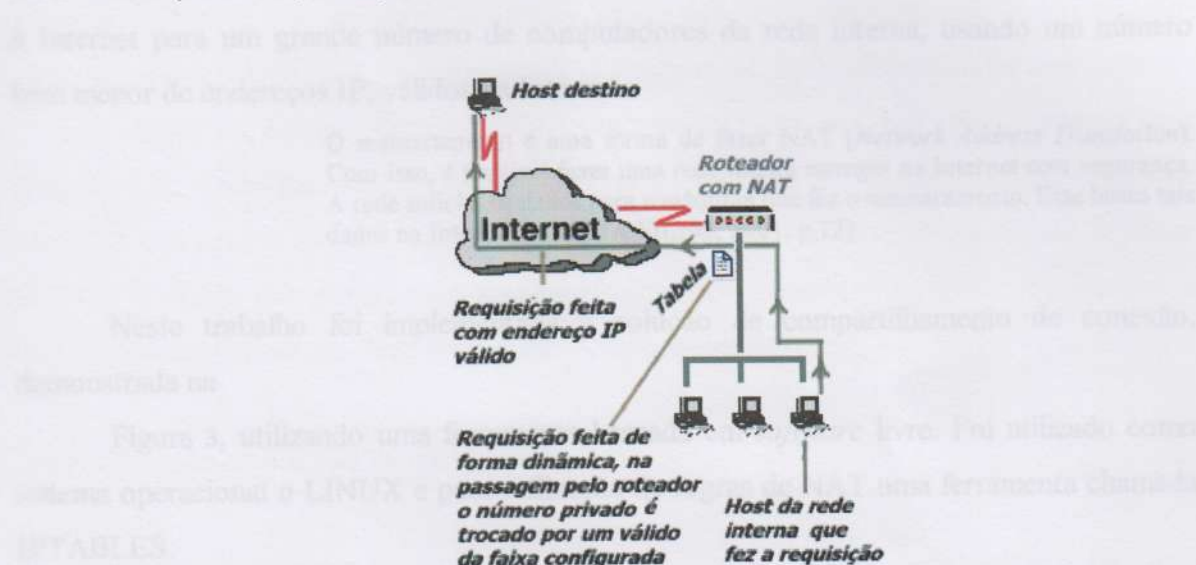


Figura 2 - Esquema de NAT (*Network Address Translator*)

O NAT é uma das soluções que existem para a economia de endereços IP e que permite que um computador, ou roteador com duas interfaces de rede, possa receber um endereço IP público, e compartilhá-lo a uma rede interna que estará ligada a segunda interface de rede. O NAT surgiu como uma alternativa real para o problema de falta de endereços IP na Internet. Cada computador que acessa a Internet deve ter o protocolo TCP/IP configurado. Para isso, cada computador da rede interna, precisaria de um endereço IP válido na Internet. Não haveria endereços IP suficiente. A criação do NAT veio para solucionar esta questão. Com o uso do NAT, os computadores da rede Interna, utilizam os

³ Equipamento utilizado para estabelecer conexão com acesso à Internet

⁴ *Request For Comments*, são notas de trabalho da comunidade de pesquisa e desenvolvimento da Internet;

chamados endereços privados. Os endereços privados não são válidos na Internet, isto é, pacotes que tenham como origem ou como destino, um endereço na faixa dos endereços privados, não serão encaminhados, serão descartados pelos roteadores. O software dos roteadores está configurado para descartar pacotes com origem ou destino dentro das faixas de endereços IP privados. As faixas de endereços privados são definidas na RFC 1597 e estão indicados a seguir: 10.0.0.0 até 10.255.255.255, 172.16.0.0 até 172.16.255.255, 192.168.0.0 até 192.168.255.255. (MOGUL, 2004).

De acordo com Mota Filho (2001), com o uso do NAT, a empresa fornece acesso à Internet para um grande número de computadores da rede interna, usando um número bem menor de endereços IP, válidos na Internet.

O mascaramento é uma forma de fazer NAT (*Network Address Translation*). Com isso, é possível fazer uma rede inteira navegar na Internet com segurança. A rede solicita os dados para a máquina que faz o mascaramento. Esse busca tais dados na Internet... (MOTA FILHO, 2001, p.12)

Neste trabalho foi implementada a solução de compartilhamento de conexão, demonstrada na

Figura 3, utilizando uma ferramenta baseada em *software* livre. Foi utilizado como sistema operacional o LINUX e para utilização de regras de NAT uma ferramenta chamada IPTABLES.

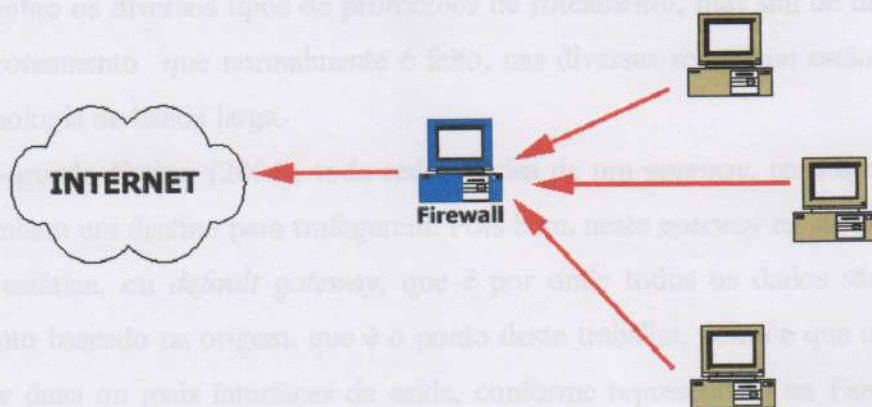


Figura 3 – Representação gráfica de compartilhamento de conexão

2.3 ROTEAMENTO

De acordo com Moura (1997, p.3), o roteamento é a principal forma utilizada na Internet para a entrega de pacotes de dados entre hosts (equipamentos de rede de uma forma geral, incluindo computadores, roteadores etc.). O modelo de roteamento utilizado é o do salto-por-salto (*hop-by-hop*), onde cada roteador que recebe um pacote de dados, abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto que vai deixar o pacote um passo mais próximo de seu destino e entrega o pacote neste próximo salto. Este processo se repete e assim segue até a entrega do pacote ao seu destinatário. No entanto, para que este funcione, são necessários dois elementos: tabelas e protocolos de roteamento.

Segundo Lyra e Torres (2004), um roteador em sua essência, é apenas uma máquina que recebe pacotes, toma alguma decisão com base neles e, finalmente, os repassa (ou não) adiante. No entanto, espera-se muito mais de um roteador do que apenas repassar pacotes. Funções que permitam o tráfego de diferentes protocolos⁵, filtros de pacotes e geração de estatísticas são desejáveis e até mesmo essenciais.

2.3.1 Roteamento Baseado na Origem

O roteamento por si só não é o ponto principal deste trabalho, já que não será tratado sobre os diversos tipos de protocolos de roteamento, mas sim de uma mudança do tipo de roteamento que normalmente é feito, nas diversas redes que estão ligadas a *links* com tecnologia de banda larga.

Segundo Freitas (2004), toda rede precisa de um *gateway*, para que os pacotes de dados tenham um destino para trafegarem. Pois bem, neste *gateway* existe o que é chamado de rota estática, ou *default gateway*, que é por onde todos os dados são enviados. No roteamento baseado na origem, que é o ponto deste trabalho, permite que um equipamento possa ter duas ou mais interfaces de saída, conforme representado na Figura 1, ligadas a provedores distintos e fazer a escolha de qual provedor será enviado o pacote de dados, independente de uma única rota padrão.

⁵ Regras padronizadas para comunicação de dados

De acordo com Hubert (2004), o roteamento baseado na origem é uma opção do protocolo IP (*Internet Protocol*), que se permite que defina a rota de saída para um determinado endereço origem, independente de uma rota padrão que é normalmente escolhida para toda uma rede. Lembremo-nos que normalmente um pacote de dados atravessa uma rede, e cada roteador poderá examinar o endereço IP de destino e escolher o próximo salto para direcionar o pacote de dados. No roteamento baseado na origem as decisões podem ser tomadas nos pacotes de origem.

Freitas (2002) afirma que o roteamento baseado na origem não é um tipo convencional de roteamento. É uma situação, em que exista mais de um provedor de Internet servindo a nossa rede local, e almeje-se que parte dessa rede utilize um dos provedores e a outra parte utilize o outro.

Freitas (2002) exemplifica o caso de uma instituição que possua dois *links* de acesso à Internet, um com a RNP e outro com a Embratel, podendo-se colocar um computador com o sistema operacional LINUX, com três interfaces de rede, uma conectada ao roteador com a RNP, outra conectada ao roteador com a EMBRATEL e a terceira conectada a rede local. Com o uso do roteamento baseado na origem, podem ser configuradas subredes na rede local, de forma que se configure a subrede 1 para ter acesso à Internet pela RNP e a subrede 2 para ter acesso à Internet pela EMBRATEL.

2.3.2 Política de Roteamento (*Routing Policy Database*)

Marsh (2000), afirma que os algoritmos clássicos de roteamento do protocolo TCP/IP usados, fazem suas decisões de roteamento baseadas somente no endereço IP de destino. Entretanto, podem-se distribuir pacotes IP dependendo não somente dos endereços de destino, mas também de outros campos do pacote tais como o endereço de origem, o protocolo do IP, as portas do protocolo de transporte, ou mesmo dados dentro do pacote. Este tipo de roteamento IP é conhecido como política de roteamento, "Routing Policy Database" ou RPDB, que seleciona a rota apropriada do endereço IP executando um conjunto de regras.

Marsh (2004), coloca a política de roteamento baseada no uso de três elementos: os endereços, as rotas e as regras. O endereço define a posição de um serviço, a rota define a

posição de um endereço e a regra define a posição de uma rota. Estes três elementos compreendem a estrutura em torno do qual a execução da política de roteamento é constituída. Através desta tríade é possível realizar o roteamento baseado na origem. A interação entre estes elementos fornece a flexibilidade e a complexidade, visto na política de roteamento. Para entender os detalhes da execução do roteamento é necessário compreender primeiramente a fundo cada elemento.

O primeiro elemento da tríade é o endereço. O endereço especifica basicamente o ponto de origem e destino ao qual a comunicação será estabelecida. Geralmente é observado o endereço de destino, que é o modo pelo qual o roteamento tradicional se baseia. No tratamento com a política de roteamento, são necessários ambos endereços, o de origem e o de destino. O segundo elemento da tríade é a rota. Quando se compara o roteamento tradicional com o roteamento em forma de política, se constata mais versatilidade e flexibilidade na especificação e nas opções do destino, com o roteamento em forma de política. Marsh (2004).

Um comando tradicional de roteamento permite que você especifique um *gateway* e algumas opções que permitam especificar controles sobre os pacotes que passam pelo roteador, como por exemplo negar a passagem de determinado pacote, de acordo com seu endereço. Marsh (2004).

Além do objeto padrão do *gateway* e todas as opções oferecidas pelo roteamento padrão, no esquema de roteamento baseado em política, uma rota pode fornecer a referência a um endereço que parte da origem. Pode-se considerar o elemento da rota da tríade da política de roteamento como uma versão avançada da estrutura tradicional de roteamento. Certamente, para as redes simples onde é fornecido o roteamento padrão, o funcionamento e a execução da política de roteamento reduzem-se à especificação tradicional. Marsh (2004).

O terceiro elemento da tríade é a regra. A regra permite que você especifique os filtros que combinam os pacotes. O filtro é parte do mecanismo da seleção da regra. Pode-se também usar regras para especificar outras opções, tais como *hosts* destino, e funções NAT. Usando uma regra pode se executar, por exemplo, a função da política de roteamento mais comum, que é a rota baseada pelo endereço de origem. Quando analisamos um

cenário onde um sistema que tenha somente uma tabela de roteamento, uma regra é aplicada sob circunstâncias limitadas. Marsh (2004).

Marsh (2004) descreve o endereço de origem como de um nível de importância tão relevante como o endereço de destino, neste processo de política de roteamento.

2.3.3 Múltiplas Tabelas de Roteamento

Marsh (2004) descreve que múltiplas tabelas de roteamento são normalmente utilizadas em sistemas que possuam roteadores, onde seja permitida a utilização de protocolos de roteamento que tenham poder de decisão para escolha de um melhor caminho, para o pacote ser roteado. Um exemplo é o protocolo OSPF (*open short path first*).

2.4 IPTABLES

Para a implementação deste trabalho de balanceamento de *links* é necessária uma ferramenta que permita uma definição de regras de tratamento de pacotes.

Segundo Freitas (2002), o IPTABLES é uma ferramenta, que é utilizada para definirmos regras especiais para entrada, saída e passagem de pacotes entre interfaces, podendo atuar antes ou após as ações referentes ao roteamento. Para filtragem de pacotes entre interfaces de rede, são utilizadas regras, que estão distribuídas em tabelas, que são:

1. **filter:** é a tabela padrão, sobre a qual são referidas três correntes de regras, ou *chains*: INPUT, pacotes que entram na interface; OUTPUT, pacotes que saem da interface e FORWARD, pacotes que estão sendo roteados de uma interface para outra;
2. **nat:** esta tabela se refere ao uso do recurso de *Network Address Translation* ou NAT, na qual são referidas as cadeias: PREROUTING, pacotes que serão alterados antes de roteamento; OUTPUT, pacotes locais que serão alterados antes do roteamento e POSTROUTING, pacotes que serão alterados após a aplicação das regras de roteamento;
3. **mangle:** usada para alterações especiais no pacote, PREROUTING, para alteração antes do roteamento e OUTPUT, pacotes locais que serão alterados antes do roteamento.

2.5 WEB PROXY CACHE

Segundo Stanger (2002), os servidores de *proxy* cache são implementados na camada de aplicativo e processam protocolos Internet específicos, tais como *Hypertext Transfer Protocol* (http) e *File Transfer Protocol* (FTP). São definidas regras no servidor *proxy* para determinar como um pedido de estação de trabalho deve ser processado.

Stanger (2002), diz que uma das principais tarefas de um servidor *proxy* é armazenar temporariamente páginas da *WEB* e arquivos de FTP para clientes *proxy*. Esses tipos de servidores *proxy* são chamados de servidores de cache *proxy*. O cache aumenta o desempenho da rede ao reduzir a quantidade de dados que são transferidos de fora da rede local.

Um dos benefícios dos servidores *proxy* é que o administrador do *proxy* pode acrescentar regras para filtrar conteúdo. Por exemplo, você pode filtrar pedidos de páginas da *WEB* que contenham certas palavras no endereço.

2.5.1 SQUID

Stanger (2002), afirma que SQUID é um *proxy-cache* de alta performance para clientes *WEB*, suportando protocolos FTP, GOPHER e HTTP. O SQUID mantém metadados e especialmente objetos armazenados na memória RAM, cacheia buscas de DNS e implementa cache negativo de *requests* falhos.

Segundo Bastos (2004), o SQUID suporta SSL, listas de acesso complexas e sistema de *login*. Por utilizar o *Internet Cache Protocol* (ICP), o SQUID pode ser configurado para trabalhar de forma hierárquica ou mista para melhor aproveitamento da banda.

Bastos (2004), diz que o SQUID consiste em um programa principal - SQUID, um sistema de busca e resolução de nomes - *DNS SERVER* - e alguns programas adicionais para reescrever requisições de páginas, fazer autenticação e gerenciar ferramentas de clientes.

A Figura 4 mostra um cenário de utilização do SQUID em uma rede de computadores.

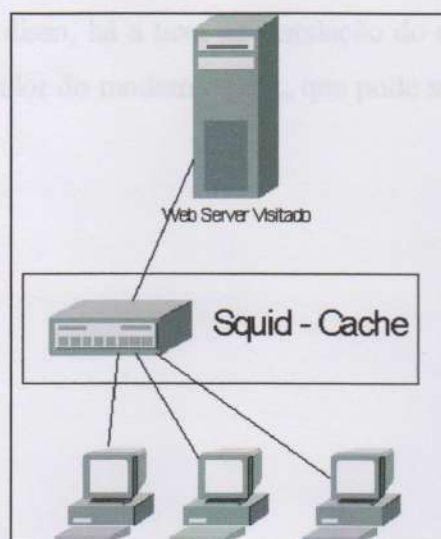


Figura 4 - Esquema de *cache* de páginas

2.6 ADSL

Segundo Monte (2000), ADSL (*Asymmetric Digital Subscriber Line*), que significa Linha Digital Assimétrica é uma das variações da tecnologia xDSL. Da mesma família são as siglas SDSL (*Symetric Digital Subscriber Line*), HDSL (*High-data-rate Subscriber Line*) e VDSL (*Very High Speed Digital Subscriber Line*).

Monte (2000), diz que essa tecnologia permite que voz e dados trafeguem juntos, em frequências diferentes, no mesmo par metálico da linha telefônica convencional, sem que o assinante pague mais pulsos telefônicos. Os dados seguem por faixas de frequência mais altas, enquanto a voz é transmitida pelas menores. Os dois são separados apenas na central da companhia telefônica. A voz vai para a rede IP da empresa de telefonia e os dados seguem para o provedor, que faz a interligação com o *backbone*⁶. A operadora de telefonia até teria condições técnicas de fazer a ligação direta entre o usuário e a Internet. No entanto, a ANATEL (Agência Nacional de Telecomunicações), proíbe que as concessionárias prestem esse tipo de serviço, que só é permitido aos provedores de acesso.

Monte (2000), ressalta que apesar de não pagar pulsos telefônicos, os assinantes ADSL têm outras despesas. Primeiro, a mensalidade do serviço que varia de acordo com a

⁶ Meio físico para interligação de redes

velocidade escolhida. Além disso, há a taxa de instalação do modem ADSL, a mensalidade do provedor de acesso e o valor do modem ADSL, que pode ser comprado ou alugado.

Principalmente questionou-se sobre a real utilização do *link* de Internet utilizado na FARN. Considerou-se que a utilização de uma LP, com disponibilidade de IP fixo, para acesso à Internet, seria inviável em termos econômicos, entretanto viável como uma possibilidade de montar em sua estrutura, um conjunto de servidores para proverem os serviços disponíveis para a Internet (DNS, EMAIL, WEB, FTP, etc.). Este tipo de circuito é caro, se comparado a tecnologias de baixo custo como a banda larga, por exemplo, que é oferecida por empresas de telefonia e TV a cabo.

Realizou-se um estudo de caso na FARN. Principalmente fez-se uma análise da utilização da Internet. Esta análise serviu para evidenciar a maior uso da LP como meio de acesso à Internet, gerando assim um prejuízo financeiro.

A análise foi realizada através de um monitoramento do *link* dedicado. Esta análise foi realizada com a utilização do protocolo SNMP (*simple network manager protocol*), utilizado com o software MRTG, através de monitoramento da interface serial do roteador ligado à LP. Os gráficos gerados permitem checar a utilização tráfego de entrada e saída. Como demonstra a Figura 3, o tráfego de entrada é representado pela cor verde, é basicamente tráfego relativo aos serviços locais pelos usuários da rede local da FARN.



Figura 3 - Gráfico gerado pelo MRTG de utilização de uma linha de Internet

O tráfego de saída representado em azul demonstra a utilização do tráfego oriundo da rede interna da FARN, do acesso do público externo à rede da FARN e o envio de mensagens do correio eletrônico, que saem do servidor de e-mail da FARN. Com este gráfico, conclui-se que a utilização de um *link* dedicado, para simples utilização do acesso à

3 ANÁLISE DO PROBLEMA

Primeiramente questionou-se sobre a real utilização do *link* de Internet utilizado na FARN. Considerou-se que a utilização de uma LP, com disponibilidade de IP fixo, para acesso à Internet, seria inviável em termos econômicos, entretanto viável como uma necessidade de manter em sua estrutura, um conjunto de servidores para proverem os serviços disponíveis para a Internet (DNS, EMAIL, WEB, FTP, etc.). Este tipo de circuito é caro, se comparado a tecnologias de baixo custo como a banda larga, por exemplo, que é oferecida por empresas de telefonia e TV a cabo.

Realizou-se um estudo de caso na FARN. Primeiramente fez-se uma análise da utilização da Internet. Esta análise serviu para evidenciar o maior uso da LP como meio de acesso à Internet, gerando assim um prejuízo financeiro.

A análise foi realizada através de um monitoramento do *link* dedicado. Esta análise foi realizada com a utilização do protocolo SNMP (*simple network manager protocol*), utilizado com o software MRTG, através de monitoramento da interface serial do roteador ligado à LP. Os gráficos gerados permitiram checar a utilização tráfego de entrada e saída. Como demonstra a Figura 5, o tráfego de entrada é representado pela cor verde. É basicamente tráfego relativo aos acessos feitos pelos usuários da rede local da FARN.

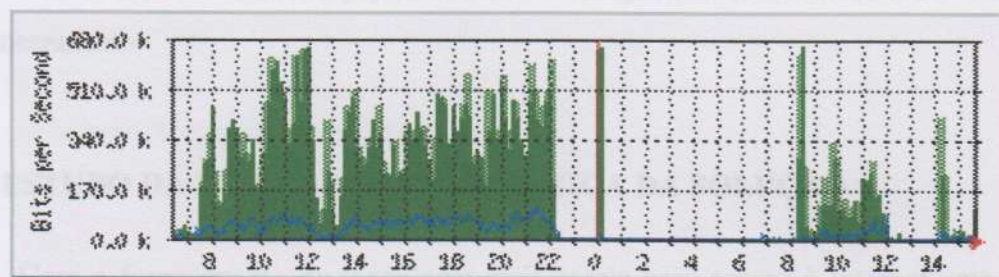


Figura 5 - Gráfico gerado pelo MRTG de utilização de um link de Internet

O tráfego de saída representado em azul demonstra a utilização do tráfego oriundo da rede interna da FARN, do acesso do público externo à rede da FARN e o envio de mensagens de correio eletrônico, que saem do servidor de e-mail da FARN. Com este gráfico, conclui-se que a utilização de um *link* dedicado, para simples utilização do acesso à

Internet, se torna caro para qualquer instituição, visto que, o maior tráfego é de acesso à Internet, demonstrado na Figura 5, podendo ser utilizada tecnologia de banda larga, oferecida por alguma operadora a um custo mais baixo.

Uma outra forma utilizada para analisar o tipo de tráfego utilizado no *link*, foi a utilização do software SQUID, que faz *cache* de páginas, juntamente com outro software chamado CALAMARIS, que faz uma análise dos endereços acessados por parte dos usuários da instituição. O CALAMARIS gera um relatório através de uma análise dos *logs*⁷ gerados pelo SQUID, podendo ser visto no Anexo I. Neste relatório gerado foram analisados os sites mais acessados, os tipos de arquivos baixados, enfim pôde-se fazer uma análise do tipo de utilização no *link* da FARN, para obter subsídios para uma tomada de decisão, para então chegar à conclusão do dimensionamento do *link* dedicado necessário para atender as necessidades da instituição, bem como os *links* de banda larga.

A primeira parte do problema estava resolvida. Bastou adquirir um *link* ADSL para poder implantar uma solução econômica. Com este novo *link*, foi possível separar a utilização da Internet em dois tipos de uso. O primeiro seria o acesso à Internet por parte dos usuários da rede, e o segundo seria o uso da LP, para prover os serviços disponíveis para a Internet (DNS, EMAIL, WEB, FTP, etc.).

O maior problema surgiria quando da necessidade de aumento da velocidade de acesso, visto que as operadoras oferecem o serviço de banda larga com limite de velocidade (a VELOX no caso é de 768 kbps). A solução foi adquirir mais um *link* ADSL e implantar o balanceamento.

3.1.1 Projeto de gateway e rede de acesso

3.1 ESTUDO DA VIABILIDADE ECONÔMICA DA SOLUÇÃO

Com o fornecimento de tecnologia mais barata para acesso à Internet, que no caso seria a chamada Internet banda larga, foi possível reduzir custos. A estratégia foi contratar um *link* ADSL, que passou a ser utilizado para acesso à Internet de uma forma geral. Com isso a banda utilizada no *link* dedicado ficou ociosa. A partir dos levantamentos feitos através de gráficos demonstrado nas figuras 11 e 12, pôde-se reduzir na FARN, de forma

⁷ Arquivos gerados para checagem dos acessos

segura, o *link* dedicado de 512 kbps para 128 kbps. Em setembro de 2003, o custo de um *link* dedicado de 512 kbps contratado à Diginet (provedor de Internet), com acesso a uma porta de Internet era R\$ 2500,00 (dois mil e quinhentos reais). De acordo com a Tabela 2, o custo na Telemar de um *link* de 512 kbps é de R\$ 3.984,12 (três mil novecentos e oitenta e quatro reais e doze centavos). A redução para 128 kbps permitiu uma economia de R\$ 1750,00 (mil setecentos e cinquenta reais), no *link* dedicado. Levando em consideração a necessidade de mais velocidade para acesso à Internet, foram contratados dois *links* ADSL de 768 kbps por R\$ 299,00 (duzentos e noventa e nove reais) cada um, conforme preços pesquisados na Telemar e descritos na Tabela 1.

Tabela 1 – Assinatura mensal do serviço Velox da Telemar*

Assinatura 256 Kbps	Assinatura 512 Kbps	Assinatura 768 Kbps
R\$ 164,61	R\$ 256,18	R\$ 299,00

Tabela 2 – Assinatura mensal do serviço TC IP ACCESS CONNECT da Telemar*

Velocidade	Valor do Acesso Local	Valor da Porta	Valor Total R\$
128 Kbps	R\$ 573,81	R\$ 896,49	R\$ 1.470,30
256 Kbps	R\$ 839,94	R\$ 1.578,38	R\$ 2.418,32
384 Kbps	R\$ 986,30	R\$ 2.550,74	R\$ 3.537,04
512 Kbps	R\$ 1.329,65	R\$ 2.654,47	R\$ 3.984,12
768 Kbps	R\$ 1.492,43	R\$ 2.701,36	R\$ 4.193,79
1 Mbps	R\$ 1.881,76	R\$ 3.009,96	R\$ 4.891,72
2 Mbps	R\$ 2.875,08	R\$ 4.407,67	R\$ 7.282,75

3.1.1 Projeção de gastos e redução de custo

Levando-se em conta que a utilização de um *link* em sua maior parte é para o tráfego de entrada, sobretudo em uma instituição de ensino cujo acesso é intenso por parte dos alunos e funcionários, e que a redução de um *link* dedicado na FARN, foi na ordem de 75%, ou seja, o *link* dedicado era de 512 kbps e foi reduzido para 128 kbps, e que a demanda fora suprida pela tecnologia ADSL, foi feito um demonstrativo nas tabelas Tabela

* Preços obtidos na TELEMAR em 15/11/2004

de quanto seria a economia para instituições que tenham *links* dedicados e queiram reduzir seus custos, usando a mesma proporcionalidade do estudo de caso aqui apresentado.

Tabela 3 – Demonstrativo p/ redução de uma LP de 512 kbps p/ 128 Kbps

SITUAÇÃO ATUAL	
Link dedicado de 512 Kbps	Custo atual: R\$ 3.984,12
SITUAÇÃO PLANEJADA	
Redução para um <i>link</i> de 128 Kbps:	R\$ 1.470,30
Acréscimo de um <i>link</i> de 512 Kbps (VELOX):	R\$ 256,18
	Custo total: R\$ 1.726,48
	Economia mensal: R\$ 2.257,64
	Economia anual : R\$ 27.091,68

O gráfico da Figura 6 é relacionado aos valores da Tabela 3 e demonstra a economia mensal, gerada com a redução de um *link* dedicado de 512 kbps para 128kbps e acréscimo de um link ADSL de 512kbps.

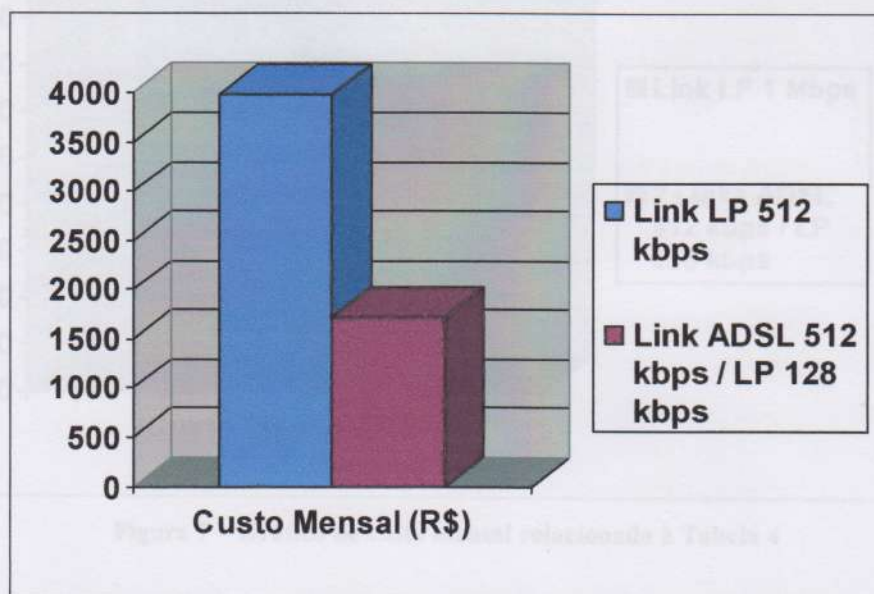


Figura 6 – Gráfico de custo mensal relacionado à Tabela 3

Tabela 4 – Demonstrativo p/ redução de uma LP de 1 Mbps p/ 256 Mbps

SITUAÇÃO ATUAL	
Link dedicado de 1 Mbps	Custo atual: R\$ 4.891,72
SITUAÇÃO PLANEJADA	
Redução para um link de 256 Kbps:	R\$ 2.418,32
Acréscimo de dois links de 512 kbps (VELOX):	R\$ 512,36
	Custo total: R\$ 2.930,68
	Economia mensal: R\$ 1.961,04
	Economia anual : R\$ 23.532,48

O gráfico da Figura 7 está relacionado aos valores da Tabela 4 e demonstra a economia mensal, gerada com a redução de um link dedicado de 1Mbps para 256kbps e acréscimo de dois links ADSL de 512kbps.

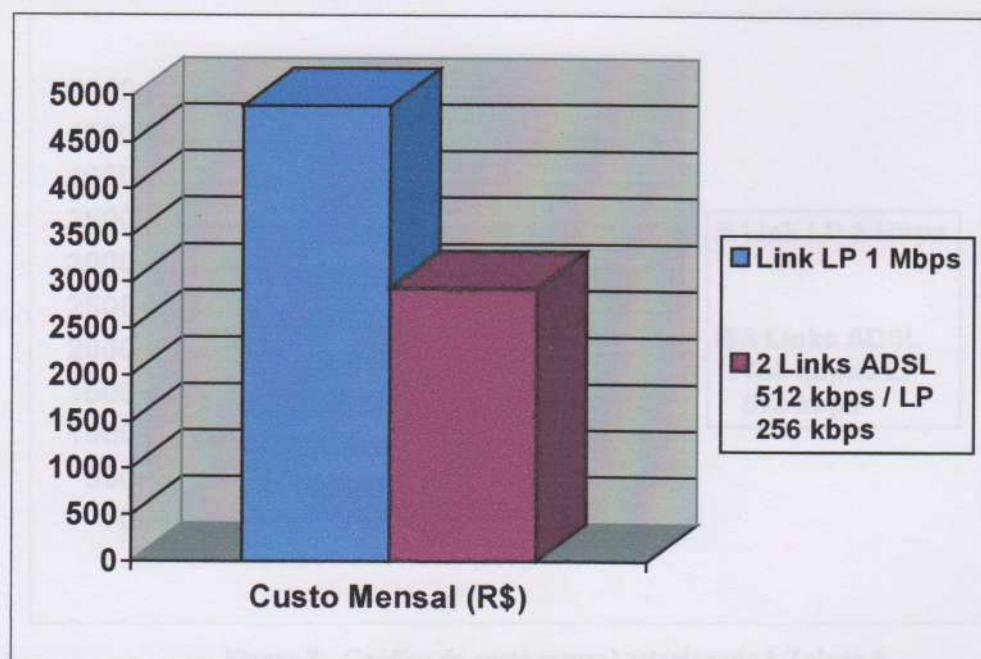


Figura 7 – Gráfico de custo mensal relacionado à Tabela 4

Tabela 5 – Demonstrativo p/ redução de uma LP de 2 Mbps p/ 512 Kbps

SITUAÇÃO ATUAL	
Link dedicado de 2 Mbps	Custo atual: R\$ 7.282,75
SITUAÇÃO PLANEJADA	
Redução para um <i>link</i> de 512 Kbps:	R\$ 3.984,12
Acréscimo de dois <i>links</i> de 768 Kbps (VELOX):	R\$ 897,00
	Custo total: R\$ 4.881,12
	Economia mensal: R\$ 2.401,63
	Economia anual: R\$ 28.819,56

O gráfico da Figura 8 está relacionado aos valores da Tabela 5 e demonstra a economia mensal, gerada com a redução de um *link* dedicado de 2 Mbps para 512Kbps e acréscimo de três *links* ADSL de 512kbps.

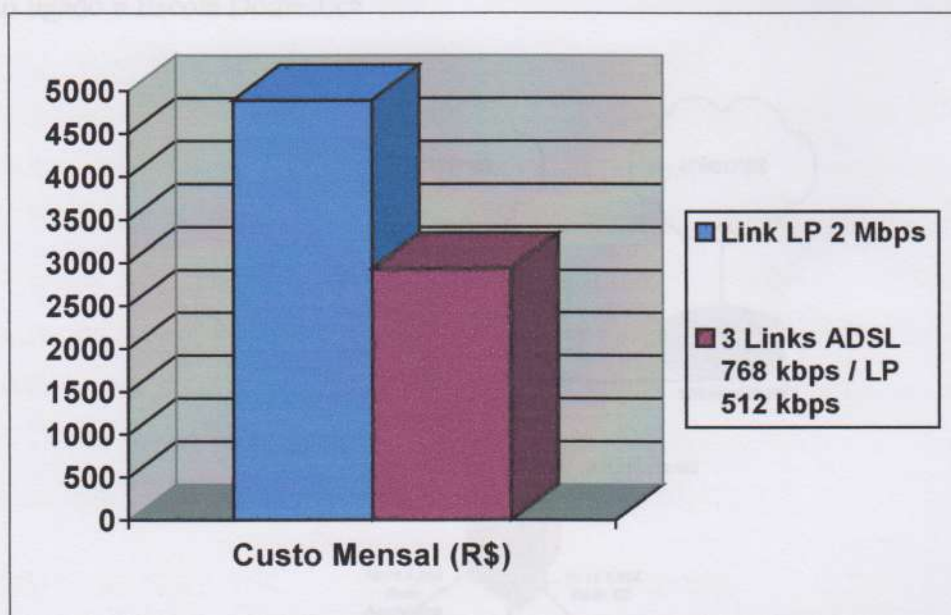


Figura 8 - Gráfico de custo mensal relacionado à Tabela 5

4 DESENVOLVIMENTO DA SOLUÇÃO PROPOSTA

Este capítulo apresenta a implementação da solução proposta na FARN, como ambiente de estudo e prática.

4.1 CONFIGURAÇÃO DO AMBIENTE

A Figura 9 representa um computador com um processador Pentium II 400, 512 Mb de memória e 40 Gb de disco padrão IDE, funcionando como um *firewall*⁸, com o sistema operacional LINUX instalado e com 5 placas de rede 10/100 Mbps. Existem três *links* ligando a rede interna, que é separada em três segmentos. O segmento acadêmico que corresponde aos laboratórios de informática e núcleos de pesquisa, o segmento administrativo que corresponde aos departamentos administrativos da instituição, e o segmento ligado à Escola Doméstica.

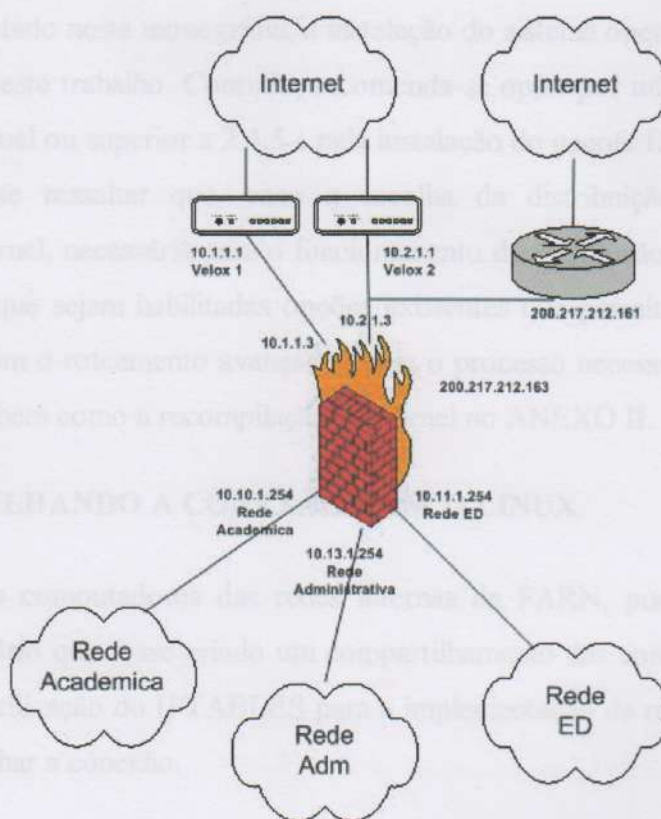


Figura 9 - Topologia lógica da Rede FARN

⁸ É uma máquina ou ativo de rede configurado para filtrar tráfego indesejado.

As ligações de saída se dão através de três *links*, dois ligados a modems ADSL D-Link 502G, que estão configurados para operarem como roteadores e são utilizados como *gateways default*, e um terceiro *link* ligado ao segmento do servidor WEB da FARN e roteador Cisco série 1600 que está conectado a uma LP.

O LINUX foi o sistema operacional utilizado, tendo como distribuição o Fedora Core 2, com a versão de *kernel*⁹ 2.6.5-1.358. O sistema operacional LINUX está disponível sob a forma de diversas distribuições. Para os propósitos desta monografia, qualquer distribuição baseada em Kernel da série 2.4, com os pacotes iptables e iproute2 poderia ser empregada. O Fedora Core 2 vem com o Kernel na versão 2.6 e o iptables, e com toda configuração necessária para o funcionamento de roteamento avançado, previamente configurada no kernel. No ANEXO II pode ser vista a descrição da otimização necessária do kernel, para os propósitos de operação de um computador com LINUX, com funções de um roteador no modo avançado.

Não será tratado nesta monografia, a instalação do sistema operacional LINUX, pois fugiria do escopo deste trabalho. Contudo, recomenda-se optar por uma distribuição com a versão do Kernel igual ou superior a 2.4.5 e pela instalação do pacote IPTABLES.

É importante ressaltar que, caso a escolha da distribuição não tenha prévia configuração do kernel, necessária para o funcionamento desta solução, o kernel deverá ser recompilado, para que sejam habilitadas opções existentes que permitam a atuação de um servidor LINUX com o roteamento avançado. Veja o processo necessário para escolha das opções necessárias bem como a recompilação do kernel no ANEXO II.

4.2 COMPARTILHANDO A CONEXÃO COM O LINUX

Para que os computadores das redes internas da FARN, pudessem ter acesso à Internet, foi necessário que fosse criado um compartilhamento das conexões de saída. Para isso, foi preciso a utilização do IPTABLES para a implementação de regras de NAT com o intuito de compartilhar a conexão.

⁹ Núcleo do sistema operacional

Para que fosse feito o compartilhamento, foram implementadas regras que se chamam *Masquerading*. Regras de *Masquerading* são utilizadas quando uma máquina atua como um *gateway* entre a Internet e a Rede Local, alterando os pacotes, de modo que ele vá para o lugar certo, e retorne para o lugar em que saiu. Um jeito bem simples de se compartilhar a sua conexão, considerando que a rede local da FARN é composta de endereços IPs privados.

No caso da solução que estou apresentando, tive que implementar esta regra de *masquerading* para cada interface de rede ligada a um *link* de saída, cito as interfaces *eth0* e *eth1* ligadas a *links* ADSL, e ao segmento do roteador que está conectado a uma LP.

Para habilitar a função de roteamento na máquina LINUX, foi habilitada a função *IP Forwarding* do *kernel* do LINUX. O comando para habilitar o roteamento está descrito no Quadro 1.

Quadro 1 - Comando de habilitação de roteamento

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

O passo seguinte foi habilitar um módulo do *kernel* que permite o *masquerading* e a aplicação das regras necessárias, para que as máquinas da rede interna pudessem navegar pela Internet. Os comandos para habilitar o mascaramento estão descritos no Quadro 2.

Quadro 2 - Comandos para fazer *masquerading* no Firewall

```
modprobe iptables_nat  
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE  
/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

O comando descrito na primeira linha do Quadro 2 habilita a função de NAT, para que possa existir o compartilhamento de conexão. Os demais comandos habilitam o mascaramento nas interfaces *eth0* e *eth1*, fazendo com que os pacotes que saiam através das interfaces *eth0* e *eth1*, estejam mascarados pelo endereço correspondente a interface de saída.

No APÊNDICE I, está descrito um *script* básico que implementa a solução de compartilhamento de conexão.

4.3 IMPLEMENTANDO O BALANCEAMENTO DE LINKS

Para se criar um balanceamento de *links*, foi necessário utilizar a ferramenta IPROUTE2. Esta ferramenta fornece opções avançadas de roteamento, possibilitando rotear os pacotes pela origem e definir a carga nos *links* de saída, tornando possível o balanceamento de *links*. O IPROUTE2 pode ser encontrado pelo endereço <ftp://ftp.inr.ac.ru/ip-routing/>.

A distribuição utilizada já possuía a ferramenta IPROUTE2, portanto não foi preciso instalá-la. Existe um diretório `/etc/iproute2` no qual contém o arquivo de configuração `rt_tables`. É nesse arquivo onde são definidas as tabelas de roteamento. Originalmente o arquivo `rt_tables` tem o conteúdo apresentado conforme o Quadro 3.

Quadro 3 - Conteúdo do arquivo `rt_tables`

```
#
# reserved values
#
255    local
254    main
253    default
0      unspec
#
# local
#
#1     inr.ruhep
```

Cada número representa uma tabela de roteamento, a tabela principal é a tabela *main* com o número 254. O *Kernel* utiliza três tabelas iniciais:

- **local**: identificada no Kernel por 255. É associada com a regra de prioridade 0, possui rotas para endereços locais e de *broadcast*, tal regra não pode ser alterada;
- **main**: identificada no Kernel por 254. É associada com a regra de prioridade 32766, possui as demais rotas normais do sistema, sem envolver quaisquer políticas especiais de roteamento, podendo ser alterada livremente pelo administrador, ou até apagada;

- **default:** identificada no Kernel por 253. É associada com a regra de prioridade 32768, por padrão está vazia, é reservada para alguma atividade de pós-processamento, se o pacote não foi selecionado por nenhuma das tabelas iniciais.

Através do comando **ip rule list** pode-se verificar as regras padrão conforme Quadro 4.

Quadro 4 - Comando para listar as regras de roteamento

```
[root@firewall root]# ip rule list
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default
```

Não foi necessário fazer qualquer alteração na tabelas existentes. Entretanto, foi necessário criar duas novas tabelas de roteamento, como pode ser visto nos comandos descritos no Quadro 5.

Quadro 5 - Criando uma nova tabela de roteamento

```
echo "10    velox1" >> /etc/iproute2/rt_tables
echo "20    velox1" >> /etc/iproute2/rt_tables

cat /etc/iproute2/rt_tables
#
# reserved values
#
255    local
254    main
253    default
0      unspec
#
# local
#
# 1    inr.ruhep
10     velox1
20     velox2
```

As tabelas de roteamento criadas, foram utilizadas como rotas de saída da rede e para balanceamento. As demais rotas das redes que estão ligadas diretamente às interfaces, foram criadas automaticamente e atribuídas à tabela *main*. Sempre que se ativa uma interface de rede, a rota para essa rede é automaticamente configurada e associada à tabela *main*.

Através do comando *ip link show*, verifica-se as interfaces de rede utilizadas, conforme demonstrado no Quadro 6.

Quadro 6 - Exibindo as interfaces de redes

```
[root@firewall1 init.d]# ip link show
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
    link/ether 00:00:1c:db:13:c6 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
    link/ether 00:50:bf:0e:69:68 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
    link/ether 00:e0:7d:ac:c6:d4 brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
    link/ether 00:50:bf:0e:62:2e brd ff:ff:ff:ff:ff:ff
6: eth4: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
    Link/ether 00:00:b4:32:83:71 brd ff:ff:ff:ff:ff:ff
```

O comando *ip route list tables main* é utilizado para checar as rotas criadas automaticamente pelo sistema. O resultado deste comando pode ser visto no Quadro 7.

Quadro 7 - Verificando as rotas criadas automaticamente pelo sistema

```
[root@firewall1 init.d]# ip route list table main
200.217.212.160/29 dev eth1 proto kernel scope link src
200.217.212.163
10.2.1.0/24 dev eth1 scope link
10.10.1.0/24 dev eth2 scope link
10.1.1.0/24 dev eth0 scope link
10.13.1.0/24 dev eth3 scope link
10.11.1.0/24 dev eth4 scope link
```

```
127.0.0.0/8 dev lo scope link
```

O próximo passo foi vincular as rotas às tabelas. Nesse passo é informado para a tabela, qual o roteador é utilizado para determinado IP de origem. O comando ip com o objeto route foi utilizado, como pode ser visto no Quadro 8.

Quadro 8 - Vinculando as rotas às tabelas de roteamento

```
ip route add 10.1.1.0/24 dev eth0 src 10.1.1.3 table velox1
ip route add 10.2.1.0/24 dev eth1 src 10.2.1.3 table velox2
```

As interfaces eth0 e eth1 estão ligadas diretamente a modems ADSL.

A seguir, foram adicionadas as regras às novas tabelas de roteamento, criadas utilizando o comando ip com o objeto rule. Neste ponto os vínculos entre as tabelas e as interfaces foram criados, informando que elas deverão rotear. Os comandos para criar regras de roteamento estão descritos no Quadro 9.

Quadro 9 - Adicionando as regras às tabelas de roteamento

```
ip rule add from 10.1.1.3 table velox1
ip rule add from 10.2.1.3 table velox2
```

Após adicionar as rotas às tabelas de roteamento, foi preciso adicionar as rotas padrão para as tabelas criadas, conforme demonstrado no Quadro 10.

Quadro 10 - Adicionando a rota padrão para as tabelas de roteamento

```
ip route add default via 10.1.1.1 table velox1
ip route add default via 10.1.2.1 table velox2
```

|_____|
 |
 ip do gateway

|_____|
 |
 tabela de roteamento

Após criadas as rotas padrão e vinculá-las as tabelas velox1 e velox2, o passo seguinte foi balancear os links. Para que o balanceamento possa ser feito, é necessário que

esteja habilitada a seguinte opção no kernel do sistema operacional: CONFIG_IP_ROUTE_MULTIPATH=y. Os comandos necessários para o balanceamento estão descritos no Quadro 11.

Quadro 11 - Criando o balanceamento de uso dos links

```
ip route add default equalize \
  nexthop via 10.1.1.1 dev eth0 weight 1 \
  nexthop via 10.2.1.1 dev eth1 weight 1
```

Através do parâmetro equalize é feito o balanceamento entre as interfaces de rede, a opção weight determina o peso atribuído para cada link. Este peso determina a quantidade de conexões que serão estabelecidas em cada link. Como os dois links tem a mesma velocidade, foram atribuídos pesos iguais.

4.4 PROBLEMAS NA IMPLEMENTAÇÃO

Durante a implementação desta solução houve um problema com o *proxy* SQUID. O SQUID é utilizado para fornecer *cache* de páginas, e sempre requer as páginas através de uma rota padrão. Foram utilizadas regras com o IPTABLES para redirecionar o tráfego destinado a porta¹⁰ 80 do protocolo TCP para porta 3128. A porta 3128 é a porta padrão do SQUID. Este redirecionamento foi feito para se criar um *proxy* transparente. A descrição do redirecionamento é vista no Quadro 12.

Quadro 12 - Habilitando *proxy* transparente

```
iptables -t nat -A PREROUTING -i eth2 -s 0/0 -p tcp -d ! 200.217.212.162
  --dport 80 -j REDIRECT --to-ports 3128

iptables -t nat -A PREROUTING -i eth3 -s 0/0 -p tcp -d ! 200.217.212.162
  --dport 80 -j REDIRECT --to-ports 3128

iptables -t nat -A PREROUTING -i eth4 -s 0/0 -p tcp -d ! 200.217.212.162
  --dport 80 -j REDIRECT --to-ports 3128
```

¹⁰ Termo utilizado para referenciar o número de conexão de algum tipo de serviço (WEB, FTP, etc).

Com os comandos no Quadro 12, todo o tráfego destinado para a porta 80 do protocolo TCP foi redirecionado para a porta 3128. A partir daí, as solicitações das páginas passaram a ser feitas pelo SQUID, portanto as conexões WEB partem da máquina *proxy* que por sua vez redireciona para as máquinas requerentes, que estão na rede interna. O SQUID utiliza o *gateway* padrão para buscar as páginas. As regras necessárias para o balanceamento de link foram implementadas, mas o *gateway* que estava especificado no arquivo `/etc/sysconfig/network-scripts/ifcfg-eth0`¹¹ foi mantido, o que ocasionou um conflito de *gateways*. Foi percebido que o balanceamento deixava de funcionar quando se usava o *proxy*. Quando o tráfego era direcionado para o *proxy*, somente havia passagem de pacotes por uma interface, que era a interface marcada como *gateway* padrão no arquivo `ifcfg-eth0`.

A solução foi desabilitar a opção *gateway* do arquivo `ifcfg-eth0` e verificar se no arquivo `/etc/sysconfig/network` (arquivo de configuração de parâmetros de rede), não havia referencia a nenhum *gateway*. A partir daí, deixou de existir conflito com a implementação do *gateway default* realizada pelo `iproute2`. O *gateway default* criado pelo `IPROUTE2` apontava para duas saídas de forma simultânea.

Neste diretório `/etc/sysconfig/network-scripts` estão as configurações de rede, incluindo os endereços IP correspondentes às placas de rede. No Quadro 13 está listado o conteúdo do arquivo `ifcfg-eth0`.

Quadro 13 - Conteúdo do arquivo `ifcfg-eth0`

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.1.1.255
IPADDR=10.1.1.3
NETMASK=255.255.255.0
NETWORK=10.1.1.0
#GATEWAY=10.1.1.1
ONBOOT=yes
```

¹¹ Os arquivos que iniciem com `ifcfg-eth` contidos no diretório `/etc/sysconfig/network-scripts`, correspondem a arquivos de configuração das interfaces de rede.

A linha com a opção GATEWAY precisou ser comentada para que não fosse assumido nenhum *gateway* padrão.

O problema foi solucionado e o SQUID passou a reconhecer as duas saídas como *gateway* padrão.

4.5 GARANTINDO A CONTINUIDADE DO SERVIÇO

O balanceamento foi implementado entre dois *links* ADSL através do produto VELOX da TELEMAR. Foi utilizado um *script*¹² para monitorar e garantir a continuidade da conexão destes *links*. A cada cinco minutos este *script* é executado. O *script* está demonstrado no Quadro 14.

Quadro 14 - Script de inicialização do serviço

```
#!/bin/bash
route add -host 200.165.104.14 gw 10.1.1.1
/etc/ppp/velox.sh
route del -host 200.165.104.14 gw 10.1.1.1
route add -host 200.165.104.14 gw 10.2.1.1
/etc/ppp/velox.sh
Route del -host 200.165.104.14 gw 10.2.1.1
```

O *script* descrito no Quadro 14, adiciona uma rota para o *host* 200.65.104.14 (endereço do site de autenticação do veloxzone), vincula este endereço à interface correspondente ao primeiro *link* velox que se quer checar, executa o *script* velox.sh (responsável por verificar o *status* do *link* e fazer a autenticação, caso seja necessário), remove a rota criada e faz o mesmo procedimento com o segundo *link*.

A listagem completa do *script* velox.sh pode ser vista no APÊNDICE II.

¹² Arquivo de lote para execução de comandos.

5 ANÁLISE DOS RESULTADOS

Para apresentar os resultados deste trabalho, foram utilizadas ferramentas que comprovam a passagem de tráfego nas interfaces de rede que estão ligadas aos modens ADSL, que são os *links* de saída da rede.

Através do aplicativo IPTRAF, pode-se ver de forma gráfica o tráfego passante nas interfaces em questão.

Para demonstração dos resultados, foram realizados *downloads* de alguns arquivos, com um computador conectado ao segmento da rede interna cujo endereço IP é 10.13.1.25. Na Figura 10, podem ser verificadas, conexões estabelecidas tendo como origem o endereço IP 10.13.1.25 apontado por uma seta vermelha e como destino os endereços 143.107.253.20, 143.107.253.167, 200.137.5.10, e 212.143.22.110, apontados por setas amarelas.

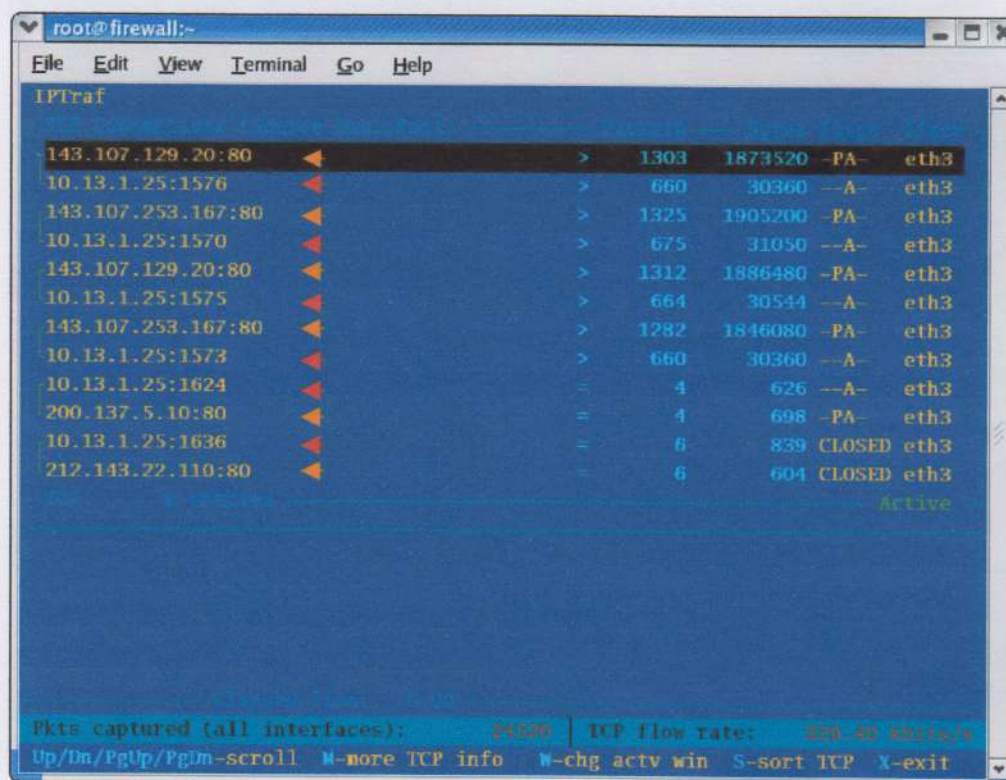


Figura 10 – Tráfego da interface eth3

Observa-se o tráfego passante nas interfaces eth0 e eth1 conforme figuras 11 e 12, capturado no momento do *download* feito pela máquina com o IP 10.13.1.25, representada na Figura 10. Essas interfaces estão conectadas respectivamente aos *links* de saída velox1 e velox2. Nestas figuras, as setas amarelas indicam os endereços de destino, que correspondem aos endereços conectados ao endereço de origem 10.13.1.25.

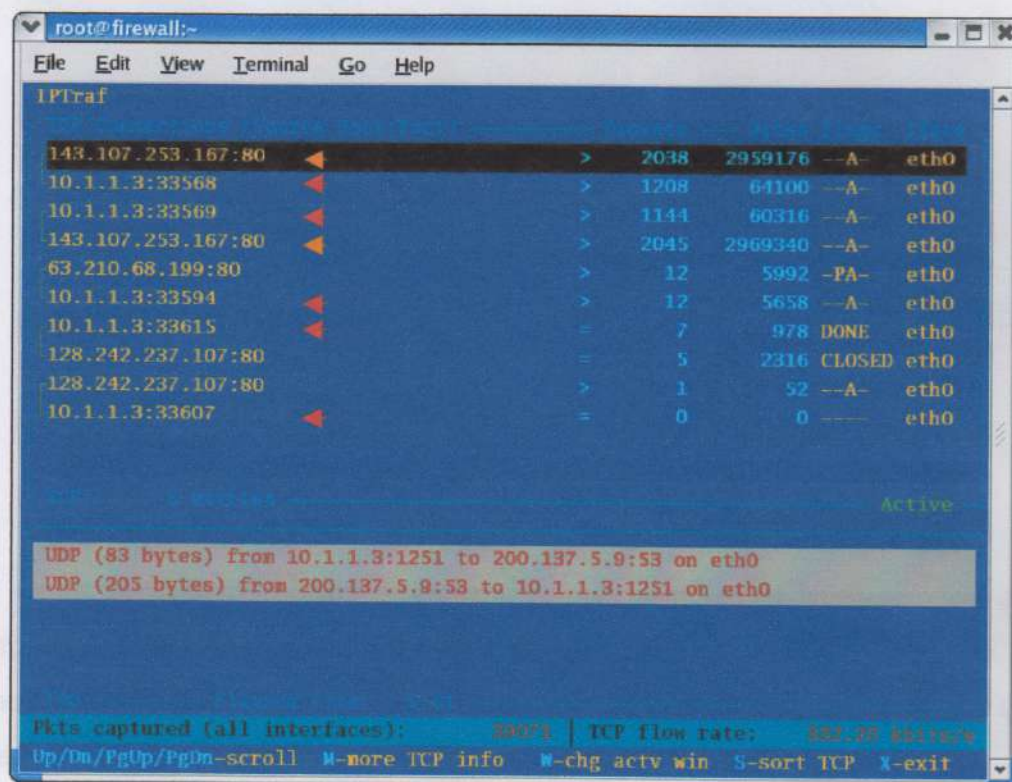


Figura 11 – Tráfego da interface eth0

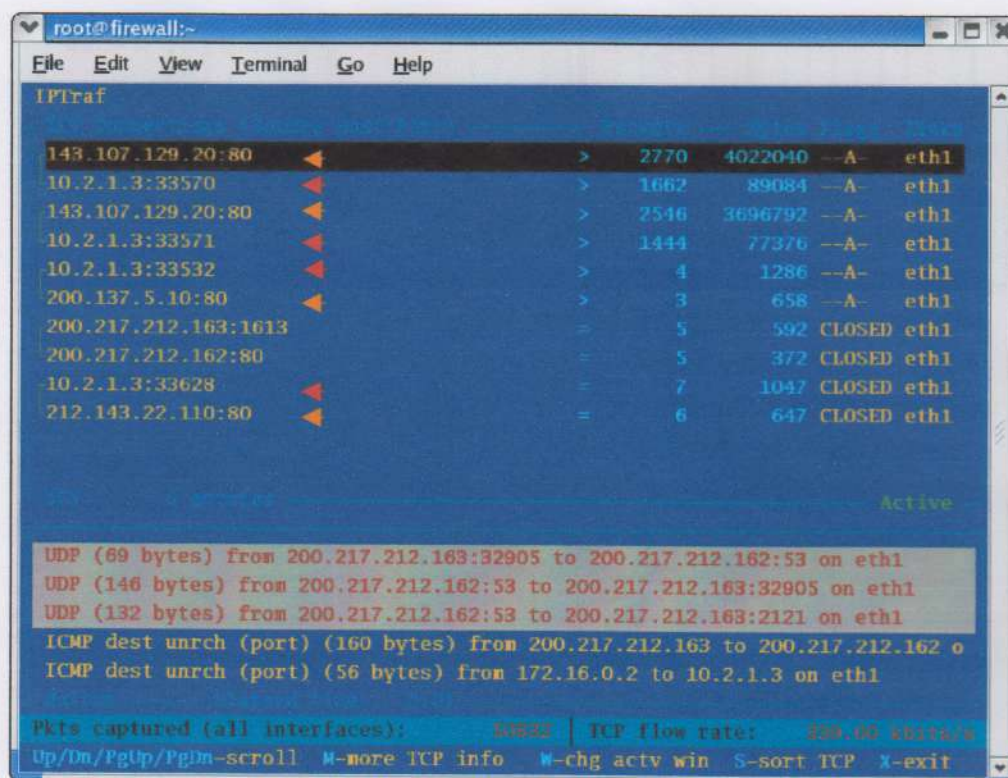


Figura 12 – Tráfego da interface eth1

Outra forma utilizada para demonstrar o funcionamento do balanceamento entre os *links*, foi através da medição do tráfego da rede com o programa MRTG. As figuras 13 e 14 demonstram que existe tráfego nas duas interfaces de saída no mesmo horário, o que nos levou a concluir a existência do balanceamento entre os links.

Observando os gráficos das figuras 13 e 14, evidencia-se que não são idênticos. Identifica-se por exemplo, que às 14:00 hs, o gráfico do link velox 1 está indicando mais tráfego do que o link velox 2. Isto por que a divisão do tráfego não se dá por quantidade de dados trafegados e sim por distribuição de conexões. Quando por exemplo é feito um *download* de um arquivo, é estabelecida uma conexão entre a origem e o destino, e o tráfego deste *download* passará somente pela interface ao qual a conexão iniciou. Uma próxima conexão estabelecida pode ser de uma consulta a WEB, essa conexão será destinada ao próximo *gateway*.

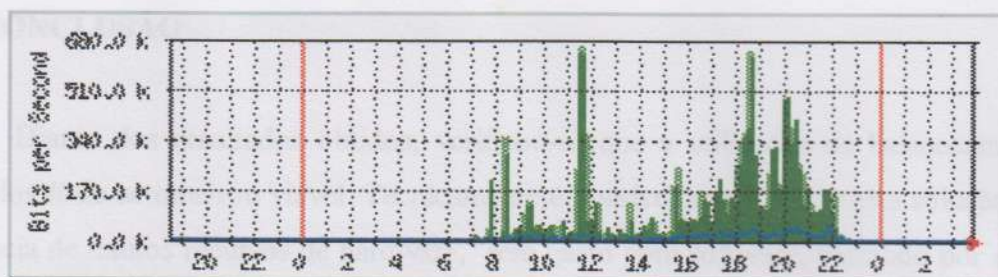


Figura 13- Medição do tráfego do link velox 1

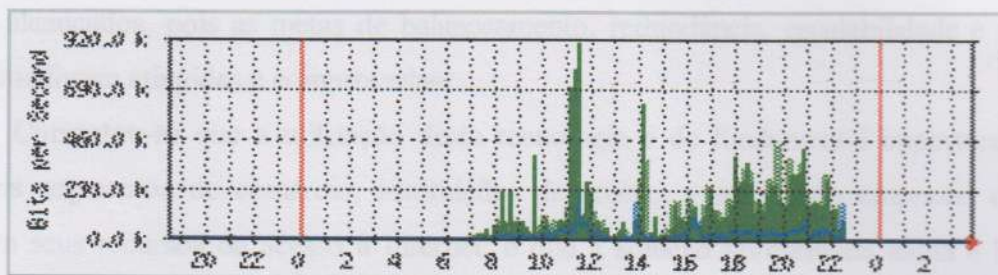


Figura 14 - Medição do tráfego do link velox 2

6 CONCLUSÃO

Diante dos resultados obtidos, verificou-se que a utilização de balanceamento de múltiplos *links* se mostrou viável. Tecnicamente é possível implementar esta solução, sem a exigência de muitos recursos de hardware, sem gasto com software, bastando por exemplo uma máquina Pentium com processador 166 e a utilização de *software* livre. Os objetivos foram alcançados, pois as metas de balanceamento, redundância, escalabilidade e redução de custos foram atingidas e comprovadas.

Constatou-se que a utilização desta tecnologia é de fundamental importância para diversos segmentos de comércio, instituições de ensino, e sobretudo empresas que mal utilizam seus recursos de acesso à Internet, e que a solução apresentada ainda é bastante desconhecida por parte das empresas e demais segmentos, que se beneficiariam com a implementação da mesma.

Foi visto no presente trabalho o uso de roteamento avançado com LINUX, onde foram demonstrados os benefícios oferecidos por esta solução. Embora tenha se explicado neste trabalho como se balancear *links*, o objetivo principal do mesmo era o de apresentar a solução e mostrar sua viabilidade. Os comandos utilizados restringiram-se a mostrar o básico do roteamento avançado, para simplesmente atingir as metas traçadas no projeto desta monografia. Entretanto, existe uma série de recursos e comandos de roteamento avançado utilizando-se LINUX, não apresentados nesta monografia que podem ser explorados.

Almeida, João Eriberto. Firewall no Linux (publica, 2001). Disponível em: <<http://www.pfSense.org.br/>>. Acesso em 27/05/2004.

Monra, A. S. Roteamento: O que é importante Saber. RNP - Rede Nacional de Ensino e Pesquisa. Revista NovaGeneration, v.1, n.1, 1997. Disponível em: <<http://www.rnp.br/nova/gen/9705/n1-1.html>>. Acesso em 25/04/2004.

Stamper, James. Rede Segura Linux, 1. ed. Rio de Janeiro: Alta Books, 2002.

REFERÊNCIAS BIBLIOGRÁFICAS

Bastos, Eri Ramos. Configurando um Squid. Disponível em: <<http://www.linuxman.pro.br/squid/#toc2>>. Acesso em 14/07/2004.

Freitas, Allan Edgard Silva. Roteamento avançado com linux . Disponível em: <http://www.rnp.br/newsgen/0201/roteamento_linux.html>. Acesso em: 20/04/2004

Hubert, Bert. Linux Advanced Routing & Traffic Control HOWTO. Disponível em: <<http://lartc.org/howto/index.html>>. Acesso em: 20/04/2004.

Lyra, Christian; Torres, Pedro. Construindo Roteadores com Linux. Disponível em <<http://lyra.soueu.com.br/index.php/CursosPalestras/LinuxRouter>>. Acesso em 26/05/2004

Marsh, Mattew G. Artigo: Policy Routing in Linux. Disponível em: <<http://www.unixreview.com/documents/s=1247/urm0006d/0006d.htm>>. unixreview.com, 2000.

_____. Policy Routing With Linux - Online Edition. Disponível em: <<http://www.policyrouting.org/PolicyRoutingBook/ONLINE/TOC.html>>. Acesso em: 10/08/2004.

Mogul, Jeffrey. RFC 917 - Internet subnets. Disponível em: <<http://www.faqs.org/rfcs/rfc917.html>>. Acesso em: 20/04/2004.

Monte, Fabiana. Para ver a banda larga passar. Artigo disponível em <http://www.timaster.com.br/revista/materias/main_materia.asp?codigo=231&pag=1>. Revista TI MASTER, 2000.

Mota Filho, João Eriberto. Firewall no Linux iptables, 2001. Disponível em: <<http://www.iptablesbr.cjb.net/>>. Acesso em 27/05/2004.

Moura, A. S. Roteamento: O que é Importante Saber. RNP – Rede Nacional de Ensino e Pesquisa. Revista NewsGeneration, v.1, n.1, 1997. Disponível em <<http://www.rnp.br/newsgen/9705/n1-1.html>>. Acesso em 25/04/2004

Stanger, James. Rede Segura LnuX. 1. ed. Rio de Janeiro: Alta Books, 2002.

BIBLIOGRAFIA CONSULTADA

Bey, Hisham Mardam. Load Balancing Across Multiple *Links*. Disponível em: <<http://linux.com.lb/wiki/index.pl?node=Load%20Balancing%20Across%20Multiple%20Links>>. Acesso em: 20/04/2004.

Coates, Jack. LRP Load Balancing HOWTO. Disponível em: <<http://leaf-project.org/doc/howto/LRP-Load-Balancing-HOWTO.html>>. Acesso em: 20/04/2004.

F5.Networks. A *Link* Load Balancing Solution for Multi-Homed Networks. Disponível em: <http://www.f5.com/solutions/tech/multi_homing.html>. Acesso em: 20/04/2004.

Lewis, Chris. Cisco TCP/IP Routing Professional Reference. 1. ed. New York: McGraw-Hill, 1998.

Marcelo, Antonio. Firewalls em Linux. 3. ed. Rio de Janeiro: Brasport, 2002.

Russell, Rusty. Linux 2.4 Packet Filtering HOWTO, 2002. Disponível em: <<http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO.html>>. Acesso em: 12/06/2004.

ANEXO I - RELATÓRIO GERADO PELO CALAMARIS

Proxy-Report

Report period: 30.Aug 97 00:00:18 - 06.Jun 02 21:07:05
Generated at: 06.Jun 04 20:10:16

Caused by bugs, there were some changes in Cache-File-Format in the lifetime of Calamaris. Your Cachefiles still contain some buggy lines, which causes the following problems:

The Performance data misses the Cache-Hits-value

To correct the problem you should run Calamaris with
calamaris -i buggy.cache -o buggy.cache -z [usual_options]
the workarounds are scheduled to be removed at end of 2003

Summary

lines parsed: 2010556
invalid lines: 9
unique hosts/users: 227
parse time (sec): 6412

Incoming request peak per protocol

prt sec peak begins at min peak begins at hour peak begins at

UDP 22 30.Aug 97 12:32:20 325 07.Oct 98 19:21:39 4958 30.Aug 97 19:37:54
TCP 127 06.Oct 98 00:01:31 674 05.Oct 98 20:34:36 3580 04.Jun 02 05:45:38

ALL 127 06.Oct 98 00:01:31 771 03.Oct 98 21:59:05 5080 30.Aug 97 20:16:51

Request-destinations by 2nd-level-domain

destination	request	%	Byte	%	hit-%
*.geocities.com	18903	1.32	206429K	1.73	34.63
*.netscape.com	7441	0.52	199813K	1.67	53.03
*.xoom.com	9567	0.67	125275K	1.05	35.41
*.sextracker.com	14115	0.99	114839K	0.96	15.75
*.porncity.net	9743	0.68	96958402	0.79	39.38
*.theglobe.com	8369	0.59	92917003	0.76	45.33
*.microsoft.com	14855	1.04	86384991	0.71	54.21
*.aol.com	8000	0.56	78921128	0.64	31.02
*.netsurf.de	20399	1.43	72473207	0.59	72.59
*.bekkoame.ne.jp	5281	0.37	62652773	0.51	63.42
*.t-online.de	6547	0.46	53364854	0.44	30.59
*.matrox.com	3908	0.27	46921236	0.38	67.71
<error>	45526	3.19	41772908	0.34	19.27
*.usatown.net	3545	0.25	41666317	0.34	42.76
*.yahoo.de	7915	0.55	40594967	0.33	54.47
*.glabotki.de	31439	2.20	37765264	0.31	95.14
*.tripod.com	5391	0.38	36999940	0.30	44.48
*.freepage.de	3417	0.24	34726578	0.28	12.26
*.spicyworld.com	3364	0.24	34214346	0.28	43.22
*.lycos.de	5533	0.39	33958992	0.28	63.00
other: 792 2nd-level-domains	1193741	83.65	10191M	87.30	31.78

Sum 1426999 100.00 11674M 100.00 34.25

Request-destinations by toplevel-domain

destination	request	%	Byte	%	hit-%
*.com	669972	46.95	6748980K	56.46	32.00
*.de	442392	31.00	2083575K	17.43	41.52
<unresolved>	69393	4.86	981293K	8.21	30.58
*.net	93791	6.57	930078K	7.78	30.73
*.jp	18222	1.28	203863K	1.71	39.22
*.org	13293	0.93	116023K	0.97	33.13
*.uk	6852	0.48	90413029	0.74	25.79
*.se	4956	0.35	89154562	0.73	17.70
*.edu	3315	0.23	63084649	0.52	23.92
*.au	1408	0.10	58862580	0.48	20.45
*.nl	5057	0.35	53610675	0.44	19.38
*.ru	7692	0.54	51097121	0.42	36.97
*.nu	5531	0.39	45326708	0.37	21.26
*.at	7518	0.53	44619573	0.36	48.00
*.kr	2143	0.15	42759260	0.35	5.83
<error>	45526	3.19	41772908	0.34	19.27
*.ca	1844	0.13	40252110	0.33	23.32
*.ch	4915	0.34	39947717	0.33	23.56
*.fi	1040	0.07	32735122	0.27	23.08
*.pl	1778	0.12	19389355	0.16	26.21
other: 37 top-level-domains	20361	1.43	193569K	1.62	27.22
Sum	1426999	100.00	11674M	100.00	34.25
# TCP-Request-protocol					
protocol	request	%	Byte	%	hit-%
http:	1416812	99.29	10272M	88.00	34.47
ftp:	3602	0.25	1409643K	11.79	7.08
cache_object:	168	0.01	10681002	0.09	0.00
<none>	1827	0.13	9407643	0.08	0.00
<error>	4112	0.29	4232007	0.03	3.38
<secure>	406	0.03	1609987	0.01	0.00
linkdl.cgi?http:	34	0.00	28050	0.00	0.00
file:	25	0.00	22111	0.00	0.00
gopher:	4	0.00	6831	0.00	0.00
	8	0.00	6440	0.00	0.00
news:	1	0.00	781	0.00	0.00
Sum	1426999	100.00	11674M	100.00	34.25
# Requested content-type					
content-type	request	%	Byte	%	hit-%
image/jpeg	280478	19.66	3332702K	27.88	22.64
image/gif	511683	35.86	2250055K	18.82	34.50
text/html	283242	19.85	1746478K	14.61	16.39
application/octet-stream	4301	0.30	1637715K	13.70	25.23
application/zip	2716	0.19	1173252K	9.81	9.13
multipart/x-mixed-replace	1147	0.08	311156K	2.60	0.70
text/plain	8115	0.57	282471K	2.36	19.06
video/mpeg	352	0.02	261036K	2.18	15.91
<unknown>	276770	19.40	160404K	1.34	67.66
video/vnd.vivo	248	0.02	101508K	0.85	6.45

application/x-zip-compressed	107	0.01	88883031	0.73	5.61
audio/mpeg	79	0.01	76521158	0.63	0.00
video/x-msvideo	139	0.01	75752218	0.62	14.39
video/msvideo	64	0.00	45201489	0.37	6.25
<error>	45525	3.19	41767606	0.34	19.27
video/quicktime	95	0.01	31879987	0.26	13.68
application/x-shockwave-flash	474	0.03	26246339	0.21	70.04
application/x-tar	54	0.00	24869543	0.20	1.85
application/pdf	99	0.01	24102815	0.20	24.24
audio/basic	157	0.01	22139478	0.18	29.30
other: 36 content-types	11154	0.78	250273K	2.09	25.47

Sum	1426999	100.00	11674M	100.00	34.25
-----	---------	--------	--------	--------	-------

Requested extensions

extensions	request	%	Byte	%	hit-%
jpg	291470	20.43	3027061K	25.32	28.31
gif	591369	41.44	2051839K	17.16	48.23
exe	3837	0.27	1498238K	12.53	10.76
zip	3045	0.21	1224422K	10.24	8.21
<none>	138078	9.68	663941K	5.55	17.23
html	102567	7.19	535128K	4.48	36.08
htm	58266	4.08	329597K	2.76	25.42
JPG	24082	1.69	286988K	2.40	32.24
mpg	331	0.02	221608K	1.85	16.01
<dynamic>	30051	2.11	214051K	1.79	9.65
pl	5973	0.42	166950K	1.40	11.97
mp3	403	0.03	159714K	1.34	1.24
cgi	50097	3.51	154936K	1.30	7.21
viv	360	0.03	105231K	0.88	8.06
GIF	19979	1.40	78930190	0.64	47.03
CAB	240	0.02	75769211	0.62	35.00
ev	358	0.03	66235944	0.54	21.51
asp	8728	0.61	62968067	0.51	0.07
<error>	45526	3.19	41772908	0.34	19.27
mid	1452	0.10	34084609	0.28	46.90
other: 51 extensions	50787	3.56	962662K	8.05	20.94

Sum	1426999	100.00	11674M	100.00	34.25
-----	---------	--------	--------	--------	-------

Calamaris \$Revision: 2.59 \$

Copyright (C) 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 Cord Beermann.

Calamaris comes with ABSOLUTELY NO WARRANTY. It is free software, and you are welcome to redistribute it under certain conditions. See source for details.

Calamaris-Homepage: <http://Calamaris.Cord.de/>

ANEXO II - COMPILANDO O KERNEL

```
# cd /usr/src/linux # make menuconfig
```

Este comando permite a configuração através de menus das funções a serem compiladas no Kernel. Parte destas funções estão em processo de constante desenvolvimento e modificação, portanto, no item "*Code maturity level options*", selecione:

[*] Prompt for development and/or incomplete code/drivers

Devem ser habilitados os drivers de dispositivos correspondentes às interfaces de rede existentes no sistema, através do item *Network Device Support*.

As opções existentes referentes ao subsistema de rede do Linux se encontram em *Networking Options*. Faremos uma descrição sucinta dos itens de maior relevância. Por padrão, o protocolo IP na sua versão 4, na qual se baseia a Internet, encontra-se habilitado através de:

[*] TCP/IP Networking.

Há uma versão mais atual do protocolo IP, o IPv6, a qual foi desenvolvida para ser utilizada no futuro na Internet. Caso se queira, pode-se fazer experimentações com esta nova versão do protocolo. As ferramentas abordadas neste artigo atuam com o IPv6 e maiores informações sobre o protocolo podem ser obtidas no Projeto 6Bone-BR em <http://www.6bone.rnp.br/>. As opções referentes ao mesmo são:

<*>The IPv6 Protocol

[*] enable EUI-64 token format

Para utilizar a ferramenta **iptables**, ou comandos da ferramenta **ip** sobre o objeto *rule*, possibilitando recursos com NAT e *Proxy Transparent*, devemos habilitar as opções:

[*] Network packet filtering (replaces ipchains)

[*] Network packet filtering debugging

[*] Socket Filtering

E, ainda, devemos ativar as opções existentes no subitem "IP: Netfilter Configuration -->", dentre as quais o suporte a **iptables**.

Para o suporte ao estabelecimento de túneis de protocolo, ative:

<*> IP: tunneling

<*> IP: GRE tunnels over IP

Um recurso bastante interessante de rede (com algumas melhorias com o IPv6), o *Multicast*, é uma opção a se observar:

- [*] IP: multicasting
- [*] IP: multicasting routing

Opções avançadas de roteamento, incluindo NAT, devem estar ativas para os nossos propósitos:

- [*] IP: advanced router
- [*] IP: policy routing
- [*] IP: use netfilter MARK value as routing key
- [*] IP: fast network address translation
- [*] IP: equal cost multipath
- [*] IP: use TOS value as routing key
- [*] IP: verbose route monitoring
- [*] IP: large routing tables

Para, então, compilar o Kernel, salva-se a configuração e segue-se os seguintes passos:

```
# make dep
# make clean
# make bzImage
# make modules
# make install
# make modules_install
```

APÊNDICE I - SCRIPT PARA COMPARTILHAMENTO DE CONEXÃO

Implementando as regras no firewall

```
#!/bin/bash

# Ativando link com velox
/etc/ppp/velox.sh
#
# Carregando os modulos basicos:

echo -n "Carregando os modulos..."
modprobe ip_tables
modprobe iptable_filter
modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe iptable_nat
modprobe ip_nat_ftp
modprobe ipt_LOG
modprobe ipt_state
modprobe ipt_MASQUERADE
echo " [OK]"

# INICIALIZANDO VARIÁVEIS
echo -n "Inicializando variáveis..."

$IPTABLES=/sbin/$IPTABLES

VELOX_IFACE1=eth0
VELOX_IFACE2=eth1
SERVIDORES_IFACE=eth2
#INTERNAL_IFACE2=eth3
#INTERNAL_IFACE3=eth4
#EXTERNAL_IFACE=eth0
DNS1=200.217.212.162
DNS2= 200.149.55.142

# Resetando o Firewall:

echo -n "Resetando o firewall..."
$IPTABLES -F
$IPTABLES -Z
```

```

$IPTABLES -X
$IPTABLES -t nat -F
$IPTABLES -P INPUT DROP
#$IPTABLES -P INPUT ACCEPT

$IPTABLES -P FORWARD DROP
#$IPTABLES -P FORWARD ACCEPT

$IPTABLES -P OUTPUT ACCEPT
echo " [OK]"

# Habilitando o roteamento de pacotes:

echo -n "Habilitando o roteamento..."
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo " [OK]"

# Liberando a chain INPUT para o localhost:

echo -n "Liberando acesso do localhost..."
$IPTABLES -A INPUT -p ALL -s 127.0.0.1 -i lo -j ACCEPT
$IPTABLES -A INPUT -p ALL -s 10.1.1.3 -i lo -j ACCEPT
$IPTABLES -A INPUT -p ALL -s 10.2.1.3 -i lo -j ACCEPT
$IPTABLES -A INPUT -p ALL -s 10.10.1.254 -i lo -j ACCEPT
$IPTABLES -A INPUT -p ALL -s 10.11.1.254 -i lo -j ACCEPT
$IPTABLES -A INPUT -p ALL -s 10.13.1.254 -i lo -j ACCEPT
$IPTABLES -A INPUT -p ALL -s 200.217.212.163 -i lo -j ACCEPT

echo " [OK]"

echo -n "Habilitando o mascaramento..."
$IPTABLES -t nat -A POSTROUTING -o $VELOX_IFACE1 -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -o $VELOX_IFACE2 -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -o $SERVIDORES_IFACE -j MASQUERADE

# Mantendo conexoes ativas:

echo -n "Manutencao de conexoes ativas..."
$IPTABLES -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
echo " [OK]"

# Liberando acesso ao DNS para a rede interna:

echo -n "Liberando DNS para rede interna..."

```

```
$IPTABLES -A FORWARD -p udp -s 10.0.0.0/8 -d $DNS1 --dport 53 -j ACCEPT
$IPTABLES -A FORWARD -p udp -s 10.0.0.0/8 -d $DNS2 --dport 53 -j ACCEPT
$IPTABLES -A FORWARD -p udp -s $DNS1 --sport 53 -d 10.0.0.0/8 -j ACCEPT
$IPTABLES -A FORWARD -p udp -s $DNS2 --sport 53 -d 10.0.0.0/8 -j ACCEPT
echo " [OK]"
```

#Bloqueio para smtp

```
$IPTABLES -I FORWARD -s 10.0.0.0/8 -d ! 200.217.212.162 -p tcp --dport 25 -j DROP
```

Desabilitando o filtro de pacotes do martian source

```
echo -n "Desligando rp_filter..."
for eee in /proc/sys/net/ipv4/conf/*/rp_filter; do
echo 0 > $eee
done
echo " [OK]"
```

Redirecionando a saída www (PROXY TRANSPARENTE)

```
$IPTABLES -t nat -A PREROUTING -i eth2 -s 0/0 -p tcp -d ! 200.217.212.162 --dport 80 -
j REDIRECT --to-ports 3128
$IPTABLES -t nat -A PREROUTING -i eth3 -s 0/0 -p tcp -d ! 200.217.212.162 --dport 80 -
j REDIRECT --to-ports 3128
$IPTABLES -t nat -A PREROUTING -i eth4 -s 0/0 -p tcp -d ! 200.217.212.162 --dport 80 -
j REDIRECT --to-ports 3128
```

APÊNDICE II - *SCRIPT* PARA AUTENTICAÇÃO NA VELOX

```
#!/bin/sh

# #####
# Script para autenticação do Velox no linux
#
#
# Versão 5.2
# Autor: Manoel Pinho <pinho@uninet.com.br>
# Data: 29/11/2003
#
# Adaptado para realidade da FARN por George Henrique Bezerra
#
# -----
#
# #####
# Definições dos comandos utilizados para conexão e autenticação
# #####
#
# LEIA COM ATENÇÃO AS EXPLICAÇÕES E PREENCHA OS SEUS DADOS PARA
# A CONEXÃO
#
# Descomente para debug
# set -xv

# #####
# Definições dos comandos utilizados para conexão e autenticação
# #####

# Definição do tipo do modem
# -----
# Escolha somente uma das opções conforme o modelo do seu modem ADSL.
#
# Se voce precisa "disar" a conexão antes de autenticar, então o tipo é BRIDGE.
# Nesse caso, a ligação PPPOE sera levantada automaticamente antes de autenticar.

# OBS: mesmo tento um modem BRIDGE, caso queira usar o script SOMENTE para
# autenticar (e ativar a conexao PPPOE manualmente), coloque o tipo como ROUTER.

MODEM=""
#MODEM='BRIDGE'
MODEM='ROUTER'

# diretorio do programa curl (necessario nesta versao)
```

```

# -----
CURL=/usr/bin/curl

# Caminho completo para o ping (necessario para testar a conexao apos autenticar)
# -----
PING=/bin/ping

# Preencha aqui seus dados
# *****

# Defina se seu velox e' residencial ou comercial
# -----

VELOX=""

# Descomente (retire o # da frente) correspondente a sua opcao.
# Valores :
# 'RES' = Residencial
# 'COM' = Comercial

#VELOX='RES'
VELOX='COM'

# Provedores habilitados para o Velox RESIDENCIAL
# *****

PROVEDOR=""

## Lista de provedores implementada por Adilson Junior <cabide@brfree.com.br>

# => descomente (retire o # da frente) correspondente a linha do seu provedor

# seu login (NO PROVEDOR) - SOMENTE PARA VELOX RESIDENCIAL
# -----

LOGIN=""

# sua senha (NO PROVEDOR) - SOMENTE PARA VELOX RESIDENCIAL
# -----

SENHA=""

# Caso use o velox COMERCIAL
# *****

```

COMERCIAL=""

Descomente (retire o # da frente) correspondente a sua opção.

No Rio de Janeiro:

#COMERCIAL='AARJ'

Em Minas Gerais:

#COMERCIAL='AAMG'

Na Bahia, Alagoas, Ceará, Espírito Santo, Maranhão, Paraíba, Pará, Pernambuco, Piauí, Rio G. do Norte, Sergipe
COMERCIAL='AABA'

OBS: Pode ser necessário alterar a string acima de acordo com a sua região.

Página de autenticação do Velox (pode mudar a qualquer momento)

#HOST='www.veloxzone.com.br'

HOST='200.165.104.14'

#HOST='200.165.104.28' # endereço IP do veloxzone no RJ caso tenha problema com
www.veloxzone.com.br

Hosts para teste de ICMP PING (um deles tem que responder ao menos)

#Pode ser utilizado qualquer host ou use estes como padrão.

PHOST1='ns.dns.br'

PHOST2='ns1.dns.br'

PHOST3='a.root-servers.net'

Parâmetros adicionais

PARAM_CURL=""

PARAM_PING='-c 1'

Quem sou eu ?..

MEUNOME=""`basename \$0`"

#####

#####

FIM DA CONFIGURAÇÃO

#####

#####

#-----

```

verifica_programas ()
{

echo
echo "Verificando a existência dos programas necessários para o script ..."
echo

if [ -x $PING ]; then
    echo "OK! "Ping" encontrado em $PING"
else
    echo "$MEUNOME: ERRO! o ping NÃO foi encontrado em $PING."
    echo "    Edite o script !!"
    exit 2
fi

if [ -x $CURL ]; then
    echo "OK! "CURL", encontrado em $CURL"
else
    echo "$MEUNOME: ERRO! o curl NÃO foi encontrado em $CURL."
    echo "Edite o script !"
    exit 2
fi

}

# Autenticacao do usuario no provedor
# *****
# main ()

verifica_programas

echo

# Verificacao se o usuario já definiu o tipo do modem
if [ -z "$MODEM" ]; then
    echo "$MEUNOME: É necessário definir o tipo do modem !"
    echo "    Edite o script !!"
    exit 2
fi

# Verificacao se o usuario já definiu se o Velox é Residencial ou Comercial
if [ -z "$VELOX" ]; then
    echo "$MEUNOME: É necessário definir se o Velox é residencial ou comercial !"
    echo "    Edite o script !!"
    exit 2

```

```

fi

# Verificacao se o usuario já escolheu o provedor no caso de Velox Residencial
if [ "$VELOX" = 'RES' -a -z "$PROVEDOR" ]; then
    echo "$MEUNOME: É necessário configurar um provedor para Velox Residencial !"
    echo "      Edite o script !!"
    exit 2
fi

# Verificacao se o usuario já preencheu o login do provedor (Velox Residencial)
if [ "$VELOX" = 'RES' -a -z "$LOGIN" ]; then
    echo "$MEUNOME: É necessário preencher o login do provedor no Velox Residencial !"
    echo "      Edite o script !!"
    exit 2
fi

# Verificacao se o usuario já preencheu a senha do provedor (Velox Residencial)
if [ "$VELOX" = 'RES' -a -z "$SENHA" ]; then
    echo "$MEUNOME: É necessário preencher a senha do provedor no Velox Residencial !"
    echo "      Edite o script !!"
    exit 2
fi

# Verificacao se o usuario já escolheu o código correto (Velox Comercial)
if [ "$VELOX" = 'COM' -a -z "$COMERCIAL" ]; then
    echo "$MEUNOME: É necessário configurar um dos códigos para Velox Comercial !"
    echo "      Edite o script !!"
    exit 2
fi

if [ "$MODEM" = 'BRIDGE' ]; then
    liga_pppoe
fi

echo "Host Autenticação Velox = $HOST"
echo "Host Teste ICMP PING 1 = $PHOST1"
echo "Host Teste ICMP PING 2 = $PHOST2"
echo "Host Teste ICMP PING 3 = $PHOST3"
echo

# Verificando se ja esta autenticado...

# obs: caso não queira fazer isso para que o script execute mais rápido,
# chame-o com a opção boot. Ex: ./nomedascript boot

```

```

echo "Verificando se já está autenticado... Por favor aguarde !!"

if [ "$1" != "boot" ]; then
  if ( ($PING $PARAM_PING $PHOST1 > /dev/null 2>&1) ||
    ($PING $PARAM_PING $PHOST2 > /dev/null 2>&1) ||
    ($PING $PARAM_PING $PHOST3 > /dev/null 2>&1) ); then
    echo "$MEUNOME: Jáá autenticado. Saindo..."
    exit 0
  fi
fi

echo
echo "Não está autenticado! Realizando a autenticação..."

# URL usadas para autenticação. Podem mudar a qualquer momento e talvez possam ser
# alteradas no futuro ou sejam diferentes em outros estados. Foram testadas no RJ com
# sucesso,
# tanto num Velox residencial quanto num Velox comercial. Caso seja necessário alguma
# modificação na sua região e vc tenha obtido sucesso, por favor compartilhe conosco
# mandando um
# email para mim com a versão modificada.

AUT_RES="-d service=internet_$PROVEDOR -d fcn=serviceLogon -d ac=home -d usr= -
-d username=$LOGIN -d password=$SENHA -d OK=OK $HOST/serviceLogon"

AUT_COM="-d confirmed=true $HOST/serviceStart?service=internet_$COMERCIAL"

if [ "$VELOX" = 'RES' ]; then
  echo "Modo Residencial"
  echo "Provedor : $PROVEDOR"
  echo "Login : $LOGIN"
  AUT=$AUT_RES
elif [ "$VELOX" = 'COM' ]; then
  echo "Modo Comercial"
  echo "Código: $COMERCIAL"
  AUT=$AUT_COM
else
  echo "$MEUNOME ERRO! Tipo do velox não configurado. Edite o script !!"
  exit 2
fi

echo "!!! ***** AGUARDE ***** !!!"

```

```

# Comando para autenticação
AUTH="$CURL $PARAM_CURL $AUT"

if ( $AUTH > /dev/null 2>&1 ) then
    while !( ($PING $PARAM_PING $PHOST1 > /dev/null 2>&1) ||
        ($PING $PARAM_PING $PHOST2 > /dev/null 2>&1) ||
        ($PING $PARAM_PING $PHOST3 > /dev/null 2>&1) )
    do
        echo "$MEUNOME: ERRO! Servidor não liberou acesso, senha ou
configuração incorreta..."
        echo "          Tentando novamente..."
        ( $AUTH > /dev/null 2>&1 )
    done

    echo "$MEUNOME: OK! Autenticado no Velox ..."
    mail -s "Nova autenticao do VELOX" george@farn.br < /tmp/velox.log

    if [ "$FIREWALL" != " " ]; then
        source $FIREWALL
        echo "Firewall iniciado !"
    fi

    exit 0
else
    echo "$MEUNOME: ERRO! Nao é possivel conectar a $HOST !!"
    exit 1
fi

#
# Mantenha descomentado mesmo com o debug comentado no início. Isto força a
# finalização do debug.
set +xv

```