UNIPAC
UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS
FACULDADE DE CIÊNCIA DA COMPUTAÇÃO E COMUNICAÇÃO SOCIAL

CURSO DE CIÊNCIA DA COMPUTAÇÃO

Samuel Sander de Carvalho

AUDITORIA DE REDES UTILIZANDO MRTG E SARG

BARBACENA

DEZEMBRO DE 2004

SAMUEL SANDER DE CARVALHO

AUDITORIA DE REDES UTILIZANDO MRTG E SARG

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação e ao Departamento da Faculdade de Ciência da Computação da UNIPAC – Universidade Presidente Antônio Carlos como requisito parcial para a obtenção do Titulo de Bacharel em Ciência da Computação.

ORIENTADOR: Prof. Luís Augusto Mattos Mendes

BARBACENA

DEZEMBRO DE 2004
Samuel Sander de Carvalho

AUDITORIA DE REDES UTILIZANDO MRTG E SARG

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação e ao Departamento da Faculdade de Ciência da Computação da UNIPAC - Universidade Presidente Antônio Carlos como requisito parcial para a obtenção do Titulo de Bacharel em Ciência da Computação.

Aprovada em _____/_____/_____.

BANCA EXAMINADORA

_____
Prof. Luís Augusto Mattos Mendes – Orientador do Trabalho

_____
Prof. Gustavo Campos Menezes

_____
Prof. Eduardo Macedo Bhering

Dedico este trabalho a minha namorada, Keylla Teixeira de Carvalho, pelos seus incentivos, apoio e compreensões nas horas de dificuldades.

Agradeço primeiramente a Deus por ter me dado força, inspiração e paciência nas horas de aflição. Agradeço ao meu Orientador que com sua competência e paciência me ajudou a concluir este trabalho e aos meus pais que me deram muita força para chegar aonde cheguei, agradeço também aos meus colegas e amigos que me apoiaram para a conclusão deste trabalho.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Desde o início da civilização sempre houve dificuldade na troca de informações. Com o avanço da tecnologia e o surgimento da *internet* os problemas diminuíram. A *internet* é utilizada para os mais diversos fins, como troca de dados, comunicação entre pessoas, busca de informações, enfim, permite a interação entre pessoas de qualquer parte do planeta. E, por isso, se faz presente nas mais diversas áreas, sendo sua utilização de fundamental importância em casa, nas escolas, faculdades e no trabalho.

Com essa vinda da *internet*, houve a necessidade de se usar redes de computadores com acesso dedicado para que se possa haver um ganho na produção e na troca de informações. Devido à *internet* se expandir e se tornar de fácil acesso, esta, acabou por se transformar em um local onde os usuários “acessam” sites com alguma freqüência, sendo estes muitas vezes impróprios (indevidos) ao perfil da instituição.

Para evitar que essas instalações se tornem locais por onde trafegam indiscriminadamente informações de qualquer origem, criou-se o projeto, sobre *AUDITORIA DE REDES UTILIZANDO MRTG E SARG*, que trata de monitorar a rede através destas ferramentas, possibilitando ao administrador gerenciar e coibir a utilização indevida dos computadores.

Este projeto demonstra a utilização das ferramentas SARG e MRTG monitorando uma rede de computadores apresentando seus principais aspectos, características e finalidades, além de abordar uma possível configuração das ferramentas, apontando como resultado, relatórios gráficos produzidos por estas.

Para um melhor entendimento da necessidade de uma auditoria de rede, o trabalho está organizado da seguinte forma:

No capítulo 2, Ferramentas para auditoria, aborda a descrição das ferramentas, explicando suas finalidades e mostrando no que elas serão benéficas, apresentando suas

características. Já no capítulo 3, Documentação das ferramentas, abordará uma possível configuração das mesmas, explicando passo a passo o funcionamento de cada linha de código, sendo estas apenas um exemplo e não uma regra. No 4º capítulo, Estudo de caso e análise dos resultados, serão abordados todos os dados obtidos com o uso das ferramentas em forma de gráficos e descrições textuais, por sua vez, estes serão analisados e verificados. Finalizando no capítulo 5, Conclusão, será apresentado a conclusão deste projeto.

2. FERRAMENTAS DE AUDITORIA

Este capítulo apresentará as ferramentas de auditoria utilizadas pelo administrador da rede especificando suas funcionalidades e suas características, também abordará conceitos sofre os servidores onde as ferramentas são instaladas

2.1. MRTG

> "O MRTG *(Multi Router Traffic Grapher)* é um sistema com a capacidade de ler dados de um dispositivo através de protocolos. Inicialmente foi desenvolvido para ler dados de roteadores, com a intenção de melhorar sua funcionalidade, passou por várias alterações e adaptações, podendo assim gerar gráficos de uso da rede por determinados computadores, tais como nome do dispositivo, IP (*Internet Protocol*), dados enviados e recebidos, etc, mostrando tráfego da rede referente ao dispositivo monitorado" (Anônimo, 2004)

O MRTG é um *software* livre escrito em *Perl* e *C* que roda sob plataforma *Unix* e *Windows NT* e, que além de gerar relatórios diários, também cria representações visuais do tráfego durante os últimos 7 dias, das últimas 4 semanas e dos últimos 12 meses. Isto é possível porque ele mantém um *log* de todos os dados que lhe são fornecidos pelo roteador. Embora o seu foco seja o acompanhamento de componentes da rede através do protocolo SNMP *(Simple Network Management Protocol)*, pode-se muito bem utilizar este *software* para verificar o funcionamento de computadores domésticos ou de estações de trabalho.

O MRTG normalmente é usado para monitorar a Carga do Sistema, Sessões Logadas, Disponibilidade de *Modens*, além de permitir o acúmulo de duas ou mais fontes de dados em um único gráfico. Desta forma, conforme campos (2004), ele é usado para monitorar o tráfego

em *links* de rede. Seus gráficos são gerados em páginas HTML *(Hypertext Markup Language)* contendo imagens PNG *(Portable Network Graphics)* que possibilitam a visualização do tráfego.

2.1.1. Características

> "O MRTG apresenta portabilidade, o que o permite trabalhar em sua maior parte nas plataformas *UNIX* e *Windows NT*; além disso ele é escrito em *Perl* e vem com todo o código fonte, sendo que para aumentar seu desempenho, as rotinas mais críticas foram escritas em *C* graças à iniciativa de Dave Rand; também pode usar uma implementação SNMP de alta portabilidade. Graças a Simon Leinen não é necessário instalar qualquer pacote SNMP externo. As interfaces dos roteadores podem ser identificadas pelo Endereço IP, Descrição e Endereço *Ethernet* em adição ao número da interface normal, o que as tornam confiáveis; outra característica importante é que os arquivos de *log* do MRTG não crescem, graças ao uso de um algoritmo de consolidação de dados único; pode-se também dizer que o MRTG pode fazer a sua configuração automaticamente devido ao conjunto de ferramentas de configuração que torna essa configuração muito simples; finalizando, os gráficos são gerados diretamente no formato PNGs e não em GIF (*Graphics Interchange Format*), o que aumenta a qualidade destas imagens e a aparência das páginas produzida pelo MRTG é altamente configurável". (CAMPOS, 2004)

2.1.2. SNMP

O SNMP, Protocolo Simples de Gerenciamento de Redes, é criado para o gerenciamento de equipamentos usando rede TCP/IP (*Transmission Control Protocol/Internet Protocol*) cujo objetivo é disponibilizar uma forma simples e prática de realizar o controle dos equipamentos de uma rede de computadores. Definido em nível de aplicação, O SNMP utiliza os serviços do protocolo de transporte UDP *(User Datagram Protocol)* para enviar suas mensagens através da rede. "Ele pode ter tanto ação passiva (monitoração) como ativa (modificação de configuração)" (SOUZA, 2004).

A ação do SNMP é dada pelo fornecimento, coleta e manipulação de objetos chamados de MIB (*Management Information Base* - Base de Informação de Gerenciamento). Outros objetos como o RMON (*Remote Monitoring* - Monitoração Remota) também são utilizados para esse fim.

Nos últimos anos o SNMP tem dominado o mercado de sistemas de gerenciamento de redes devido, principalmente, a sua simplicidade de implementação, pois consome poucos recursos de redes e de processamento, o que permite a sua inclusão em equipamentos bastante simples.

Segundo oliveira (2003), o SNMP ajuda o administrador a localizar e corrigir erros ou problemas de uma rede. Através de agentes SNMP, o administrador da rede consegue visualizar estatísticas de tráfego da rede e após analisar esses dados o administrador pode atuar na rede, alterando a sua configuração.

2.2. SARG

O SARG *(Squid Analysis Report Generator)* é uma ferramenta desenvolvida por um brasileiro que permite ver para "onde" seus usuários estão “navegando” na *Internet* através da análise do arquivo de *log* "*access.log*" do *Proxy Squid*. Essa ferramenta pode dizer quais usuários acessaram quais *sites*, a que horas se deu esses acessos, quantos *bytes* foram baixados, quantas conexões foram feitas, relatórios de *sites* mais acessados, usuários que mais acessam, relatório de *sites* negados, falha de autenticação, entre outros. A gerência que se pode obter com isso é muito boa, principalmente para as empresas que querem economizar o uso da *Internet*.

Pode-se configurar o SARG para trabalhar conforme as necessidades de cada instituição.

O SARG utiliza a licença GPL (*General Public License*), que permite sua utilização e alteração conforme a necessidade de cada um, contanto que cada implementação seja enviada ao autor para que seja implementada e liberada em futuras versões.

2.3. Servidor *Proxy* (*Squid*)

Quando se acessa, por exemplo, uma página da *Web* ou um arquivo de FTP *(File Transfer Protocol)*, uma requisição parte da máquina que fez o acesso até o servidor, só então os dados são transmitidos para a máquina. Como muitas vezes, à distância entre o servidor e a máquina poderá ser muito grande, e a qualidade das linhas de transmissão ser muito irregular, este processo acaba por tornar-se bastante lento. Além disso, a maioria dos dados requisitados são estáticos, ou seja, eles não mudam com o tempo. Os logotipos que as empresas colocam em suas páginas por exemplo, não tendem a mudar. Entretanto, eles são, muitas vezes, bastante grandes. Isso é um enorme desperdício de recursos da rede e de tempo.

Uma solução encontrada foi o chamado *caching*. Sempre que é feita uma requisição de algum objeto da *Internet*, o servidor *Proxy* consulta o *cache* para verificar se este objeto já não foi requisitado previamente. Se ele foi, então o servidor *Proxy* pode responder à requisição utilizando sua própria cópia local do objeto. Isso acelera significativamente as operações na *Internet*, já que grande parte dos objetos acaba trafegando apenas localmente.

O servidor *Proxy* verifica se a sua cópia é atualizada, caso não seja, o *Proxy* faz a atualização dessa cópia. Naturalmente, um servidor de *cache* não poderia guardar todos os objetos acessados para sempre, pois isso iria rapidamente saturá-lo. A solução é simples: o servidor mantém apenas os arquivos utilizados a menos tempo. Isso garante, de uma forma indireta, que os objetos mais freqüentemente utilizados sempre estejam no *cache*.

Esta solução implementa um servidor *Proxy* utilizando o *Squid*, que é completamente livre e com excelente suporte para operação em servidores *Linux*.. Ele oferece alto desempenho de *cache* para servidores *Web*. Também oferece grandes vantagens em comparação com outros servidores *Proxy*. Além do *cache* de objetos como arquivos de FTP e páginas da *Web*, realiza também um *cache* de procuras de DNS *(Domain Name System)*. Isso quer dizer que ele guarda informações sobre o mapeamento entre endereços IP e nomes de máquinas da *Internet* acelerando a procura de máquinas; além de manter os objetos mais utilizados na memória RAM (cujo uso pode ser limitado pela configuração); também suporta SSL *(Secure Sockets Layer)* (acesso a páginas criptografadas) para segurança em transações; o *Proxy Squid* pode ser organizado em hierarquias de servidores de *cache* para uma melhora

significativa de desempenho e responde às requisições em um único processo de acesso a disco.

Todo o servidor *Proxy Squid* consiste de um programa principal (*Squid*) e de seu próprio programa de resolução de nomes (*dnsserver*). Quando o *Squid* é inicializado, ele cria o processo do *dnsserver*, diminuindo o tempo de espera pela resposta do DNS.

Com o *Squid* pode-se instalar um servidor *Linux* com acesso à *Internet*, e fazer com que outras máquinas clientes (usando *Linux*, Windows ou outro sistema operacional) acessem páginas *Web* e *sites* FTP através do servidor *Linux*, mesmo que estas máquinas clientes não tenham conexão direta com a *Internet* - tudo que elas precisam é o acesso ao próprio servidor onde está rodando o *Squid*.

A única configuração necessária na máquina cliente é feita no próprio *browser*. Necessita-se definir qual o endereço do servidor *Proxy*, *e*sta é uma operação bastante simples, disponível nos menus do *Netscape*, do *Internet Explorer* e dos demais *browsers* em geral.

Segundo campos (2004) o *Squid* dá acesso somente a serviços como *https* (*Web* segura) e FTP.

2.4. Servidor *Apache*

O verdadeiro responsável por todas essas ferramentas funcionarem é o *Apache*, que é o servidor *Web* mais utilizado hoje na *I*nternet, de acordo com a pesquisa do *NetCraft* sobre *sites* da *Web*. O nome "*Apache*" surgiu durante o desenvolvimento inicial do *software* porque ele era "*a patchy server*", criado com "*patches*" ("remendos") de códigos livres disponíveis no servidor *Web* da NCSA HTTPd. Durante algum tempo, após o projeto da NCSA HTTPd ter sido interrompido, algumas pessoas escreveram uma variedade de *patches* para um código, fosse para consertar bug ou para adicionar os recursos que desejavam. Havia uma porção desse código por aí e as pessoas estavam compartilhando livremente desse código, mas ele se encontrava completamente desorganizado.

Após algum tempo, Bob Behlendorf e Cliff Skolnick criaram um repositório centralizado desses *patches* e nascia o projeto *Apache*.

Nos últimos anos, tem havido um aumento de interesse em relação ao projeto *Apache*, parcialmente incentivado pelo novo interesse pelo código aberto. Isso também é em parte devido ao compromisso da IBM de oferecer suporte e de usar o *Apache* como base para as

ofertas da companhia relacionadas a *Web*. Dedicaram recursos substanciais ao projeto, afinal, é mais lógico usar um servidor *Web* bem estabelecido e testado na prática, do que tentear escrever um eles mesmos.

> “Em meados de 1999, a ASF (*Apache Software Foundation*) foi incorporada como uma companhia não voltada para o lucro. Uma equipe de diretores, que são eleitos em bases anuais pelos membros da ASF, supervisiona a companhia. Essa companhia fornece as bases para diversos projetos de desenvolvimento de software de código aberto - inclusive o projeto *Apache Web Server*” (BALL, 2002).

3. DOCUMENTAÇÃO DAS FERRAMENTAS

A abordagem das configurações descritas neste capítulo, são as utilizadas para a geração do estudo de caso e análise dos resultados do próximo capítulo. Não são uma regra, dependendo da necessidade de cada um, essas configurações poderão e serão mudadas, isso porque cada servidor terá formas diferentes, com necessidades distintas, no entanto, todas as configurações terão semelhanças entre si.

3.1. MRTG

Para poder criar o arquivo de configuração do MRTG, deve-se criar uma pasta dentro do servidor na qual este será armazenado. Após a criação, o arquivo deve ser editado para se poder fazer as modificações necessárias

As seguintes linhas de código foram às utilizadas para poder configurar o MRTG que foi utilizado para a geração dos relatórios no 4º capítulo.

O comando *WorkDir* determina o diretório onde vai ficar a página com os gráficos gerados pelo MRTG, neste caso o diretório se encontra em */var/www/default/mrtg.*

```
WorkDir: /var/www/default/mrtg
```

Refresh determina o tempo, em segundos, em que o *browser* irá atualizar a página, para tal,

```
Refresh: 600
```

As informações apresentadas nos relatórios que são exibidos no *browser* são atualizadas junto aos *hosts* conforme o tempo determinado pelo comando *Interval*, onde esse tempo foi de 5 minutos para este script.

```
Interval: 5

WriteExpires: Yes
```

Para poder informar a língua que será utilizada pelo MRTG na exibição das mensagens na página, utiliza-se o comando *Language*, neste caso a língua escolhida foi a brasileira (*brazilian*).

```
Language: brazilian
```

Segundo cisneiros (2004) O "*cron*" é um programa de "agendamento de tarefas". Com ele você pode programar para ser executado qualquer coisa numa certa periodicidade ou até mesmo em um exato dia, numa exata hora. Estas tarefas são programadas para todo dia, toda semana ou todo mês. A configuração do *cron* geralmente é chamada de *crontab*. Para não precisar utilizar o *crontab*, rode o MRTG como *Daemon*, isso significa que só precisará colocar um comando na inicialização do *Linux*, ou seja, o MRTG ficará carregado, e vai buscar os dados do host conforme o parâmetro *Interval*, mas para isso o comando *RunAnAemon* será inserido no script seguido da opção *yes*.

```
RunAsDaemon: Yes
```

O comando Optinos [_] seguido da(s) opção(ões) *growright* define que o gráfico cresce para a direita, e *bits m*ostrar a velocidade em *bits* (*bits/bytes*) que o crescimento terá.

```
Options [_]: growright, bits
```

OBS. Não deixe nenhum espaço no inicio da linha, ou então poderá dar erro na execução do MRTG.

O comando indexmaker gera o link para a página onde os gráficos do MRTG se encontram, este link será identificado como index.html, mas para isso deve-se indicar o arquivo de configuração do MRTG (mrtg.cfg.).

```
indexmaker mrtg.cfg >
```

O comando final mrtg mrtg.cfg serve para gerar os gráficos do MRTG.

```
mrtg mrtg.cfg
```

3.2. SARG

Os comandos a seguir definem a configuração do SARG. Para um maior entendimento, os comandos que aparecerem com as opções *none*, significa que este está usando o *default* do comando.

language define qual será a linguagem utilizada nos relatórios do SARG, mesmo em inglês os resultados serão em português do Brasil.

```
language English
```

O comando *access_log* determina onde se encontrará o arquivo de *log* do *Squid*, que neste caso, localiza-se em: */var/log/squid/access.log.*

```
access_log /var/log/squid/access.log
```

O comando a seguir (*title*) determina o título da página HTML, gerado pelo SARG.

```
title "Relatório do Proxy Squid - Do Dia"
```

Todos os comandos abaixo, *font_face*, *header_oclor*, etc. são utilizados para deixar o visual do relatório (fonte, cor, etc.) de acordo com o que o administrador da rede deseja.

```
font_face Arial
header_color darkblue
header_bgcolor blanchedalmond
header_font_size -1
background_color white
text_color black
text_bgcolor beige
title_color green
logo_image none
logo_text_color black
background_image none

password none
```

temporaty_dir define o nome de diretório temporário para arquivos de trabalho do SARG.

```
temporary_dir /tmp
```

O comando *output_dir* indica o diretório de saída para a página de relatório, ou seja, onde o relatório vai ficar para consulta via um navegador. Geralmente esse diretório tem que estar dentro do *root* de seu servidor *Web*. O diretório usado aqui foi /var/www/default/relatorio/sarg

```
output_dir /var/www/default/relatorio/sarg
```

output_email indica qual será o *e-mail* utilizado para o envio dos relatórios.

```
output_email none

resolve_ip yes
user_ip no
```

O comando *topuser_sort_field* é utilizado para organizar a seção de usuários, neste caso a organização será feita pelo maior número de *Bytes* de cada usuário.

```
topuser_sort_field BYTES reverse
```

O próximo comando, *user_sort_field*, irá organizar a seção de usuários da mesma forma que o item anterior, através dos Bytes acessados

```
user_sort_field BYTES reverse
```

Para ambos os casos o comando poderá ser USER, ordenado por nome de usuário; CONNECT, ordenado por número de conexão; BYTES, ordenado por número de Bytes que é o nosso caso; TIME, ordenado por tempo de acesso.

O comando seguinte, *exclude_users*, indica quais usuários deverão ser excluídos dos relatórios.

```
exclude_users none
```

Semelhante ao comando anterior, este (*exclude_hosts*), indicará não os usuários mas os *hosts* que não devem estar nos relatórios.

```
exclude_hosts none
```

```
useragent_log none
```

O comando abaixo *date_formate*, define qual será o formato da data, onde, as opções são *e, u, w*, e representam respequitivamente dd/mm/yy, mm/dd/yy, = yy/ww.

```
date_format e
```

O comando a seguir, *per_usre_limit*, pode ser usada para incapacitar acesso de usuário se o usuário exceder um limite de *download*.

```
per_user_limit none
```

lastlog 0

O próximo comando *remove_temp_files*, é utilizado para remover arquivos temporários após o uso.

```
remove_temp_files yes
```

O comando *index* gerar o arquivo *index.html.*

```
index yes
```

overwrite_report é o comando utilizado para sobrescrever os relatórios se já existirem.

```
overwrite_report yes
```

O comando *records_without_userid* serve para ignorar registros sem usuário.

```
records_without_userid ip
```

O próximo comando mail_utility é um utilitário usado para envio do e-mail com os relatórios.

```
mail_utility mail
```

topsites_num indica a quantidade de sites que será exibido no relatório que indicará os sites mais acessados, e para esse relatório foi utilizado os 100 mais.

```
topsites_num 100
```

O próximo comando indica que diz para ordenar os sites mais acessados, correspondente ao comando acima, por conexão (CONNECTI) em forma decrescente (D), ele também poderia ser ordenado por Bytes transmitidos. A ordenação poderia ser feito de forma ascendente (A).

Opções: *CONNECT/BYTE A/D*

```
topsites_sort_order CONNECT D
```

exclude_codes define quais arquivos de código HTTP devem ser ignorados no relatório.

```
exclude_codes /etc/sarg/exclude_codes
```

max_elapsed indica qual o tempo de checagem máximo em milesegundos dos arquivos do SARG.

```
max_elapsed 28800000
```

report_type define o tipo de relatório a ser gerado no SARG, eles podem ser:

topsites – Mostra o *site*, conexão e bytes.
sites_users – Mostra que usuários estavam acessando um *site*
users_sites – Mostra sites acessados pelo usuário.
date_time – Mostra quantidade de *bytes* usados por dia e hora
denied – Mostra todos os sites negados com *URL* completa
auth_failures – Mostra falhas de autenticação.

```
report_type topsites sites_users users_sites sites_users
     date_time denied auth_failures

usertab none
```

O *long_url* seve para exibir URLs completas. Ele gera informações seqüenciais e não seqüenciais.

```
long_url no
```

O comando date_teme_by indica que os relatórios de *Date/Time* usarão *bytes* ou decorrerão tempo.

```
date_time_by bytes
```

Para finalizar, o comando charset indica uma série completa de *byte* único e unificado de multi-línguas, codificado a (8*bit*) de caráter gráfico, com o objetivo de escrever em idiomas alfabéticos

```
charset Latin1
```

3.3. Servidor *Proxy* (*Squid*)

O *Squid* como as outras ferramentas, já vêm com uma pré-configuração e outras linhas de comandos comentados para uso do administrador se desejar, caso precise alterar estes valores, descomente a linha e troque pelos valores adequados e compatíveis.

http_port indica qual a porta o *Squid* irá atender as requisições feitas a ele. O *default* é 3128. Um outro exemplo é *http_port 3000.*

```
http_port 3128
```

O *Squid* utiliza bastante memória por razões de performance, ele leva muito tempo para ler algo do disco rígido, por isso o faz diretamente da memória., então recomenda-se colocar no máximo 1/4 da quantidade de RAM (*Random Acess Memory*) de sua máquina no comando *cache_mem*, se não for um serviço dedicado desta máquina. Se a máquina roda apenas o *Squid*, pode-se colocar metade da memória para seu uso. Por exemplo, em uma máquina com 64MB de memória:

cache_mem 32 *MB*

Este trabalho utiliza uma memória de 96MB.

```
cache_mem 96 MB
```

cache_swap_low , *cache_swap_high,* estes comandos definem os valores mínimo e máximo para reposição de objetos armazenados. Estes valores são expressos em porcentagem. Quanto mais próximo ao valor máximo, mais objetos são descartados do *cache* para entrada de novos.

O *default* sendo 90% para *cache_swap_low* e 95% para *cache_swap_high*.

```
cache_swap_low 90
cache_swap_high 95
```

maximum_object_size, medido em *bytes*, especifica o tamanho máximo dos arquivos a serem cacheados. Quaisquer objetos maiores do que este tamanho, não é salvo no disco. O *default* é 4MB, ou seja, 4096 KB.

```
maximum_object_size 4096 KB
```

cache_dir é o diretórios de *cache* no servidor. Pode-se especificar múltiplas linhas *cache_dir* para dividir a *cache* entre diferentes partições da HD (Hard Disk). A sintaxe desta linha é:

cache_dir Tipo Path MB N1 N2

Onde:

Tipo: especifica o tipo de sistema de alocação que será usado. Geralmente é do tipo "*ufs*".

Path: especifica o diretório onde os arquivos serão armazenados. O *Squid* não cria este diretório, ele deve existir. Note que, caso nenhuma entrada *cache_dir* for especificada, o sistema utilizará o diretório */var/spool/squid;*

Obs.: Na versão Conectiva Linux 7.0, o diretório de *cache* do *Squid* é: */var/cache/squid*;

MB: é a quantidade máxima de espaço a ser utilizado neste diretório.

N1: especifica o número máximo de subdiretórios que poderão ser criados abaixo do diretório de *cache*;

N2: especifica o número máximo de subdiretórios que poderão ser criados abaixo dos subdiretórios criados em N1.

```
cache_dir ufs /var/cache/squid 900 16 256
```

Com isto dizemos para o *Squid* utilizar o diretório */var/cache/squid*, até 900 *MB*, criando 16 sub-diretórios e 256 sub-diretórios abaixo deste último.

cache_access_log é o comando que indica o arquivo no qual será gerado *log* dos acessos ao servidor. O *default* é */var/log/squid/access.log*

```
cache_access_log /var/log/squid/access.log
```

cache_log é o comando que indica o arquivo onde são guardadas informações gerais sobre o comportamento da *cache*. O *default* é */var/log/squid/cache.log*

```
cache_log /var/log/squid/cache.log
```

Aparentemente o comando *cache_store_log* indicará o diretório onde será armazenado um "*tracking*" dos objetos do *Squid*, esse "*tracking*" seria as seguintes informações: quando entram para a memória, quanto tempo ficam lá, e quando são retirados da mesma. Essa configuração assume esse diretório como sendo */var/log/squid/store.log*

```
cache_store_log /var/log/squid/store.log
```

Os comandos *cache_effective_user e cache_effective_group* indicam que se o root inicializar o servidor *Proxy*, ele irá mudar seu efetivo UID/GID para o especificado abaixo, por questões de segurança. Geralmente se muda o UID/GID abaixo para *nobody*.

```
cache_effective_user proxy
cache_effective_group proxy
```

Já o próximo comando, error_directory, é utilizado para indicar o caminho (diretório) onde estão as mensagens de erro que o *Squid* reporta para o navegador. por exemplo, as respostas são dadas em inglês, e encaminhado para um diretório onde tem as mensagens em português.

EX.: *access Deny* -> Acesso Proibido. Alem disso você pode editar as mensagens, elas estão em formato HTML.

```
error_directory /etc/squid/errors/Portuguese
```

Opções de Segurança:

A grande maioria dos administradores de sistemas provavelmente irão desejar definir uma política de segurança no *Squid*, isto é, definir quem irá acessar e o que poderá ser acessado.

O primeiro passo para a definição de controle de acesso ao *Proxy* do *Squid* é a criação de listas de acesso (*acl*).

As listas de acesso meramente dão nomes a objetos. Estes objetos podem ser domínios de origem, domínios de destino, endereços de IP, etc.

A forma geral de uma linha de lista de acesso é:

```
acl NOME TIPO OBJ1 OBJ2...
```

Onde:

NOME: é um nome que será utilizado para identificar esta lista de acesso;

TIPO: indica o que é o objeto a que nos referimos nesta linha. Pode ser: situações que partiram da rede.

OBJ1 e OBJ2: podem ser domínios de origem, domínios de destino, endereços IP, etc.

O campo abaixo é um campo comentado devido ao símbolo "#" (tralha) à sua frente.

```
# ACL's
```

O *Squid* define *access lists* padrões, as quais estão abaixo:

O próximo acl, define todos os *hosts* da rede (0.0.0.0/0.0.0.0) com o nome "*all*".

```
acl all src 0.0.0.0/0.0.0.0
```

O campo "*proto*" nesta linha de comando abaixo, significa que a *acl* bloqueia um protocolo específico, neste caso o protocolo "*cache_object*". Poderia ser os protocolos FTP ou HTTP. Se você não conhece o protocolo "*cache_object*", não se preocupe é um protocolo apenas do *Squid* que retorna informação para o servidor de como a *cache* está configurada, ou como ela está rodando.

```
acl manager proto cache_object
```

A *acl* abaixo define qual é a máquina *localhost*, que por sua vez recebe o mesmo nome. Ela especifica uma lista de acesso chamada *_localhost_* definida como requisições vindas da máquina local (127.0.0.1).

```
acl localhost src 127.0.0.1/255.255.255.255
```

As próximas *acls* contém as portas consideradas seguras para o *Proxy*. Todas as outras portas são consideradas inseguras, e o acesso é negado.

```
acl SSL_ports port 443 563
acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443 563
acl Safe_ports port 70
acl Safe_ports port 210
acl Safe_ports port 1025-65535
acl Safe_ports port 280
```

```
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
```

A a*cl* seguinte contem o método de acesso aos arquivos na rede (GET, POST). O método CONNECT vale tanto por GET (receber) como por POST (enviar).

```
acl CONNECT method CONNECT
```

A próxima a*cl* tem a finalidade de rejeitar acesso à rede da administração

```
acl rede_adm src 192.168.0.1-192.168.0.50
```

Assim coma a a*cl*, esta tem como objetivo proibir acesso a sites indevidos

```
acl proibe_sites dstdomain -i "/etc/squid/listas/sites"
```

Onde:

dstdomain: especifica um domínio de destino, ou seja, entram nesta categoria as requisições de objetos localizados naquele domínio;

"*/etc/squid/listas/sites*": é o arquivo onde estão os domínios que serão rejeitados.

Acl que proíbe acesso a sites que contem palavras indevidas em seus endereços é a seguinte.

```
acl proibe_palavras url_regex -i "/etc/squid/listas/palavras"
```

Onde:

"*/etc/squid/listas/palavras*": arquivo onde estão listadas todas os domínios de palavras que serão rejeitados.

A próxima a*cl* é a que libera o acesso a sites que contem palavras que normalmente seriam bloqueadas.

```
acl libera_palavras url_regex -i
"/etc/squid/listas/libera_palavras"
```

Onde:

"*/etc/squid/listas/libera_palavras*": arquivo onde estão listados todos os domínios de palavras que serão liberados e que antes estavam rejeitados.

Atenção: o domínio é liberado de um endereço específico, qualquer outro endereço com o mesmo domínio será bloqueado.

A seguinte *acl* informa os *downloads* que serão proibidos de se fazer.

```
acl proibe_downloads urlpath_regex -i
"/etc/squid/listas/proibe_downloads"
```

Onde:

"*/etc/squid/listas/proibe_downloads*": arquivo onde estão listados os domínios de *downloads* que serão. Rejeitados.

A a*cl* seguinte indica a liberação de *downloads* que normalmente seriam bloqueadas.

```
acl libera_downloads url_regex -i
"/etc/squid/listas/libera_downloads"
```

Onde:

"*/etc/squid/listas/libera_downloads*": arquivo onde estão listados os domínios que antes rejeitados agora são liberados..

Atenção: o domínio é liberado de um *download* específico, qualquer outro domínio de *download* com o mesmo nome e extensão será bloqueado.

O próximo *acl* define qual será o horário de funcionamento do Squid

```
acl horario time MTWHF 06:00-23:00
```

Onde:

time: especifica uma expressão descrevendo “tempo”

Agora que já temos as *access lists*, precisamos aplicá-las informando ao *Squid* se o acesso a elas será ou não permitido. O campo *http_access* é responsável por esta tarefa.

```
# TAG: http_access
```

O comando *http_access allow manager* dá acesso ao protocolo *cache_object* apenas para o próprio servidor (*localhost*).

```
http_access allow manager localhost
```

http_access deny nega o acesso ao protocolo *cache_object* para qualquer outra máquina.

```
http_access deny manager
```

http_access deny nega o acesso a qualquer outra porta além das definidas na *acl Safe_ports*.

```
http_access deny !Safe_ports
```

É perigoso permitir ao *Squid* conectar-se a certas portas. Por exemplo, pode-se usar o *Squid* como *relay* de SMPT (*e-mail*). *Relays* de SMTP são uma das formas possíveis de se "*floodar*" (lotar) nossos *mailboxes*. Para prevenir o *relay* de *e-mails*, o *Squid* nega requisições quando o número da porta da *URL* é 25 (porta SMTP). Outras portas também são bloqueadas.

A regra *http_access deny !Safe_ports* informa ao *Squid* para negar o acesso a qualquer porta que não esteja na lista *Safe_ports*. A regra *http_access deny* CONNECT !SSL*_ports* nega qualquer conexão que não seja referente às portas seguras.

O padrão do *Squid* é negar acesso a tudo E a todos. Para permitir a utilização do *Proxy* do *Squid*, você deve configurá-lo para permitir o acesso

```
http_access deny CONNECT !SSL_ports
```

O comando *http_access deny proibe_downloads* proíbe os *downloads* que contenham palavras existentes no arquivo *proibe_downloads*

```
http_access deny proibe_downloads !proibe_downloads
```

http_access deny proibe_downloads nega o acesso a qualquer outra *download* além das definidas na *acl libera_download*...

```
http_access deny proibe_downloads !libera_downloads
```

http_access deny proíbe o acesso a URL que contenham os endereços existentes no arquivo *proibe_sites*

```
http_access deny proibe_sites
```

http_access deny proibe_palavras nega o acesso a qualquer outra *URL* além das definidas na *acl libera_palavras*...

```
http_access deny proibe_palavras !libera_palavras
```

O próximo comando *http_acess deny* não restringe nem um pouco o acesso ao seu *Proxy*. Pelo contrário, permite o acesso ao *Proxy* a partir de qualquer máquina na *Internet*.

```
http_access deny all
```

O comando abaixo *icp_access allow* permite que qualquer um acesse o *Proxy*

```
icp_access allow all


visible_hostname on
```

É possível apresentar um *hostname* “especial” em mensagens de erro e outras mensagens, especificando o “*hostname*”. Se não for especificado, é usado o valor retorno de *gethostbyname (),* (normalmente o próprio *hostname* do servidor Proxy)

Os comandos abaixo fazem o *Squid* rodar como acelerador *Web* ou *Proxy* transparente.

```
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
httpd_accel_port 80
httpd_accel_host virtual
```

3.4. Servidor *Apache* ou *http.conf*

Nesta seção iremos configurar o IP e porta que o servidor virtual terá. A definição deste é que você não precisa ter vários computadores rodando *http servers* neles, com apenas um você pode ter *www.teste.com* e *www.teste1.com*, cada um abrindo uma página diferente (em diferentes diretórios do CPU (*Central Processing Unit*)) e cada um possuindo um IP (mas ambos apontarão para o mesmo CPU, isso se chama *IP ALIAS*).

O comando abaixo *NameVirtualHost* indica o nome o *Host Vitual*, usa-se o número de IP do servidor.

```
NameVirtualHost IP_DO_SERVIDOR
```

O comando *ServerType* diz ao sistema se o *httpd* vai ser rodado via script próprio (*standalone*), ou a partir do arquivo *inetd.conf (inetd)*. (em "*inetd*" o *httpd* fica ocioso, enquanto o *inetd* fica monitorando as requisições, quando houver alguma, ele avisa e o serviço começa a funcionar)

```
ServerType standalone
```

O próximo comando *ServerRoot* cuida do caminho do diretório onde irão ficar os arquivos de configuração. Pode ser mudado se necessário

```
ServerRoot /etc/httpd
```

PidFile indica o arquivo que o servidor gravará os detalhes sobre seu PID (*Process Identifier*) quando iniciar

```
PidFile /var/run/httpd.pid
```

ScoreBoardFile aponta o arquivo usado para armazenar detalhes do processo interno do servidor. Nem todas as arquiteturas requerem esta diretiva, mas se a sua requerer (você saberá porque este arquivo será criado quando executar o *Apache*) então você deverá ter certeza que dois processos do *Apache* não utilizam o mesmo arquivo *ScoreBoardFile*.

```
ScoreBoardFile /var/run/httpd.scoreboard
```

Timeout é o tempo máximo (em segundos) que o servidor esperará, mantendo uma conexão aberta com o cliente. Se o limite for excedido, ele terá de criar uma nova conexão com o mesmo, a linha de código abaixo indica o valor como sendo de 300 segundos.

```
Timeout 300
```

O comando *KeepAlive* é diretamente ligado com a opção acima, ele define se o processo de manter a conexão com o cliente está ativo ou não.

```
KeepAlive On
```

MaxKeepAliveRequests representa o número máximo de conexões mantidas, sem necessidade de renovação. Quanto mais alto o número, melhor a performance (com o *hardware* adequado), foi usado nesta configuração o valor 50.

```
MaxKeepAliveRequests 50
```

O comando *KeepAliveTimeout* indica o máximo (de segundos) a espera de nova requisição, onde o tempo definido foi de 10 segundos.

```
KeepAliveTimeout 10
```

Regulagem do tamanho de *pool* do servidor. Ao invés de fazer você adivinhar quantos processos os servidores precisará, o *Apache* adapta dinamicamente de acordo com a carga que

ele vê, isto é, ele tenta manter o número de processos o bastante para manipular a carga atual, mas alguns poucos servidores esparsos para manipular requisições transientes.

Ele faz isto verificando periodicamente quantos servidores estão aguardando por uma requisição. Se lá existe menos que *MinSpareServers*, ele cria um novo processo. Se existe mais que *MaxSpareServers*, ele fecha alguns processos. O mínimo de servidores aguardando para esta configuração é 2 e o máximo é 4.

```
MinSpareServers 2
MaxSpareServers 4
```

StartServers informa o número de servidores iniciais, ou seja, logo no início do processo, o *httpd* poderia responder a 10 conexões simultâneas ao mesmo *site*, no entanto, para este foi indicado 2 servidores.

```
StartServers 2
```

MaxClients limita o número de clientes que podem conectar-se simultaneamente, se este limite é sempre atingido, os clientes poderão ser barrados, assim este valor não deve ser muito pequeno. Ele tem a intenção principal de ser um freio para manter um em execução com uma performance aceitável de acordo com os requerimentos de construção e carga calculada no servidor. O número de clientes para está configuração foi de um limite de 150 clientes

```
MaxClients 150
```

MaxRequestsPerChild é o número de requisições que cada processo tem permissão de processar antes do processo filho ser finalizado. O filho será finalizado para evitar problemas após o uso prolongado quanto ao *Apache.*

```
MaxRequestsPerChild 500
```

O comando *ation* permite definir os tipos de mídia que executarão um *script* quando um arquivo que conferir for chamado. Isto elimina a necessidade de caminhos de URLs repetidas para processadores de arquivos CGI (*Common Gateway Interface*) freqüentemente usados.

```
ation.
```

AddDefaultCharset é o comando que permite o uso das preferências padrões de exibição de caracteres

```
AddDefaultCharset On
```

Descomentando quaisquer das linhas que comecem com *LoadModule* ou *AddModule*, valida o carregamento de módulos feito na inicialização do *httpd*. Estes funcionam como opções, por exemplo, habilitar ou não o suporte a arquivos CGI no servidor, etc

```
LoadModule env_module          modules/mod_env.so
LoadModule define_module       modules/mod_define.so
LoadModule config_log_module   modules/mod_log_config.so
LoadModule agent_log_module    modules/mod_log_agent.so
LoadModule referer_log_module  modules/mod_log_referer.so
LoadModule mime_module         modules/mod_mime.so
LoadModule negotiation_module  modules/mod_negotiation.so
LoadModule status_module       modules/mod_status.so
LoadModule info_module         modules/mod_info.so
LoadModule includes_module     modules/mod_include.so
LoadModule autoindex_module    modules/mod_autoindex.so
LoadModule dir_module          modules/mod_dir.so
LoadModule cgi_module          modules/mod_cgi.so
LoadModule asis_module         modules/mod_asis.so
LoadModule imap_module         modules/mod_imap.so
LoadModule action_module       modules/mod_actions.so
LoadModule userdir_module      modules/mod_userdir.so
LoadModule proxy_module        modules/libproxy.so
LoadModule alias_module        modules/mod_alias.so
LoadModule rewrite_module      modules/mod_rewrite.so
LoadModule access_module       modules/mod_access.so
LoadModule auth_module         modules/mod_auth.so
LoadModule anon_auth_module    modules/mod_auth_anon.so
LoadModule db_auth_module      modules/mod_auth_db.so
LoadModule digest_module       modules/mod_digest.so
LoadModule expires_module      modules/mod_expires.so
LoadModule headers_module      modules/mod_headers.so
LoadModule usertrack_module    modules/mod_usertrack.so
LoadModule setenvif_module     modules/mod_setenvif.so

<IfDefine SSL>
   LoadModule ssl_module          modules/libssl.so
```

```
        </IfDefine>

    ClearModuleList
       AddModule mod_env.c
       AddModule mod_define.c
       AddModule mod_log_config.c
       AddModule mod_log_agent.c
       AddModule mod_log_referer.c
       AddModule mod_mime.c
       AddModule mod_negotiation.c
       AddModule mod_status.c
       AddModule mod_info.c
       AddModule mod_include.c
       AddModule mod_autoindex.c
       AddModule mod_dir.c
       AddModule mod_cgi.c
       AddModule mod_asis.c
       AddModule mod_imap.c
       AddModule mod_actions.c
       AddModule mod_userdir.c
       AddModule mod_proxy.c
       AddModule mod_alias.c
       AddModule mod_rewrite.c
       AddModule mod_access.c
       AddModule mod_auth.c
       AddModule mod_auth_anon.c
       AddModule mod_auth_db.c
       AddModule mod_digest.c
       AddModule mod_expires.c
       AddModule mod_headers.c
       AddModule mod_usertrack.c
       AddModule mod_so.c
       AddModule mod_setenvif.c
       AddModule mod_bandwidth.c

    <IfDefine SSL>
       AddModule mod_ssl.c
    </IfDefine>
```

O comando *Port* faz com que o *httpd* responde a porta indicada, por *default* a porta é a 80, neste campo você poderá modificá-la se quiser.

```
Port 80
```

User/Group é o nome (ou número) do usuário/grupo que executará o servidor *httpd.conf*.

```
User www
Group www
```

É sugerido que seja criado um usuário *www* e executar o servidor *httpd* como este usuário, adequando as permissões onde necessárias.

ServerAdmin é o comando que informa o endereço de *e-mail* para onde será mandado algo se o servidor acusar erro ou anormalidades, normalmente este *e-mail* deve ser a do administrador da rede.

```
ServerAdmin root@localhost
```

DocumentRoot determina o caminho onde estarão os arquivos *html* do servidor principal. Importante: o diretório deve estar com permissão 755 (*chmod* 755, este comando permite leitura, escrita e execução para o dono, leitura e execução para o grupo e outros que não sejam do grupo nem donos (*others*)). O comando *chmod* deve ser digitado direto na plataforma *Unix*.

```
DocumentRoot /var/www/default
```

O conjunto de campos indicado em <*Directory "/var/www/default"*> determinam as opções que os diretórios onde contém documentos HTMLs a serem acessados irão ter. A primeira "*This should..*", deve conter o mesmo diretório que o "*DocumentRoot*" tem (o /*html*).

A opção *Options* pode conter os valores "*None*", "*All*", ou quaisquer combinação de "*Indexes*", "*Includes*", "*FollowSymLinks*", "*ExecCGI*", ou "*MultiViews*".

Note que "*MultiViews*" deve ser explicitamente especificada, "Options *All*" não a ativa (pelo menos não ainda).

A opção *AllowOverride* informa que opções os arquivos *.htaccess* nos diretórios podem ser substituídas. Pode também conter "*All*", ou qualquer combinação de "Options", "*FileInfo*", "*AuthConfig*", e "*Limit*"

As duas outras opções *Order allow* e *Allow from* controlam quem pode obter materiais deste servidor.

```
<Directory "/var/www/default">
```

```
    Options Indexes FollowSymLinks Includes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

O diretório "*/usr/lib/cgi-bin*" deve ser modificado para o diretório que possuem seus *scripts* CGI, caso tenha configurado o suporte a CGI's no servidor. O comando abaixo tem a mesma funcionalidade do superior a diferença é que este, o diretório é *<Directory "/usr/lib/cgi-bin">*

```
<Directory "/usr/lib/cgi-bin">
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>
```

Apresenta as mesamas caracteristicas anteriores. Permite a visualização do diretório de ícones, o qual esse diretório seria *<Directory "/var/www/icons">*

```
<Directory "/var/www/icons">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

<Directory />
    Options None
    AllowOverride None
</Directory>
```

Este comando é bem útil. *UserDir* cuida de qual diretório, o usuário terá de fazer se quiser ter uma página em seu *home*. No caso, como está configurado, ele precisará criar um diretório *public_html* e colocar algo em html, podendo ser acessado com http://nome.da.maquina/~nome-do-usuário. Importante: como mencionado anteriormente, este e todos os diretórios anteriores precisam ter permissões 755 a fim de garantir acesso.

```
UserDir public_html
```

O comando seguinte, *DirectoryIndex*, é bastante importante, pois determina quais nomes de arquivos serão válidos para realizar a abertura dos mesmos em um *browser http*. No caso da configuração acima, o serviodor aceitará arquivos de nome *index.html*, *index.htm* e *index.cgi* como arquivos iniciais de uma *home page*

```
DirectoryIndex index.html index.wml
```

AccessFileName indica o nome do arquivo que será procurado em cada diretório que contém detalhes sobre as permissões de acesso a um determinado diretório e opções de listagem. Deve-se ter cuidado ao modificar o nome deste arquivo, muitas definições que trabalham em cima do nome *.htaccess* nos arquivos de configuração deverão ser modificados para não comprometer a segurança de seu servidor. Uma falta de atenção neste ponto poderá deixar este arquivo visível em qualquer listagem de diretórios facilmente...

```
AccessFileName .htaccess
```

As seguintes linhas de comando correspondente ao arquivo *.htaccess* previnem eles de serem mostrados nos clientes *Web*. Pois os arquivos *.htaccess* freqüentemente contém detalhes de autorização. O acesso é desabilitado por razões de segurança.

```
<Files .htaccess>
    Order allow,deny
    Deny from all
</Files>
```

O comando UseCanonicalName permite que se ligada, uma página que por exemplo se chame http://www.teste.com/teste/ e seja acessada como http://www.teste.com/teste (sem o / (barra) no final) seja válida, quando o comando vem seguido da opção On. Se desligada (Off), ele não irá achar mais a página.

```
UseCanonicalName On
```

O comando abaixo, *TypesConfig*, especifica o arquivo de configuração que contém os tipos usados pelo servidor

```
TypesConfig /etc/mime.types
```

DefaultType é o tipo MIME padrão que o servidor utilizará para um documento caso ele não possa determinar seu conteúdo, como através de extensões de arquivos. Se o servidor

contém em sua maioria texto ou documentos em HTML, "*text/plain*" é um bom valor. Caso a maioria do conteúdo seja binários, tal como aplicativos ou fotos, o tipo mais adequado ao seu caso poderá ser "*application/octet-stream*" para evitar que navegadores tentem exibir aplicativos binários como se fossem texto.

```
DefaultType text/plain
```

A diretiva *MIMEMagicFile* diz ao módulo onde as definições de dicas estão localizadas. O módulo *mod_mime_magic* não é parte do servidor padrão *Apache*.

Isto significa que a diretiva *MIMEMagicFile* somente será processada caso o módulo estiver ativo no servidor.

```
<IfModule mod_mime_magic.c>
    MIMEMagicFile conf/magic
</IfModule>
```

HostnameLookups registra os nomes DNS dos clientes ou apenas seus endereços IP's. O valor padrão é *off* porque permitirá menos tráfego na rede. Ativando esta opção significa que cada acesso de um cliente resultará em “no mínimo” uma requisição de procura ao servidor de nomes (DNS).

```
HostnameLookups off
```

O relatório de erros do servidor virtual é criado pelo comando *ErrorLog* e vai ser escrito em *logs/error_log*

```
ErrorLog logs/error_log
```

LogLevel determina em que nível o *httpd* irá rodar, controla o número de mensagens registradas no *ErrorLog*. É recomendado usar a opção *warn* pois não causa acúmulo de atividades no apache e é uma das mais usadas, mas elas podem ser também *debug*, *info, notice, error, crit, alert, emerg*.

```
LogLevel warn
```

As seguintes diretivas de *LogFormat* definem alguns formatos de nomes que serão usadas com a diretiva *CustomLog*.

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-
       Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

```
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
```

Para que os *logs* de acessos sejam escritos em *logs/access_log common* o comando utilizado é *CustomLog*.

```
CustomLog logs/access_log common
```

A finalidade do comando *ServerSignature* é incluir uma linha contendo a versão do servidor e um nome de *host* virtual para as páginas geradas pelo servidor (documentos de erro, listagens de diretórios FTP, saída dos módulos *mod_status* e *mod_info*, etc., exceto para documentos gerados via CGI). Use o valor "*EMail*" para também incluir um link *mailto*: para o *ServerAdmin*. Escolha entre "*On*", "*Off*" ou "*EMail*".

```
ServerSignature On
```

Alias nomeurl nomereal - "*nomeurl*" é o caminho especificado na URL e "*nomereal*" é a localização do documento no sistema de arquivos local

Note que se você incluir uma / (barra) no fim de "*nomeurl*", então o servidor requisitará que também esteja presente na URL. Para esta configuração o caminho especificado na URL é */icon/* e a localização do documento no sistema de arquivos local é */var/www/icons/*.

```
Alias /icons/ "/var/www/icons/"
```

Esta diretiva *ScriptAlias* controla que diretórios contém *scripts* do servidor.

```
ScriptAlias /cgi-bin/ "/usr/lib/cgi-bin/"
```

FancyIndexing: se você deseja o padrão *fancy index* ou padrão para a indexação de arquivos no diretório. Usando *FancyIndexing* o servidor *Apache* gerará uma listagem de arquivos que poderá ser ordenada, usar tipos de ícones e *encoding*, etc.

```
IndexOptions FancyIndexing
```

As diretivas *AddIcon* dizem ao servidor que ícone mostrar para um determinado arquivo ou extensão de arquivos. Estes somente são mostrados para os diretórios classificados através da opção *FancyIndexing*.

```
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
```

```
AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*

AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif core
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^
```

DefaultIcon apresenta o ícone que será mostrado para aplicativos que não tiverem um ícone explicitamente definido.

```
DefaultIcon /icons/unknown.gif
```

A diretiva *ReadmeName* é onde define o nome do arquivo LEIAME que o servidor procurará como padrão. Estes serão inseridos no fim da listagem de diretórios. O nome *README* será o nome do arquivo.

```
ReadmeName README
```

Finalizando o comando acima o servidor procurará primeiro por *README.html*, incluído se ele for encontrado, e então procurará pelo nome e o incluirá como texto plano, se encontrado.

Já *HeaderName* é o comando que informa o nome do arquivo que deve ser colocado no topo do índice de diretórios. As regras de procura de nome são as mesmas do arquivo *README*

```
HeaderName HEADER
```

Com o comando *IndexIgnore* você indica um conjunto de nomes de arquivos que a listagem de diretórios deve ignorar e não incluir na listagem. É permitido o uso de coringas como no interpretador de comandos.

```
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
```

Os comandos AddEncoding x-xompress e AddEnconding x-gzip gz, permitem que alguns navegadores (*Mosaic/X 2.1+*, *Netscape*, etc) descompactem dados durante sua abertura.

Nota: Nem todos os navegadores suportam isto. Esqueça os nomes parecidos, as seguintes diretivas *Add* não tem nada a ver com personalizações da opção *FancyIndexing* usada nas diretivas acima.

```
AddEncoding x-compress Z
AddEncoding x-gzip gz
```

Através das diretivas *AddLanguage* você especificar o idioma do documento. Você pode então usar a negociação de conteúdo para dar ao navegador um arquivo no idioma solicitado.

Nota 1: O sufixo não precisa ser o mesmo da palavra chave do idioma

Nota 2: As entradas de exemplos abaixo mostram que em alguns casos as duas letras de abreviação do 'Idioma' não é idêntico as duas letras do 'País' para seu país

Nota 3: No caso de 'ltz' nós violamos a RFC usando uma especificação de três caracteres. Mas existe um 'trabalho em progresso' para corrigir isto e obter os dados de referência para limpar a RFC1766.

Danish (da) - Dutch (nl) - English (en) - Estonian (ee)
French (fr) - German (de) - Greek-Modern (el)
Italian (it - Italiano) - Portugese (pt) - Luxembourgeois (ltz)
Spanish (es) - Swedish (sv) - Catalan (ca) - Czech(cz)
Polish (pl) - Brazilian Portuguese (pt-br) - Japanese (ja)

Em português os países seriam nessa ordem:

Dinamarquês - Holandês - Inglês - Estoniano

Francês - Alemão - Grego Moderno

Espanhol - Sueco - Catalão - Tcheco

Polonês - Português do Brasil - Japonês

```
AddLanguage en .en
AddLanguage fr .fr
AddLanguage de .de
AddLanguage da .da
AddLanguage el .el
AddLanguage it .it
```

Para definir a prioridade para a exibição de documentos caso nenhum documento confira durante a negociação de conteúdo utiliza-se o comando *LanguagePriority*.

Para fazer isto, especifique os idiomas em ordem de preferência de exibição de idiomas. A linha de comando abaixo, lista os idimos na seguinte ordem, inglês, francês e alemão.

```
LanguagePriority en fr de
```

Os comando *AddType* permite modificar o *mime.types* sem editar o arquivo, ou fazer a associação de arquivos a certos tipos de conteúdo.

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
AddType text/vnd.wap.wml .wml
AddType image/vnd.wap.wbmp .wbmp
AddType application/vnd.wap.wmlc .wmlc
AddType text/vnd.wap.wmlscript .wmls
AddType application/vnd.wap.wmlscriptc .wmlsc
```

O comando *AddHandler* permite mapear certas extensões de arquivos a programas "manipuladores" adequados a seu conteúdo. Estes podem ser construídos no servidor ou adicionados com o comando *Action*.

Para usar arquivos *html* gerados através do servidor deve-se usar a opção *server-parsed .shtml* .

```
AddHandler server-parsed .shtml
```

Para usar arquivos de mapas de imagens processadas no servidor deve-se usar a opção *imap-file map*.

```
AddHandler imap-file map
```

As seguintes diretivas modificam o funcionamento da resposta normal do servidor HTTP. A primeira diretiva desativa o *keepalive* para o *Netscape 2.x* e navegadores que as falsificam. Existem problemas conhecidos com estas implementações de navegadores. A segunda diretiva é para o *MS IE 4.0b2* que tem uma implementação defeituosa do *HTTP/1.1* e não suporta adequadamente o *keepalive* quando ele utiliza as respostas de redirecionamento 301 e 302.

```
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-
        response-1.0
```

Já as diretivas abaixo, desativam as respostas *HTTP/1.1* para navegadores que violam a especificação *HTTP/1.0* não sendo capaz de enviar uma resposta 1.1 básica.

```
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
```

Os comandos abaixo permite fazer o *Apache* escutar um *IP* determinado e/ou porta, em adição a padrão.

```
<IfDefine SSL>
      Listen 80
      Listen 443
</IfDefine>
```

Assim como já foi mencionado o *AddType* permite modificar o *mime.types* sem editar o arquivo, ou fazer a associação de arquivos a certos tipos de conteúdo.

```
<IfDefine SSL>
      AddType application/x-x509-ca-cert .crt
      AddType application/x-pkcs7-crl    .crl
</IfDefine>
```

```
<IfModule mod_ssl.c>
```

```
SSLPassPhraseDialog  builtin

SSLSessionCache         dbm:logs/ssl_scache
SSLSessionCacheTimeout  300

SSLMutex  file:logs/ssl_mutex

SSLRandomSeed startup builtin
SSLRandomSeed connect builtin

SSLLog      logs/ssl_engine_log
SSLLogLevel info

</IfModule>

<IfDefine SSL>
```

VirtualHost permite o *daemon* responder a requisições para mais que um endereço IP do servidor, se sua máquina estiver configurada para aceitar pacotes para múltiplos endereços de rede. Isto pode ser feito com a opção de *aliasing* do *ifconfig* ou através de *patches* do *kernel* .

Pode-se ajustar o conteúdo para manter múltiplos domínios/nomes de máquinas em sua máquina.

```
<VirtualHost _default_:443>
```

O módulo acima realiza a comunicação segura de dados (*criptografada*) via porta 443 (que é usada como padrão quando especificamos uma URL iniciando com *https://*). A transmissão *criptografada* de dados é importante quanto temos dados confidenciais que precisamos transmitir como movimentação bancária, senhas, número de cartões de crédito, fazer a administração remota do servidor, etc. SSL (*Secure Sockets Layer)* Camada Segura de Transferência.

O comando *SSLCertificateFile* apresenta o certificado do servidor

```
SSLCertificateFile
/etc/httpd/conf/ssl.crt/server.crt
```

Este comando *SSLCertificateKeyFile* relata onde está a chave privada de certificado do servidor.

```
                SSLCertificateKeyFile
            /etc/httpd/conf/ssl.key/server.key
```

Finalizando a documentação a linha abaixo força o fechamento de conexões quando a conexão com o navegador *Internet Explorer* é interrompida. Isto viola o padrão SSL/TLS (*Secure Sockets Layer/Transport Layer Security)* mas é necessário para este tipo de navegador. Alguns problemas de conexões de navegadores também são causados por não saberem lidar com pacotes *keepalive*.

```
                SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-
                          unclean-shutdown
                CustomLog logs/ssl_request_log           "%t %h %
                          {SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

        </VirtualHost>

</IfDefine>
```

4. ESTUDO DE CASO E ANÁLISE DOS RESULTADOS

O estudo de caso apresentado neste trabalho teve como cenário o laboratório de uma instituição de ensino superior. O tráfego de dados apresentado e analisado é oriundo dos laboratórios de informática, secretaria e demais departamentos que possuem computadores conectados a rede.

Visando auxiliar ao administrador de rede o gerenciamento desta instituição, visto que, são inúmeros usuários que utilizam desta rede para os mais diversos fins é que optou-se em utilizar as ferramentas MRTG e SARG, facilitando a vida deste profissional no que se refere a monitoria, gerência e auditoria da rede possibilitando uma real mensuração da utilização dos recursos providos pela referida instituição de ensino superior a cargo do administrador de rede de computadores.

Neste capítulo será apresentado o estudo de caso com base nas ferramentas para auditoria de rede e conseqüentemente será feita uma análises dos relatórios gerados pelo MRTG e SARG. Desta forma, serão mostrados no primeiro momento os gráficos gerados no MRTG e posteriormente no SARG.

4.1. Relatórios Produzidos Pelo MRTG

Neste tópico abordaremos os gráficos gerados por esta ferramenta com relação ao tráfego da rede em questão. Serão considerados os gráficos gerais diários, que são apresentados pelo MRTG e os gráficos específicos como diário, semanal, mensal e anual.

O gráfico geral, Figura 1, mostrado abaixo é uma visualização dos gráficos diários da LAN, do SROUTER (Roteador), da porta WAN e da porta WAN_02 respectivamente, o que

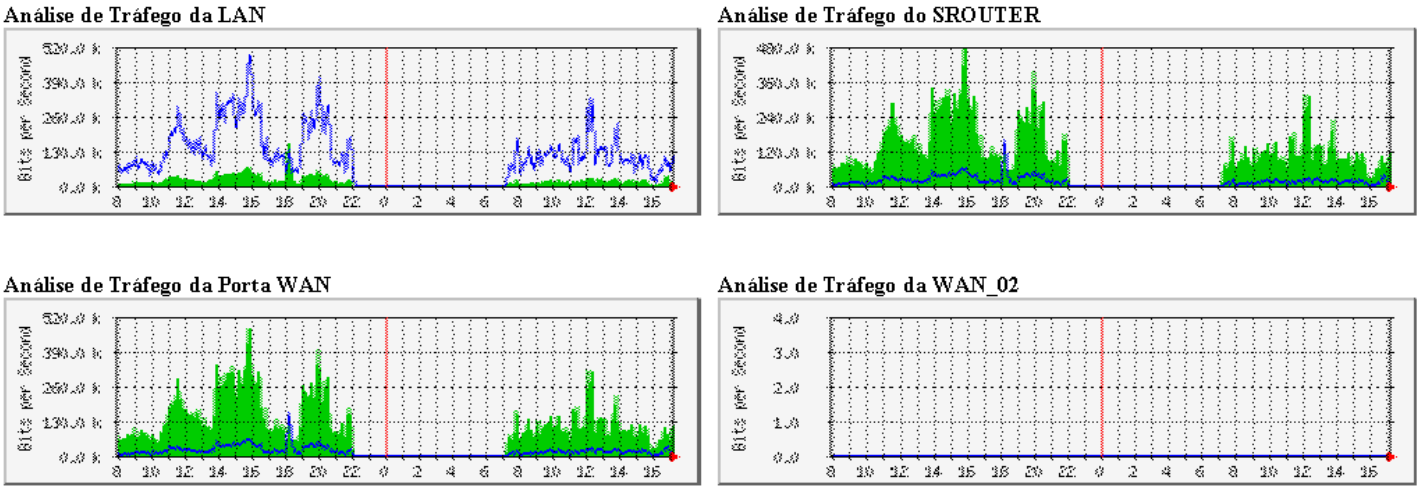


Figura 1 - Gráficos Gerais Diários do MRTG.

A Figura 1 acima apresenta 4 gráficos no relatório gerado pelo MRTG. Sendo assim, conseguimos visualizar o tráfego da rede local (Análise do Tráfego da LAN), o tráfego do roteador (Análise de tráfego do SROUTER), o tráfego da porta de conexão com a *Internet* (Análise de Tráfego da Porta WAN), e o tráfego da porta WAN 2 (Análise de Tráfego da WAN_02), que pode ser utilizada para conecta a uma filial através de *frame relay*, por exemplo.

Os dados apresentados no gráfico são referenciados em duas cores, verde e azul. A primeira refere-se a entrada de dados, ou seja, as respostas obtidas às solicitações efetuadas pela rede. A linha vertical vermelha separa dois períodos equivalentes, sejam eles dias, semanas, meses ou anos. Os dados apresentados à esquerda do gráfico representam o tráfego em *bits* por segundo, e por último, os dados abaixo do gráfico são as horas, os dias, as semanas ou os meses, de acordo com gráfico analisado.

Abaixo, será apresentado cada um dos gráficos acima para que haja um melhor entendimento quanto as suas especificações.

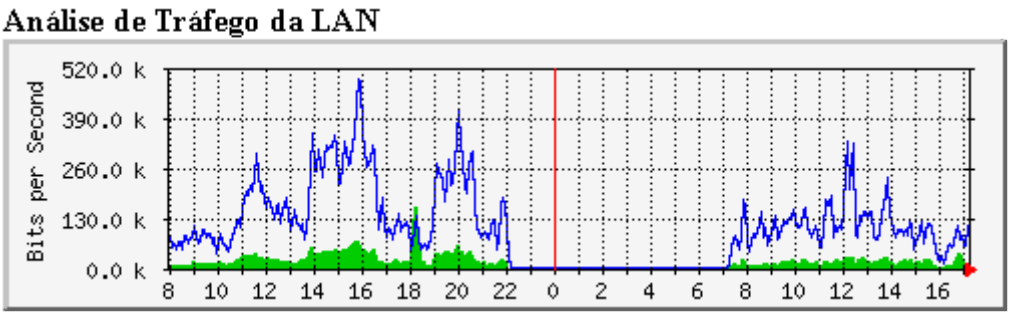


Figura 2 - Gráfico do Tráfego Diário da LAN

A Figura 2, apresentada acima, nos mostra a análise do tráfego da LAN que se refere aos dados que foram trocados internamente à rede local. Este tráfego pode indicar por exemplo, envio de recebimento de *e-mail*, acesso a servidor de banco de dados, troca de mensagens, etc.

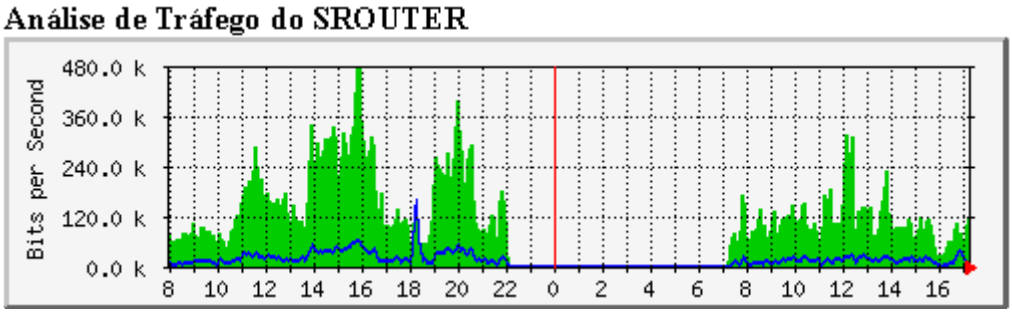


Figura 3 - Gráfico do Tráfego Diário do Roteador

A Figura 3 acima, possibilita a análise de tráfego do SROUTER o qual indica o tráfego de informação que passam pelo roteador. O tráfego que passa pelo roteador pode ser oriundo, por exemplo, da rede local em busca de informações na *Internet*.

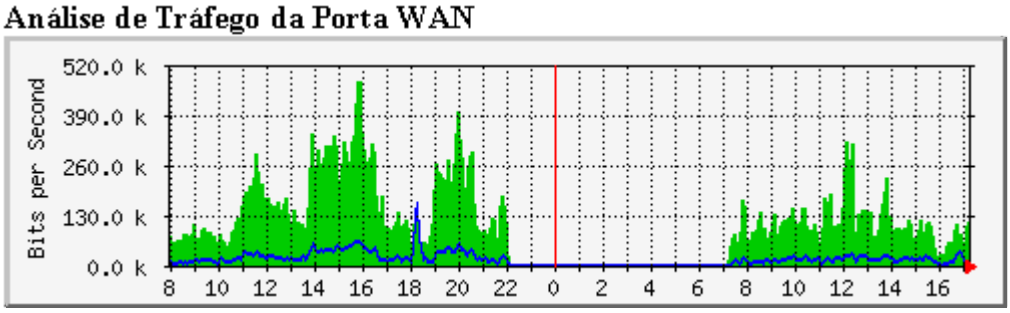
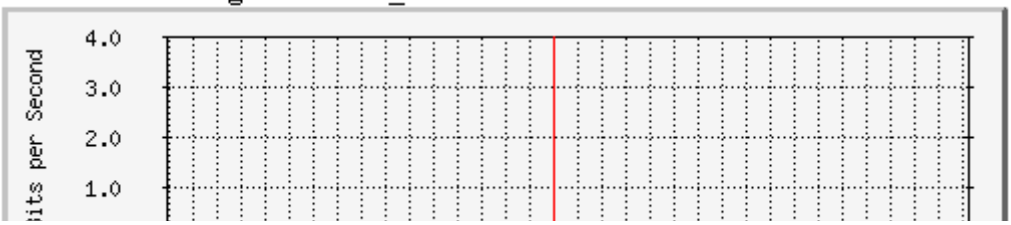


Figura 4 - Gráfico do Tráfego Diário da Porta de Acesso à *Internet*.

Acima apresentamos a Figura 4 que referencia a análise de tráfego da porta WAN, ou seja, neste gráfico são contabilizados todos os dados trocados com a *Internet* independente destas serem solicitações ou respostas às solicitações efetuadas.

Análise de Tráfego da WAN_02



Traffic Analysis for 1 --

System: in

Maintainer:

Description: LAN

ifType: ethernetCsmacd (6)

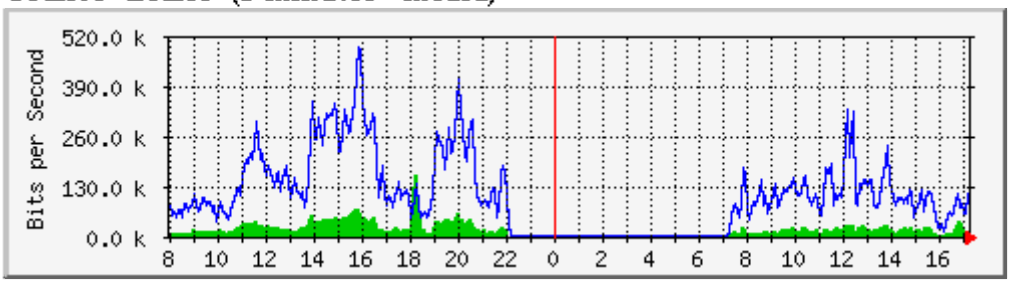
ifName:

Max Speed: 12.5 MBytes/s

Ip: IP do ROUTE

Última atualização das estatísticas: **Sexta, 29 de Outubro de 2004 às 17:18**, nesta hora dispositivo estava online por **43 days, 17:48:15**.

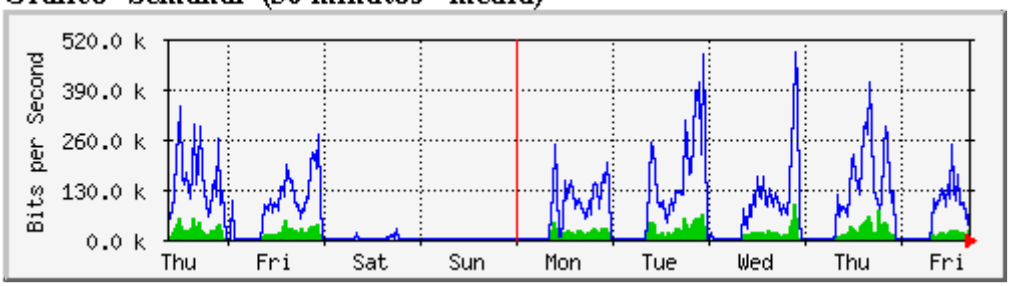
Gráfico `Diário' (5 minutos - média)



Máx Ent: 164.0 kb/s (0.2%) Média Ent: 19.6 kb/s (0.0%) Atual Ent: 11.4 kb/s (0.0%)

Máx Saí: 489.0 kb/s (0.5%) Média Saí: 105.8 kb/s (0.1%) Atual Saí: 120.0 kb/s (0.1%)

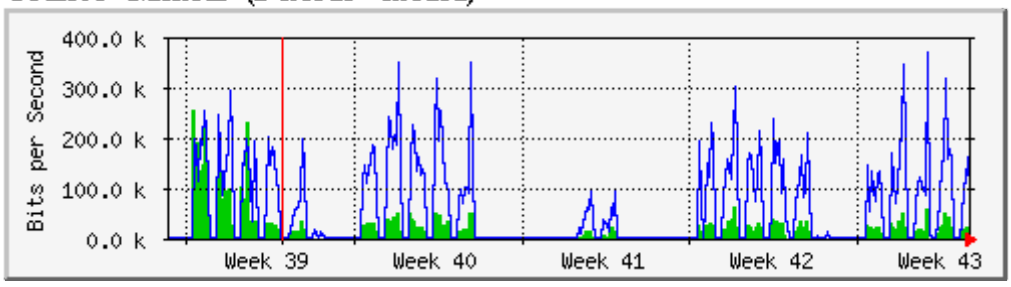
Gráfico `Semanal' (30 minutos - média)



Máx Ent: 96.2 kb/s (0.1%) Média Ent: 13.6 kb/s (0.0%) Atual Ent: 29.1 kb/s (0.0%)

Máx Saí: 486.8 kb/s (0.5%) Média Saí: 71.0 kb/s (0.1%) Atual Saí: 85.0 kb/s (0.1%)

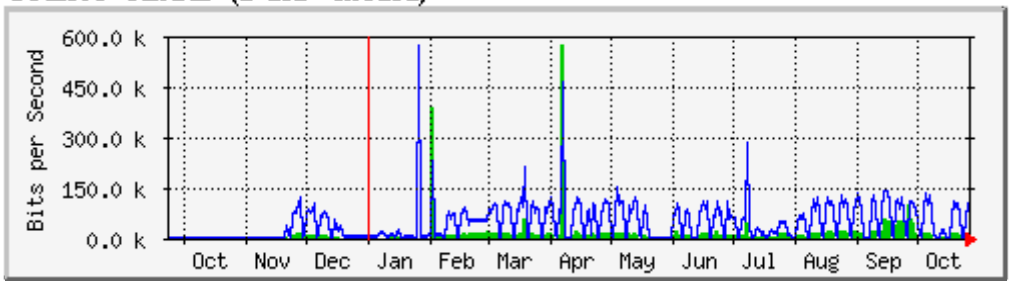
Gráfico `Mensal' (2 horas - média)



Máx Ent: 256.1 kb/s (0.3%) Média Ent: 16.0 kb/s (0.0%) Atual Ent: 19.6 kb/s (0.0%)

Máx Saí: 369.3 kb/s (0.4%) Média Saí: 59.1 kb/s (0.1%) Atual Saí: 89.2 kb/s (0.1%)

Gráfico `Anual' (1 dia - média)



Máx Ent: 578.1 kb/s (0.6%) Média Ent: 15.2 kb/s (0.0%) Atual Ent: 17.0 kb/s (0.0%)

Máx Saí: 574.8 kb/s (0.6%) Média Saí: 55.9 kb/s (0.1%) Atual Saí: 96.3 kb/s (0.1%)

MRTG MULTI ROUTER TRAFFIC GRAPHER

versão 2.9.17 Tobias Oetiker <oetiker@ee.ethz.ch> e Dave Rand <dlr@bungi.com>

Localização efetuada por Luiz Felipe R E <luizfelipe@encarnacao.com>

Figura 6 - Relatórios Gráficos de Tráfego da LAN

A Figura 6 nos permite visualizar sua descrição, sendo esta uma LAN e também nos dá sua velocidade máxima em *Bytes*, sendo de 12.5 KBytes/s

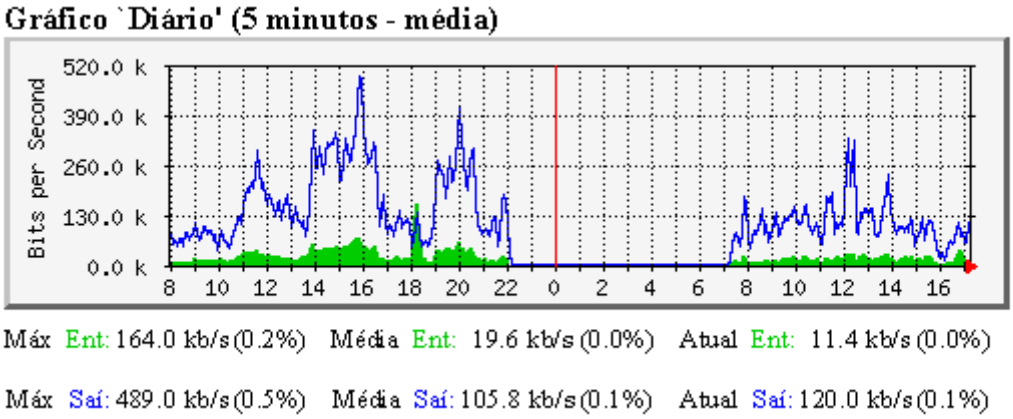


Figura 7 - Gráfico Diário de Tráfego da LAN

O gráfico apresentado na Figura 7, retrata a situação diária do tráfego na rede local referente aos dias 28 de outubro de 2004 e 29 de outubro de 2004. Por padrão o MRTG mostra o dia atual e o anterior, sendo o primeiro apresentado à direita da linha vertical vermelha e o segundo apresentado à esquerda desta linha.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

O dia 28 de outubro de 2004, referente ao lado esquerdo da linha vermelha, apresentou o maior pico de entrada (resposta) às 18 horas com um tráfego de informação de aproximadamente 163.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu aproximadamente às 16 horas apresentando um tráfego de informação próximo a 490.0 Kbps. Este mesmo dia apresentou como menor pico de entrada um valor próximo a 15.0 Kbps registrado em torno de 8 horas e como menor pico de saída foi por volta de 10 horas apresentando um resultado perto de 50.0 Kbps.

O dia 29 de outubro de 2004, que corresponde ao lado direito da linha vermelha, apresentou o maior pico de entrada (resposta) às 17 horas com um tráfego de informação de aproximadamente 50.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu aproximadamente às 12 horas apresentando um tráfego de informação próximo a 335.0 Kbps. Este mesmo dia apresentou como menor pico de entrada um valor próximo a 10.0 Kbps registrado em torno de 16 horas e como menor pico de saída foi também por volta das 15 horas apresentando um resultado perto de 20.0 Kbps.

Fazendo uma análise comparativa do dia 28 em relação ao dia 29 podemos verificar que, no dia 28 o pico máximo de saída ocorreu às 16 horas com um valor de 490.0 Kbps, nesse mesmo horário no dia 29 o tráfego foi de aproximadamente 10.0 Kbps, ou seja, o menor pico desse dia, havendo assim uma queda muito grande no tráfego nesse horário. Da mesma forma para o máximo de entrada do dia 28,este ocorreu com um valor de 163,0 Kbps às 18 horas, no entanto, para o dia 29, a coleta do gráfico se deu em torna das 17 horas, portanto não se pode analisar nada. Já fazendo a análise para os picos mínimos vemos que no dia 28 o

menor pico de entrada se deu próximo às 8 horas com um valor próximo a 15.0 Kbps, que ao vermos no dia 29 neste horário o tráfego era de aproximadamente 20.0 Kbps, por outro lado o de saída foi em torno de 10 horas com um tráfego perto de 120.0 Kbps.

A Figura 7 fornece ainda a entrada e a saída máxima mostrada no gráfico, que foi de 164.0 Kbps e 489.0 Kbps respectivamente, a média de entrada que foi de 19.6 Kbps e a de saída com um valor de 105.8 Kbps e também mostra a entrada e atual com 11.4 Kbps e a saída com 120.0 Kbps, os quais equivalem a data/hora de geração do relatório.

- ✓ **Semanal**

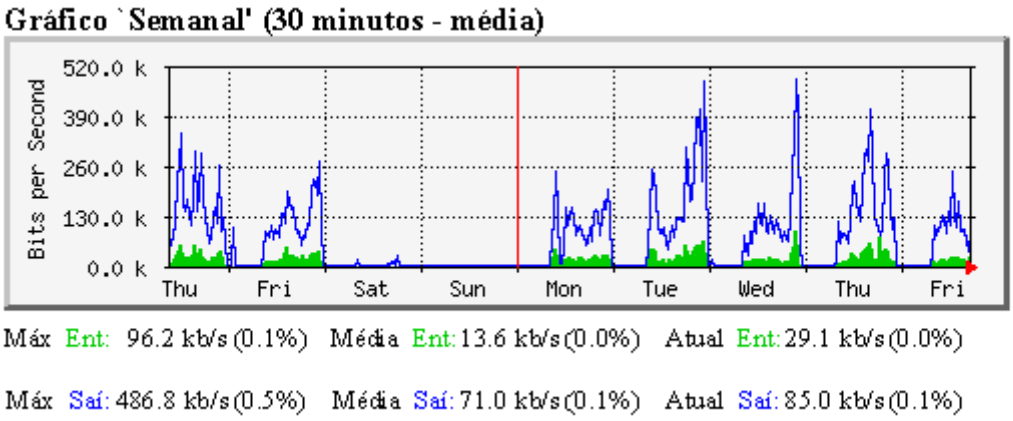


Figura 8 - Gráfico Semanal de Tráfego da LAN

O gráfico apresentado acima, retrata a situação semanal do tráfego na rede local. Por padrão o MRTG mostra a semana atual e o anterior, sendo a primeira apresentada à direita da linha vertical vermelha e a segunda apresentada à esquerda desta linha.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

A semana à esquerda da linha vermelha apresentou o maior pico de entrada (resposta) na quita-feira (*Thu*) com um tráfego de informação de aproximadamente 65.0 Kbps. Em contrapartida o maior pico de saída (solicitação) também ocorreu na quinta apresentando um tráfego de informação próximo a 375.0 Kbps. Este mesma semana apresentou como menor pico de entrada um valor próximo a 20.0 Kbps registrado também na quinta e como menor pico de saída foi neste mesmo dia, apresentando um resultado perto de 65.0 Kbps.

A semana à direita da linha vermelha, apresentou o maior pico de entrada (resposta) na quarta-feira (*Wed*) com um tráfego de informação de aproximadamente 100.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu também na quinta, apresentando um tráfego de informação próximo a 490.0 Kbps. Esta mesma semana, apresentou como menor

pico de entrada um valor próximo a 15.0 Kbps registrado na terça-feira (*Tue*) e como menor pico de saída foi na segunda-feira apresentando um resultado perto de 5.0 Kbps.

Fazendo uma análise comparativa da primeira semana em relação à segunda podemos verificar que somente os dias de quinta-feira (*Thu*) e sexta-feira (*Fri*) é que se repetem, na primeira semana o pico máximo de saída ocorreu na quinta com um valor de 375.0 Kbps, nesse mesmo dia da semana seguinte, perto do mesmo horário, o tráfego atingiu cerca de 157.0 Kbps, havendo assim uma queda razoável no tráfego em comparação com a semana anterior. Da mesma forma para o máximo de entrada da primeira semana, este ocorreu com um valor de 65.0 Kbps também na quinta, entretanto, para a semana seguinte, a coleta do gráfico nesse mesmo dia para o mesmo horário foi de aproximadamente 25.0 Kbps, portanto assim como o de saída o de entrada ocasionou de um decline no tráfego sendo este em proporção, um pouco maior. Já fazendo a análise para os picos mínimos vemos que na primeira semana o menor pico de entrada se encontra na quinta feira com um valor próximo a 25.0 Kbps, que ao vermos na semana seguinte neste mesmo horário o tráfego era de aproximadamente 20.0 Kbps, por outro lado o de saída foi em torno de 10 horas com um tráfego perto de 65.0 Kbps.

A Figura 8 fornece ainda a entrada e a saída máxima mostrada no gráfico, que foi de 96.2 Kbps e 486.8 Kbps respectivamente, a média de entrada que foi de 13.6 Kbps e a de saída com um valor de 71.0 Kbps e também mostra a entrada e atual com 29.1 Kbps e a saída com 85.0 Kbps.

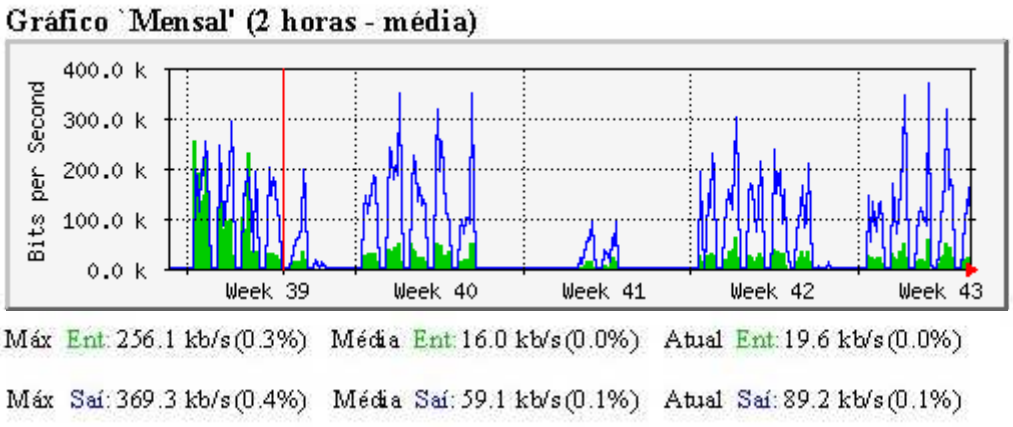


Figura 9 - Gráfico Mensal de Tráfego da LAN

O gráfico apresentado na Figura 9, retrata a situação mensal do tráfego na rede local. Por padrão o MRTG mostra o mês atual e o anterior, sendo o primeiro apresentado à direita da linha vertical vermelha e o segundo apresentada à esquerda desta linha, obs. A semana Week 39 está divida ao meio, embora ela tenha uma parte à direita da linha esta ainda corresponde ao primeiro mês.

Como o gráfico apresenta apenas cinco semanas, podemos concluir que somente duas semanas serão iguais, neste caso será a primeira semana do gráfico representada pela sigla *Week 39* e a última representada pela sigla *Week 43*.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

O mês à esquerda da linha vermelha, representado unicamente pela semana *Week 39*, apresentou o maior pico de entrada (resposta) tendo um tráfego de informação de aproximadamente 260.0 Kbps, representado no final da semana. Em contrapartida o maior pico de saída (solicitação) ocorreu no meio da semana, apresentando um tráfego de informação de 300.0 Kbps. Este mesmo mês apresentou como menor pico de entrada um valor próximo a 20.0 Kbps registrado também no final da semana e como menor pico de saída foi neste período da semana, apresentando um resultado perto de 40.0 Kbps.

O mês à direita da linha vermelha, apresentou o maior pico de entrada (resposta) na semana *Week 42* com um tráfego de informação de aproximadamente 65.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu na semana *Week 43*, apresentando um tráfego de informação próximo a 490.0 Kbps. Este mesmo mês, apresentou como menor pico de entrada um valor próximo a 5.0 Kbps registrado na semana *Week 41* e como menor pico de saída foi na semana *Week 42* apresentando um resultado perto de 1.0 Kbps.

Fazendo uma análise comparativa do primeiro mês representado pela semana *Week 39* em relação ao segundo podemos verificar que, no primeiro o pico máximo de saída ocorreu com um valor de 300.0 Kbps antes do meio da semana, nesse mesmo período do mês seguinte seguinte, o tráfego atingiu cerca de 350.0 Kbps, havendo assim uma acréscimo razoável no

tráfego em comparação ao mês anterior. Da mesma forma para o máximo de entrada do primeiro mês, este ocorreu com um valor de 260.0 Kbps no meio da semana, entretanto, para o mês seguinte, a coleta do gráfico nesse mesmo período foi de aproximadamente 30.0 Kbps, portanto o tráfego teve um decline bem alto no tráfego. Já fazendo a análise para os picos mínimos vemos que no primeiro mês o menor pico de entrada se encontra no final da semana com um valor próximo a 20.0 Kbps, e na semana seguinte, neste mesmo período, o tráfego é de aproximadamente 30.0 Kbps tendo um acréscimo mínimo no tráfego, por outro lado o de saída foi no meio da semana com um tráfego perto de 40.0 Kbps, sendo nesta mesma época para o mês posterior ocorreu um acréscimo mínimo no tráfego de 30 Kbps.

A Figura 9 fornece ainda a entrada e a saída máxima mostrada no gráfico, que foi de 256.1 Kbps e 369.3 Kbps respectivamente, a média de entrada que foi de 16.0 Kbps e a de saída com um valor de 59.1 Kbps e também mostra a entrada e atual com 19.6 Kbps e a saída com 89.2 Kbps.

- ✓ **Anual**

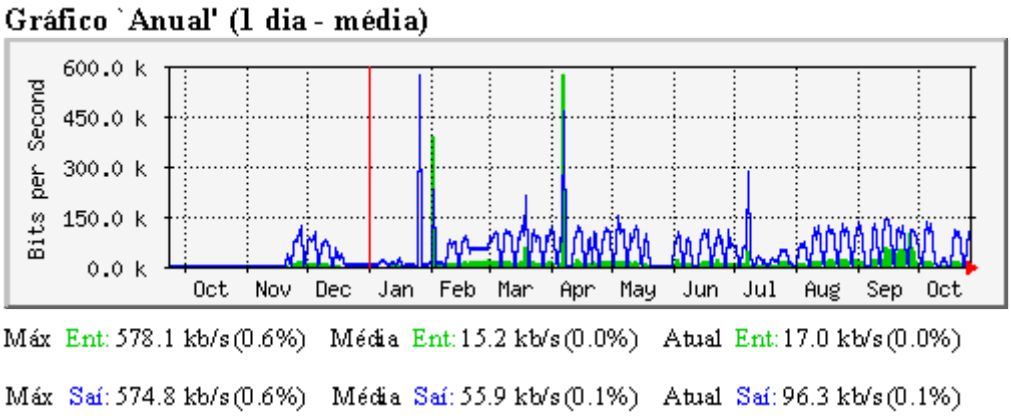


Figura 10 - Gráfico Anual de Tráfego da LAN

O gráfico apresentado acima, retrata a situação anual do tráfego na rede local. Por padrão o MRTG mostra o ano atual e o anterior, sendo o primeiro apresentado à direita da linha vertical vermelha e o segundo apresentada à esquerda desta linha.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

O ano à esquerda da linha vermelha, representado pelos meses de outubro (*Oct*) novembro (*Nov*) e dezembro (*Dec*), apresentou o maior pico de entrada (resposta) tendo um tráfego de informação de aproximadamente 30.0 Kbps, representado no final do mês de

novembro. Em contrapartida o maior pico de saída (solicitação) ocorreu no final do mês de novembro, apresentando um tráfego de informação de 130.0 Kbps. Este mesmo ano apresentou como menor pico de entrada um valor próximo a 5.0 Kbps registrado no final do mês de novembro e como menor pico de saída foi neste período da semana, apresentando um resultado perto de 38.0 Kbps, apresentado também perto do final do mês de novembro

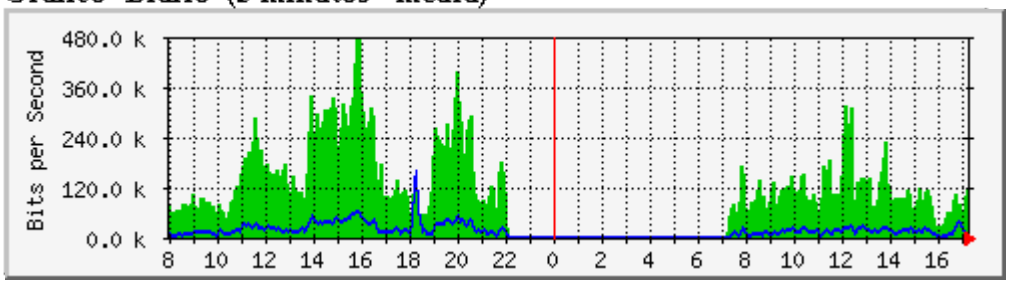
O ano à direita da linha vermelha, apresentou o maior pico de entrada (resposta) no início do mês de abril com um tráfego de informação de aproximadamente 560.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu no final do mês de janeiro,

Traffic Analysis for 2 --

System: in
Maintainer:
Description: srouter
ifType: ppp (23)
ifName:
Max Speed: 128.0 kBytes/s
Ip: IP WAN

Última atualização das estatísticas: **Sexta, 29 de Outubro de 2004 às 17:18**, nesta hora dispositivo estava online por **43 days, 17:48:15**.

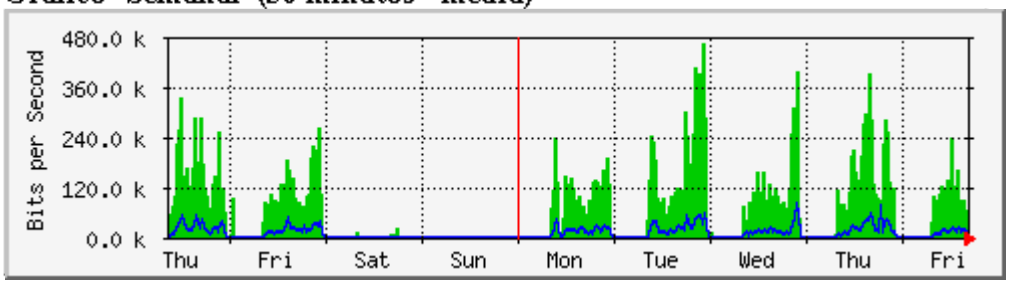
Gráfico `Diário' (5 minutos - média)



Máx Ent: 479.3 kb/s (46.8%) Média Ent: 106.3 kb/s (10.4%) Atual Ent: 118.3 kb/s (11.6%)

Máx Saí: 159.8 kb/s (15.6%) Média Saí: 17.8 kb/s (1.7%) Atual Saí: 9672.0 b/s (0.9%)

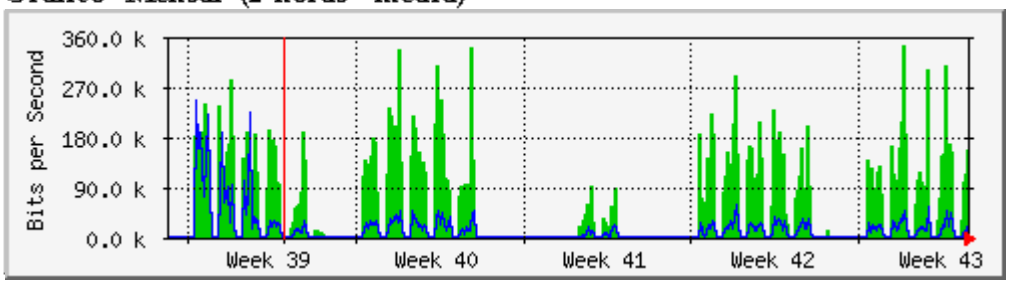
Gráfico `Semanal' (30 minutos - média)



Máx Ent: 469.4 kb/s (45.8%) Média Ent: 71.0 kb/s (6.9%) Atual Ent: 42.9 kb/s (4.2%)

Máx Saí: 85.0 kb/s (8.3%) Média Saí: 12.3 kb/s (1.2%) Atual Saí: 8040.0 b/s (0.8%)

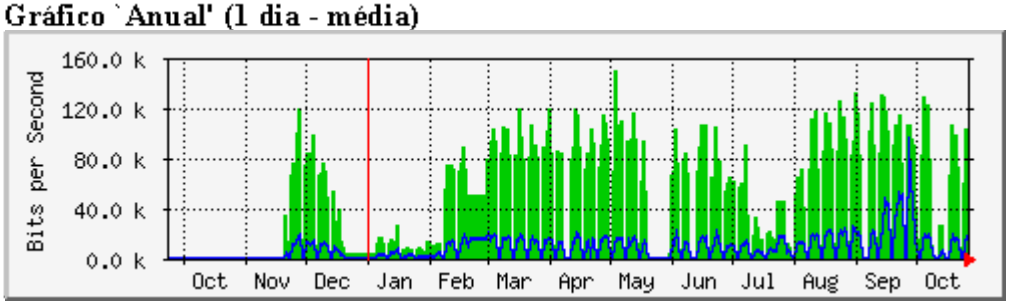
Gráfico `Mensal' (2 horas - média)



Máx Ent: 346.3 kb/s (33.8%) Média Ent: 59.4 kb/s (5.8%) Atual Ent: 159.5 kb/s (15.6%)

Máx Saí: 247.6 kb/s (24.2%) Média Saí: 15.1 kb/s (1.5%) Atual Saí: 23.0 kb/s (2.2%)

Gráfico `Anual' (1 dia - média)



Máx Ent: 150.4 kb/s (14.7%) Média Ent: 50.2 kb/s (4.9%) Atual Ent: 89.3 kb/s (8.7%)

Máx Saí: 97.4 kb/s (9.5%) Média Saí: 10.6 kb/s (1.0%) Atual Saí: 14.8 kb/s (1.4%)

VERDE ### Tráfego de Entrada em Bits por segundo

AZUL ### Tráfego de Saída em Bits por segundo

MRTG MULTI ROUTER TRAFFIC GRAPHER

versão 2.9.17 Tobias Oetiker <oetiker@ee.ethz.ch> e Dave Rand <dlr@bungi.com>

Localização efetuada por Luiz Felipe R E <luizfelipe@encarnacao.com>

Figura 11 - Relatórios Gráficos de Tráfego do Roteador (SROUTER)

A Figura 11 nos permite visualizar sua descrição, sendo esta uma SROUTER (Roteador) e também nos dá sua velocidade máxima em *Bytes*, sendo de 128 KBytes/s

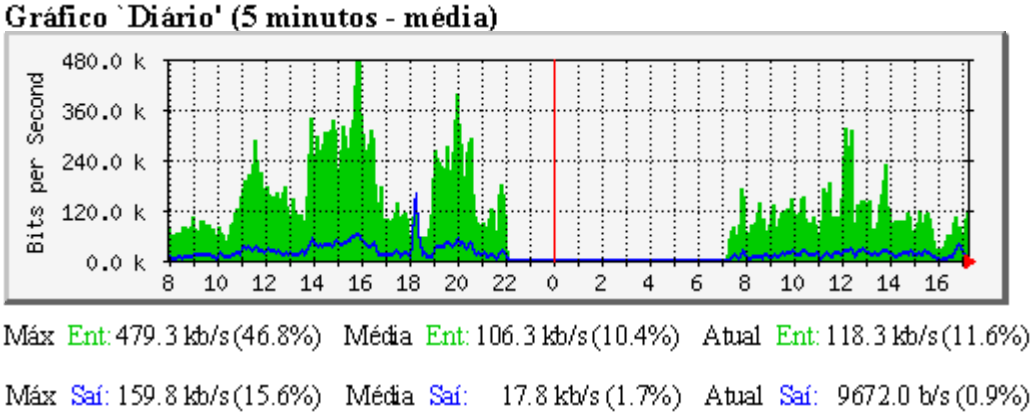


Figura 12 - Gráfico Diário do Tráfego do Roteador (SROUTE)

O gráfico apresentado acima, retrata a situação diária do tráfego no roteador. Por padrão o MRTG mostra o dia atual e o anterior, sendo o primeiro apresentado à direita da linha vertical vermelha e o segundo apresentado à esquerda desta linha.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

O dia 28 de outubro de 2004 apresentou o maior pico de entrada (resposta) às 16 horas com um tráfego de informação de aproximadamente 480.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu aproximadamente às 18 horas apresentando um tráfego de informação próximo a 170.0 Kbps. Este mesmo dia apresentou como menor pico de entrada um valor próximo a 60.0 Kbps registrado em torno de 10 horas e como menor pico de saída foi por volta de 10 horas apresentando um resultado próximo a 1.0 Kbps.

O dia 29 de outubro de 2004 apresentou o maior pico de entrada (resposta) às 12 horas com um tráfego de informação de aproximadamente 330.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu aproximadamente às 17 horas apresentando um tráfego de informação próximo a 45.0 Kbps. Este mesmo dia apresentou como menor pico de entrada um valor próximo a 30.0 Kbps registrado em torno de 16 horas e como menor pico de saída foi também por volta das 8, 11 e 16 horas apresentando um resultado perto de 1.0 Kbps.

Fazendo uma análise comparativa do dia 28 em relação ao dia 29 podemos verificar que, no dia 28 o pico máximo de saída ocorreu às 18 horas com um valor de 170.0 Kbps, no entanto, para o dia 29, a coleta do gráfico se deu em torna das 17 horas, portanto não se pode analisar nada. Da mesma forma para o máximo de entrada do dia 28, este ocorreu com um valor de 380,0 Kbps às 16 horas, nesse mesmo horário no dia 29 o tráfego foi de aproximadamente 45.0 Kbps, ou seja, o menor pico desse dia, havendo assim uma queda muito grande no tráfego nesse horário. Já fazendo a análise para os picos mínimos, vimos que no dia 28 o menor pico de entrada se deu próximo às 10 horas com um valor próximo a 60.0 Kbps, que ao vermos no dia 29 neste horário o tráfego era de aproximadamente 120.0 Kbps,

por outro lado o de saída foi em torno de 10 horas com um tráfego perto de 1.0 Kbps teve no dia 29 um pico próximo a 20 Kbps.

A Figura 12 fornece ainda a entrada e a saída máxima mostrada no gráfico, que foi de 479.3 Kbps e 159.8 Kbps respectivamente, a média de entrada que foi de 106.3 Kbps e a de saída com um valor de 17.8 Kbps e também mostra a entrada e atual com 118.3 Kbps e a saída com 9672 bps, os quais equivalem a data/hora de geração do relatório.

- ✓ **Semanal**

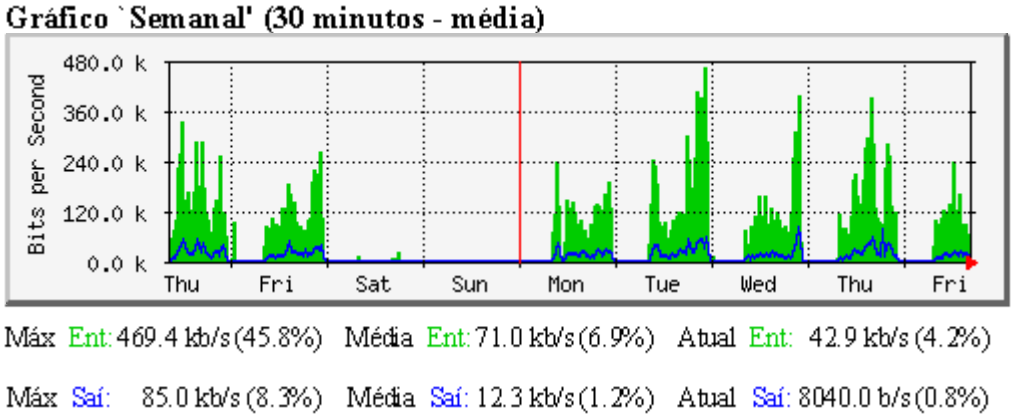


Figura 13 - Gráfico Semanal do Tráfego do Roteador (SROUTER)

O gráfico apresentado acima, retrata a situação semanal do tráfego no roteador. Por padrão o MRTG mostra a semana atual e o anterior, sendo a primeira apresentada à direita da linha vertical vermelha e a segunda apresentada à esquerda desta linha.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

A semana à esquerda da linha vermelha apresentou o maior pico de entrada (resposta) no início de quita-feira (*Thu*) com um tráfego de informação de aproximadamente 340.0 Kbps. Em contrapartida o maior pico de saída (solicitação) também ocorreu na quinta, na metade do dia, apresentando um tráfego de informação próximo a 60.0 Kbps. Este mesma semana apresentou como menor pico de entrada um valor próximo a 80.0 Kbps registrado no final de quinta-feira e como menor pico de saída foi no final deste mesmo dia, apresentando um resultado perto de 5.0 Kbps.

A semana à direita da linha vermelha, apresentou o maior pico de entrada (resposta) no final de terça-feira (*Tue*) com um tráfego de informação de aproximadamente 470.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu na quarta-feira (*Wed*),

apresentando um tráfego de informação próximo a 80.0 Kbps. Esta mesma semana, apresentou como menor pico de entrada um valor próximo a 20.0 Kbps registrado no início de segunda-feira (*Mon*) e como menor pico de saída, esta ocorreu semelhantes em 3 dias da semana, apresentando um resultado perto de 1.0 Kbps.

Fazendo uma análise comparativa da primeira semana em relação à segunda podemos verificar que somente os dias de quinta-feira (*Thu*) e sexta-feira (*Fri*) é que se repetem, na primeira semana o pico máximo de saída ocorreu na quinta com um valor de 60.0 Kbps, nesse mesmo dia da semana seguinte, perto do mesmo horário, o tráfego atingiu cerca de 30.0 Kbps, havendo assim uma queda razoável no tráfego em comparação com a semana anterior. Da mesma forma para o máximo de entrada da primeira semana, este ocorreu com um valor de 340.0 Kbps também na quinta, entretanto, para a semana seguinte, a coleta do gráfico nesse mesmo dia para o mesmo horário foi de aproximadamente 210.0 Kbps, portanto, assim como o de saída o de entrada ocasionou de um decline no tráfego sendo este em proporção, um pouco maior. Já fazendo a análise para os picos mínimos vemos que na primeira semana o menor pico de entrada se encontra na quinta feira com um valor próximo a 5.0 Kbps, que ao vermos na semana seguinte neste mesmo horário o tráfego era de 90.0 Kbps, desta forma, apresentando um acréscimo no tráfego, por outro lado o de saída foi também na quinta com um tráfego perto de 80.0 Kbps e no mesmo dia para semana seguinte este valor se encontrava perto de 100 o que indica um pequeno acréscimo no tráfego.

A Figura 12 fornece ainda a entrada e a saída máxima mostrada no gráfico, que foi de 469.4 Kbps e 85.0 Kbps respectivamente, a média de entrada que foi de 71.0 Kbps e a de saída com um valor de 12.3 Kbps e também mostra a entrada e atual com 42.9 Kbps e a saída com 8040 bps.

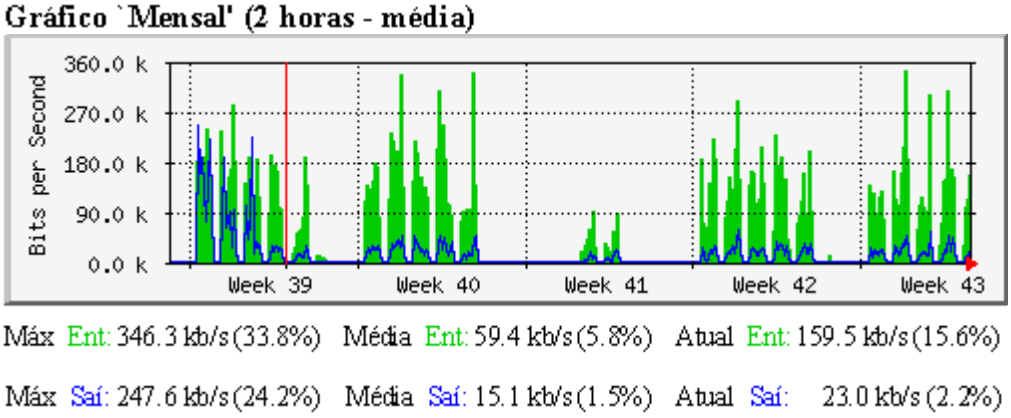


Figura 14 - Gráfico Mensal do Tráfego do Roteador (SROUTER)

O gráfico apresentado acima, retrata a situação mensal do tráfego roteador. Por padrão o MRTG mostra o mês atual e o anterior, sendo o primeiro apresentado à direita da linha vertical vermelha e o segundo apresentada à esquerda desta linha, obs. A semana Week 39 está divida ao meio, embora ela tenha uma parte à direita da linha esta ainda corresponde ao primeiro mês.

Como o gráfico apresenta apenas cinco semanas, podemos concluir que somente duas semanas serão iguais, neste caso será a primeira semana do gráfico representada pela sigla *Week 39* e a última representada pela sigla *Week 43*.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

O mês à esquerda da linha vermelha, representado unicamente pela semana *Week 39*, apresentou o maior pico de entrada (resposta) tendo um tráfego de informação de aproximadamente 290.0 Kbps, representado antes do meio da semana. Em contrapartida o maior pico de saída (solicitação) ocorreu no meio da semana, apresentando um tráfego de informação de 250.0 Kbps. Este mesmo mês apresentou como menor pico de entrada um valor próximo a 120.0 Kbps registrado também no meio da semana e como menor pico de saída foi também neste período da semana, apresentando um resultado perto de 30.0 Kbps.

O mês à direita da linha vermelha, apresentou o maior pico de entrada (resposta) antes do meio da semana *Week 43* com um tráfego de informação de aproximadamente 350.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu antes do meio da semana *Week 43*, apresentando um tráfego de informação próximo a 60.0 Kbps. Este mesmo mês, apresentou como menor pico de entrada um valor próximo a 15.0 Kbps registrado na semana *Week 41* e como menor pico de saída foi na semana *Week 41 e 42* apresentando um resultado perto de 1.0 Kbps.

Fazendo uma análise comparativa do primeiro mês representado pela semana *Week 39* em relação ao segundo podemos verificar que, no primeiro o pico máximo de saída ocorreu com um valor de 250.0 Kbps antes do meio da semana, nesse mesmo período no mês

seguinte, o tráfego atingiu cerca de 95.0 Kbps, havendo assim uma redução no tráfego em comparação ao mês anterior. Da mesma forma para o máximo de entrada do primeiro mês, este ocorreu com um valor de 290.0 Kbps antes do meio da semana, entretanto, para o mês seguinte, a coleta do gráfico nesse mesmo período foi de aproximadamente 350.0 Kbps, portanto o tráfego teve um acréscimo bem alto no tráfego. Já fazendo a análise para os picos mínimos vemos que no primeiro mês o menor pico de entrada se encontra no meio da semana com um valor próximo a 120.0 Kbps, e na semana seguinte, neste mesmo período, o tráfego é de aproximadamente 15.0 Kbps tendo uma redução significativa no tráfego, por outro lado o de saída foi no meio da semana com um tráfego perto de 30.0 Kbps, sendo nesta mesma época para o mês posterior, houve uma pequena diminuição no tráfego de 20.0 Kbps.

A Figura 14 fornece ainda a entrada e a saída máxima mostrada no gráfico, que foi de 256.1 Kbps e 369.3 Kbps respectivamente, a média de entrada que foi de 16.0 Kbps e a de saída com um valor de 59.1 Kbps e também mostra a entrada e atual com 19.6 Kbps e a saída com 89.2 Kbps.

- ✓ **Anual**

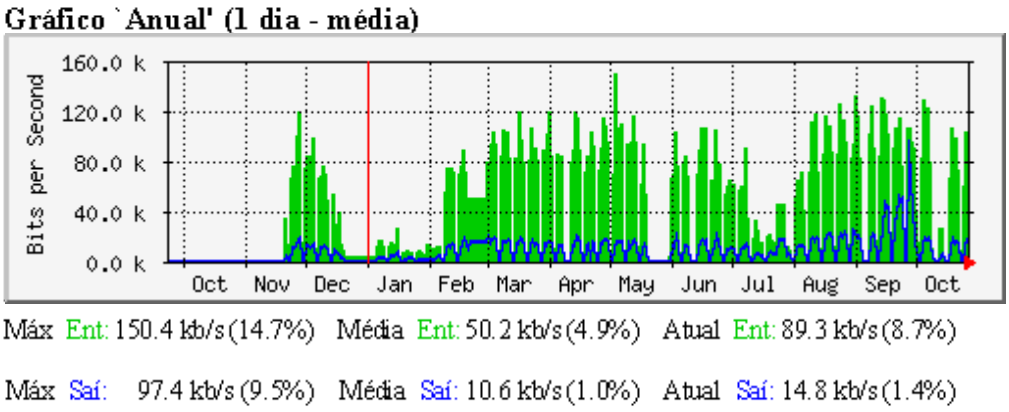


Figura 15 - Gráfico Anual do Tráfego do Roteador (SROUTER)

O gráfico apresentado acima, retrata a situação anual do tráfego no roteador. Por padrão o MRTG mostra o ano atual e o anterior, sendo o primeiro apresentado à direita da linha vertical vermelha e o segundo apresentada à esquerda desta linha.

Com relação ao tráfego de informações na rede interna o MRTG apresenta as entradas (respostas) de verde e saídas (solicitações) de azul.

O ano à esquerda da linha vermelha, representado pelos meses de outubro (*Oct*) novembro (*Nov*) e dezembro (*Dec*), apresentou o maior pico de entrada (resposta) tendo um

tráfego de informação de aproximadamente 120.0 Kbps, representado no final do mês de novembro. Em contrapartida o maior pico de saída (solicitação) ocorreu também no final do mês de novembro, apresentando um tráfego de informação de 20.0 Kbps. Este mesmo ano apresentou como menor pico de entrada um valor próximo a 10.0 Kbps registrado no final do mês de novembro e como menor pico de saída foi neste mesmo período da semana, apresentando um resultado perto de 1.0 Kbps, apresentado do início do mês de novembro

O ano à direita da linha vermelha, apresentou o maior pico de entrada (resposta) no início do mês de maio (*May*) com um tráfego de informação de aproximadamente 140.0 Kbps. Em contrapartida o maior pico de saída (solicitação) ocorreu no final do mês de

Traffic Analysis for 65 --

System: in

Maintainer:

Description: WAN Port

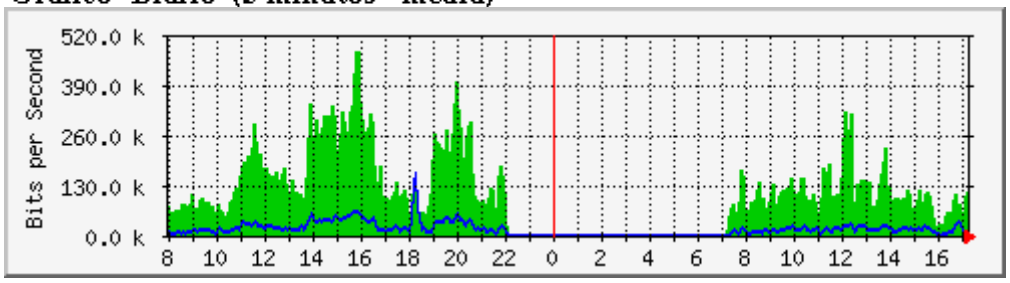
ifType: sdlc (17)

ifName:

Max Speed: 128.0 kBytes/s

Última atualização das estatísticas: **Sexta, 29 de Outubro de 2004 às 17:18**, nesta hora dispositivo estava online por **43 days, 17:48:15**.

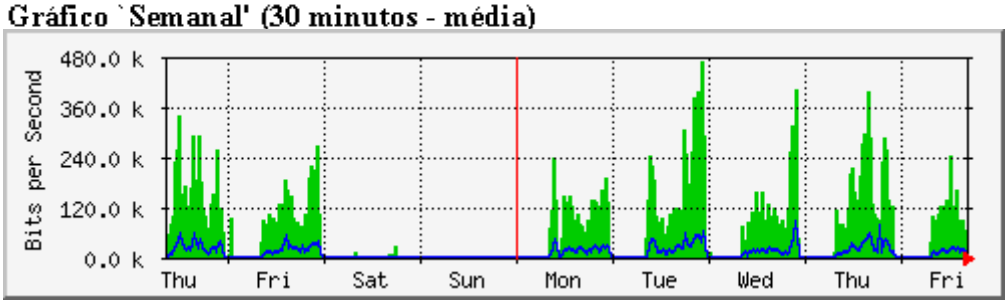
Gráfico `Diário' (5 minutos - média)



Máx Ent: 479.3 kb/s (46.8%) Média Ent: 106.3 kb/s (10.4%) Atual Ent: 118.3 kb/s (11.6%)

Máx Saí: 159.8 kb/s (15.6%) Média Saí: 17.8 kb/s (1.7%) Atual Saí: 9672.0 b/s (0.9%)

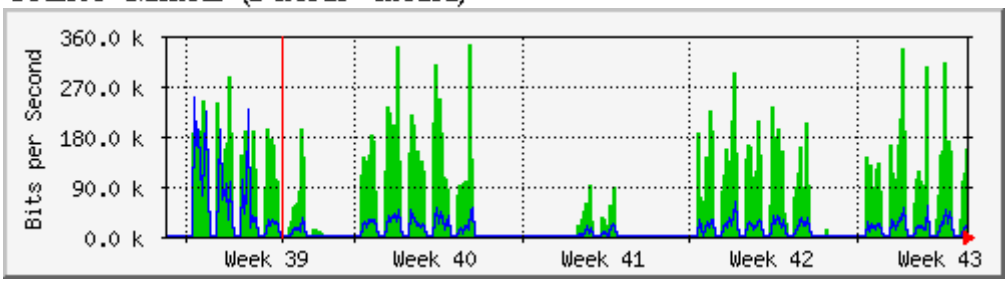
Gráfico `Semanal' (30 minutos - média)



Máx Ent: 469.4 kb/s (45.8%) Média Ent: 71.0 kb/s (6.9%) Atual Ent: 42.9 kb/s (4.2%)

Máx Saí: 85.0 kb/s (8.3%) Média Saí: 12.3 kb/s (1.2%) Atual Saí: 8040.0 b/s (0.8%)

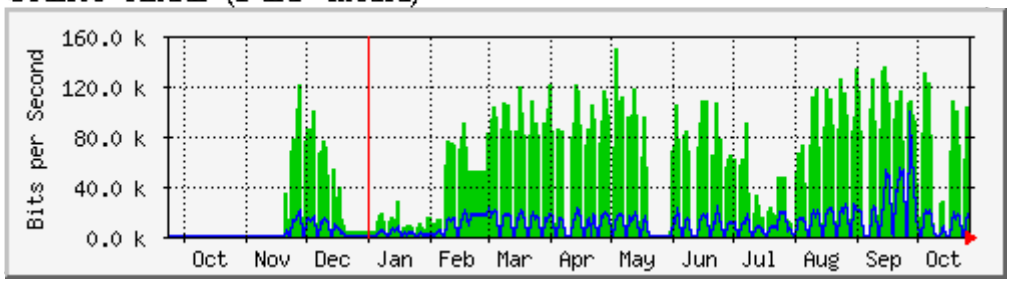
Gráfico `Mensal' (2 horas - média)



Máx Ent: 346.3 kb/s (33.8%) Média Ent: 59.4 kb/s (5.8%) Atual Ent: 159.5 kb/s (15.6%)

Máx Saí: 247.6 kb/s (24.2%) Média Saí: 15.1 kb/s (1.5%) Atual Saí: 23.0 kb/s (2.2%)

Gráfico `Anual' (1 dia - média)



Máx Ent: 150.4 kb/s (14.7%) Média Ent: 50.2 kb/s (4.9%) Atual Ent: 89.3 kb/s (8.7%)

Máx Saí: 97.4 kb/s (9.5%) Média Saí: 10.6 kb/s (1.0%) Atual Saí: 14.8 kb/s (1.4%)

VERDE ### Tráfego de Entrada em Bits por segundo

AZUL ### Tráfego de Saída em Bits por segundo

MRTG MULTI ROUTER TRAFFIC GRAPHER

versão 2.9.17 Tobias Oetiker <oetiker@ee.ethz.ch> e Dave Rand <dlr@bungi.com>

Localização efetuada por Luiz Felipe R E <luizfelipe@encarnacao.com>

Figura 16 - Relatórios Gráficos de Tráfego da WAN

A Figura 16 nos permite visualizar sua descrição, sendo esta uma WAN, porta para a rede externa e também nos dá sua velocidade máxima em *Bytes*, sendo de 128 KBytes/s

Fazendo uma comparação destes relatórios (WAN) com os relatórios gerados pelos gráficos do roteador (SROUTER). Podemos perceber que os relatórios apresentam valores iguais sendo que em alguns gráficos a única diferença é a escala, os valores gerados são os mesmos. Isso ocorre porque quando o MRTG foi configurado para verificar o trafego da WAN, provavelmente este, por engano ficou também encarregado do roteador. O roteador deveria ter o tráfego da LAN mais o tráfego da WAN, isso porque quando há uma solicitação de informação o roteador verifica no *Proxy* se esta informação já esta em *cache*, se houver o requisito, o tráfego não passa pela WAN, desta forma somente o tráfego da LAN e do roteador sofreriam alterações, porque não haveria necessidade de buscar no servidor de destino as solicitações pedidas, por outro lado, se o requisito não estiver no *Proxy* o roteador faz o tráfego passar pela porta WAN, gerando tráfego na mesma, no Roteador e na LAN para poder buscar o que foi solicitado no servidor de destino.

4.2. Relatórios Produzidos Pelo SARG

Neste tópico abordaremos os relatórios gerados por esta ferramenta com relação aos dados fornecidos pelo *Proxy Squid*. Esses relatórios são atualizados diariamente. Serão considerados os relatórios apresentados pelo SARG para demonstrar o que os usuários da rede estão acessando e trafegando por esta. A princípio, os gráficos serão apresentados da forma que o SARG os disponibiliza.

Em um segundo momento, será feito uma análise dos dados de cada relatório apresentado pela ferramenta.

4.2.1. Relatórios do *Proxy Squid* do Dia

Index.html

Relatório do Proxy Squid - Do Dia

ARQUIVO/PERÍODO	DATA CRIAÇÃO	USUÁRIOS	BYTES	MÉDIA
18Oct2004-28Oct2004	Sex Out 29 14:21:22 BRST 2004	83	1.251.069.673	15.073.128

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 27 - Índice do Arquivo de Relatórios e Dados Atuais

O primeiro relatório do *Squid*, Figura 17, apresenta as seguintes informações:

- ✓ ARQUIVO/PERÍODO: Refere-se ao período de execução. Tendo como apresentação data inicial – data final.
- ✓ DATA CRIAÇÃO: informa a data e hora de criação do arquivo.
- ✓ USUÁRIOS: informa o número de usuários logados no momento em que o *Index.html* foi gerado.
- ✓ *BYTES*: quantidade total de *Bytes* baixados pelos usuários.

- ✓ MÉDIA: quantidade média de *Bytes* baixados por usuário.

4.2.1.1 Ordenação por *Bytes* Decrescente

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Ordem: BYTES, reverse
Topuser Relatorio

Topsites Relatorio
Sites & Users Relatorio
Negado Relatorio

NUM	USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-	TEMPO	MILISEG	%TEMPO
1	192.168.1.99	21.721	116.617.045	9.32%	26.92%	73.08%	02:15:07	8.107.682	6.06%
2	192.168.1.98	17.559	101.286.045	8.10%	27.69%	72.31%	01:50:23	6.623.972	4.95%
3	192.168.1.95	21.035	101.160.085	8.09%	27.36%	72.64%	02:10:06	7.806.986	5.84%
4	192.168.1.93	22.382	95.908.352	7.67%	13.20%	86.80%	02:42:58	9.778.807	7.31%
5	192.168.1.97	17.694	82.095.338	6.56%	29.84%	70.16%	03:14:28	11.668.682	8.73%
6	192.168.1.96	12.993	53.521.171	4.28%	21.40%	78.60%	04:16:30	15.390.524	11.51%
7	192.168.1.76	3.960	36.832.014	2.94%	25.24%	74.76%	01:11:01	4.261.656	3.19%
8	192.168.1.71	4.409	34.342.988	2.75%	21.94%	78.06%	00:55:32	3.332.052	2.49%
9	192.168.1.80	9.993	33.067.343	2.64%	31.65%	68.35%	01:04:07	3.847.826	2.88%
10	192.168.1.66	2.561	29.420.468	2.35%	18.99%	81.01%	00:38:01	2.281.349	1.71%
11	192.168.1.78	4.982	28.592.110	2.29%	25.64%	74.36%	00:56:38	3.398.886	2.54%
12	192.168.1.69	3.658	28.112.433	2.25%	35.27%	64.73%	00:40:50	2.450.137	1.83%
13	192.168.1.70	3.623	25.696.950	2.05%	18.47%	81.53%	00:54:53	3.293.797	2.46%
14	192.168.1.77	4.760	25.450.350	2.03%	12.77%	87.23%	01:30:29	5.429.761	4.06%
15	192.168.1.81	4.064	25.301.609	2.02%	25.69%	74.31%	00:33:56	2.036.543	1.52%
16	192.168.1.61	3.582	23.892.973	1.91%	22.17%	77.83%	00:44:19	2.659.936	1.99%
17	192.168.1.79	4.529	22.163.977	1.77%	21.68%	78.32%	00:48:11	2.891.936	2.16%
18	192.168.1.72	3.603	19.662.602	1.57%	21.42%	78.58%	00:32:52	1.972.420	1.48%
19	192.168.1.65	2.450	18.958.429	1.52%	20.62%	79.38%	00:46:27	2.787.230	2.08%
NUM	USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-	TEMPO	MILISEG	%TEMPO
20	192.168.1.57	2.949	18.353.054	1.47%	37.88%	62.12%	00:29:26	1.766.133	1.32%
21	192.168.1.126	3.224	16.893.823	1.35%	13.28%	86.72%	00:31:43	1.903.803	1.42%
22	192.168.1.63	2.848	14.925.784	1.19%	26.41%	73.59%	00:21:16	1.276.473	0.95%
23	192.168.1.67	2.598	14.648.091	1.17%	33.27%	66.73%	00:42:19	2.539.816	1.90%
24	192.168.1.125	1.060	13.625.983	1.09%	9.58%	90.42%	00:17:40	1.060.104	0.79%
25	192.168.1.27	3.007	12.842.805	1.03%	45.74%	54.26%	00:23:01	1.381.191	1.03%
26	192.168.1.123	2.772	12.798.574	1.02%	15.85%	84.15%	00:20:09	1.209.606	0.90%
27	192.168.1.60	2.976	12.150.077	0.97%	27.02%	72.98%	00:19:24	1.164.559	0.87%
28	192.168.0.21	2.822	11.647.545	0.93%	13.83%	86.17%	00:14:04	844.592	0.63%
29	192.168.1.64	1.126	11.514.665	0.92%	24.99%	75.01%	00:16:19	979.351	0.73%
30	192.168.1.38	2.155	10.837.384	0.87%	13.89%	86.11%	00:10:07	607.752	0.45%
31	192.168.1.59	2.528	10.757.888	0.86%	31.54%	68.46%	00:17:10	1.030.034	0.77%
32	192.168.1.75	2.685	10.730.039	0.86%	30.66%	69.34%	00:21:20	1.280.123	0.96%
33	192.168.1.127	1.207	9.743.589	0.78%	12.33%	87.67%	00:07:24	444.024	0.33%
34	192.168.1.52	2.117	9.063.583	0.72%	39.57%	60.43%	00:15:43	943.822	0.71%
35	192.168.1.54	1.556	8.350.317	0.67%	31.07%	68.93%	00:09:15	555.909	0.42%
36	192.168.1.68	2.127	7.781.653	0.62%	24.87%	75.13%	00:12:09	729.734	0.55%

NUM	USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-		TEMPO	MILISEG	%TEMPO
37	192.168.0.32	978	7.103.631	0.57%	6.47%	93.53%	00:05:49	349.664	0.26%
38	192.168.1.11	2.170	6.716.349	0.54%	37.91%	62.09%	00:07:28	448.568	0.34%
39	192.168.1.58	1.240	6.416.065	0.51%	26.85%	73.15%	00:07:29	449.727	0.34%
40	192.168.0.7	2.206	6.371.306	0.51%	14.28%	85.72%	00:12:09	729.127	0.55%
41	192.168.0.5	2.185	6.098.052	0.49%	18.23%	81.77%	00:20:16	1.216.366	0.91%
42	192.168.1.16	1.254	5.770.291	0.46%	14.45%	85.55%	00:10:20	620.789	0.46%
43	192.168.1.18	772	5.282.415	0.42%	39.35%	60.65%	00:03:19	199.083	0.15%
44	192.168.1.91	1.886	5.105.009	0.41%	11.69%	88.31%	00:11:07	667.907	0.50%
45	192.168.1.53	1.286	4.860.096	0.39%	40.72%	59.28%	00:08:20	500.675	0.37%
46	192.168.1.33	579	4.859.548	0.39%	23.29%	76.71%	00:06:13	373.413	0.28%
47	192.168.1.20	1.029	4.856.283	0.39%	16.60%	83.40%	00:14:08	848.779	0.63%
48	192.168.1.94	1.014	4.771.808	0.38%	19.89%	80.11%	00:11:21	681.096	0.51%
49	192.168.1.37	1.130	4.615.661	0.37%	53.42%	46.58%	00:06:06	366.428	0.27%
50	192.168.1.122	1.618	4.568.573	0.37%	26.01%	73.99%	00:10:38	638.223	0.48%
51	192.168.1.29	463	4.381.200	0.35%	22.19%	77.81%	00:02:42	162.980	0.12%
52	192.168.0.37	1.466	4.332.886	0.35%	26.97%	73.03%	00:06:59	419.944	0.31%
53	192.168.1.14	844	4.175.200	0.33%	43.13%	56.87%	00:03:03	183.161	0.14%
54	192.168.1.36	984	4.029.687	0.32%	19.97%	80.03%	00:06:06	366.535	0.27%
55	192.168.1.51	855	3.929.443	0.31%	13.50%	86.50%	00:12:06	726.343	0.54%
56	192.168.1.101	1.019	3.847.088	0.31%	18.20%	81.80%	00:06:39	399.160	0.30%
57	192.168.0.34	696	3.586.024	0.29%	17.02%	82.98%	00:03:39	219.749	0.16%
58	192.168.1.19	726	3.360.997	0.27%	24.17%	75.83%	00:04:24	264.876	0.20%
59	192.168.0.22	683	3.216.215	0.26%	31.47%	68.53%	00:05:30	330.539	0.25%
60	192.168.1.35	349	2.900.478	0.23%	43.26%	56.74%	00:01:51	111.312	0.08%
61	192.168.1.22	678	2.840.510	0.23%	21.99%	78.01%	00:02:02	122.044	0.09%
62	192.168.1.34	451	2.818.159	0.23%	44.39%	55.61%	00:02:10	130.750	0.10%
63	192.168.1.24	461	2.733.538	0.22%	30.67%	69.33%	00:02:22	142.861	0.11%
64	192.168.0.33	624	2.290.548	0.18%	41.69%	58.31%	00:01:50	110.020	0.08%
65	192.168.1.17	489	2.228.734	0.18%	13.22%	86.78%	00:05:00	300.302	0.22%
66	192.168.1.56	409	1.832.199	0.15%	44.66%	55.34%	00:13:59	839.583	0.63%
67	192.168.1.102	239	1.744.303	0.14%	1.08%	98.92%	00:01:39	99.280	0.07%
68	192.168.1.124	391	1.701.755	0.14%	33.82%	66.18%	00:02:08	128.678	0.10%
69	192.168.1.40	375	1.628.429	0.13%	32.87%	67.13%	00:01:14	74.794	0.06%
70	192.168.1.21	295	1.499.943	0.12%	13.75%	86.25%	00:01:14	74.519	0.06%
71	192.168.1.39	257	896.803	0.07%	39.21%	60.79%	00:00:43	43.912	0.03%
72	192.168.1.28	229	838.151	0.07%	61.46%	38.54%	00:00:37	37.320	0.03%
73	192.168.1.26	183	805.542	0.06%	26.14%	73.86%	00:01:40	100.373	0.08%
74	192.168.1.25	229	729.274	0.06%	31.14%	68.86%	00:00:39	39.842	0.03%
75	192.168.1.100	122	610.355	0.05%	4.61%	95.39%	00:01:36	96.073	0.07%
76	192.168.1.12	118	554.643	0.04%	21.71%	78.29%	00:02:42	162.646	0.12%
77	192.168.1.142	218	494.119	0.04%	7.10%	92.90%	00:01:52	112.146	0.08%
78	192.168.1.31	77	262.567	0.02%	38.99%	61.01%	00:00:19	19.584	0.01%
79	192.168.1.41	47	231.971	0.02%	56.77%	43.23%	00:00:21	21.786	0.02%
80	192.168.1.73	54	154.703	0.01%	76.27%	23.73%	00:00:01	1.103	0.00%
81	192.168.1.4	3	138.863	0.01%	0.00%	100.00%	00:00:05	5.253	0.00%
82	192.168.1.121	34	82.625	0.01%	91.20%	8.80%	00:00:15	15.943	0.01%
83	192.168.0.35	18	50.498	0.00%	1.90%	98.10%	00:00:25	25.193	0.02%
TOTAL		**242.748**	**1.251.069.673**		**24.58%**	**75.42%**	**37:08:35**	**133.715.657**	
MÉDIA		**2.924**	**15.073.128**				**00:26:51**	**1.611.032**	

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:22

Figura 18 - Relatório de Usuários (Computadores) Ordenado por *Bytes*

Este relatório apresenta como período de 18 de outubro de 2004 a 28 de outubro de 2004, onde os dados são apresentados em ordem decrescente de *Bytes* baixados pelos usuários. Neste relatório são encontradas as seguintes informações:

- ✓ NUM: número seqüencial utilizado para identificar a ordenação, por *Bytes* em ordem decrescente das informações apresentadas no relatório.
- ✓ USUÁRIO: apresenta o *Login* ou Nome do usuário. Neste caso em particular é apresentado o endereço IP, pois não é feita a autenticação dos usuários, o que possibilita a identificação através de *Login*.
- ✓ CONEXÃO: apresenta o número total de conexões efetuadas pelo usuário.
- ✓ *BYTES*: quantidade total de *Bytes* baixados pelo usuário.
- ✓ %*BYTES*: porcentagem referente ao total de *Bytes* baixados para um determinado servidor.
- ✓ *IN-CACHE*: porcentagem do que foi pego em *cache*.
- ✓ *OUT-CACHE*: porcentagem no que foi pego for a do *cache* (servidor de destino).
- ✓ TEMPO GASTO: tempo que levou para baixar todos os seus *Bytes*.
- ✓ MILISEG: tempo que levou para baixar os seus *Bytes*, porém este é apresentado em milesegundos.
- ✓ %TEMPO: porcentagem referente ao total de tempo gasto

Para ilustrar o entendimento das informações apresentadas acima utilizaremos como exemplo o item de número 8 que contém a seguinte informação.

NUM	USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
8	192.168.1.71	4.409	34.342.988	2.75%	21.94%	78.06%	00:55:32	3.332.052	2.49%

Figura 19 - Especificação de Dados do Relatório de Ordem Decrescente de *Bytes*

A figura 19 acima possibilita-nos identificar que o 8º (oitavo) maior número de *Bytes* baixados foi ferio pelo usuário 192.168.1.71. Este usuário efetuou um total de 4.406 conexões, baixando 34.342.988 *Bytes* o que representa 2,75% dos *Bytes* total baixados no período de 18 de outubro de 200 a 28 de outubro de 2004. O percentual *cahe-in* representa

que 21,94% dos dados baixados, estavam disponíveis no *Proxy*, ou seja, não sendo necessário buscá-lo na *Internet*. em contrapartida o *cache-out* representa que 78,06% dos dados baixados não estavam disponíveis no *Proxy*, desta forma, sendo necessário buscá-lo na *Internet*. para efetuar as 4.409 conexões e baixar 34.342.988 *Bytes* gastou-se um tempo de 55 minutos e 32 segundos, o que representa 3.332.052 milesegundos que equivale a 2,49% do tempo total dos *Bytes* total baixados.

4.2.1.2. Relatório dos 100 *Sites* Mais Acessados

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Top 100 sites

	LOCAL ACESSADO	CONEXÃO	BYTES
1	image.ig.com.br	17.624	20.517.437
2	www.unipac.br	14.806	35.611.840
3	www.oi.com.br	13.263	10.262.425
4	img.bol.com.br	10.708	20.531.925
5	voxcards.ig.com.br	5.174	28.350.062
6	br.adserver.yahoo.com	4.708	7.270.498
7	gonline.uol.com.br	4.421	7.149.564
8	us.js1.yimg.com	4.102	59.227.023
9	64.4.55.109	3.530	1.166.381
10	i.s8.com.br	3.498	4.669.687
11	us.i1.yimg.com	3.370	4.751.124
12	img.terra.com.br	3.341	4.569.555
13	www.mercadolivre.com.br	2.443	16.572.848
	LOCAL ACESSADO	CONEXÃO	BYTES
14	zipmail.uol.com.br	2.167	10.699.573
15	mail.opi.yahoo.com	2.158	1.028.964
16	64.4.55.45	2.100	623.398
17	www.globo.com	1.970	3.292.953
18	rad.msn.com	1.938	2.366.828
19	de.uol.com.br	1.901	2.842.136
20	lancenet.ig.com.br	1.867	4.182.976
21	www.acessa.com	1.814	2.649.310
22	www.terra.com.br	1.678	7.387.286
23	br.i1.yimg.com	1.652	8.023.314
24	lp-tc.bol.com.br	1.475	4.523.974
25	www.telemigcelular.com.br	1.452	4.842.335
26	oglobo.globo.com	1.451	3.219.289
27	www.emotioncard.com.br	1.419	4.666.837
28	www.msn.com.br	1.403	4.467.348
29	images.ig.com.br	1.374	818.327
30	adserver.ig.com.br	1.372	3.513.905
31	ipanorama.globo.com	1.341	4.096.321
32	us.csc.adserver.yahoo.com	1.229	500.112
33	www.microsoft.com	1.119	5.845.701
34	www.google.com.br	1.108	2.763.391
35	www.universo.br	1.088	3.027.423

36	www.friweb.com.br	1.008	3.968.122
37	www.ig.com.br	1.005	7.113.692
38	tools.hpg.ig.com.br	1.003	2.300.917
39	www.tribunademinas.com.br	974	3.283.440
40	h.msn.com	948	356.804
41	de.i.uol.com.br	882	6.562.440
42	www.aol.com.br	875	3.338.427
43	www.ibest.com.br	872	1.488.027
44	www.alunoonline.unipac.br	839	1.946.203
45	sc.groups.msn.com	789	1.422.029
46	www2.uol.com.br	778	3.693.679
47	global.msads.net	755	8.898.225
48	barra.uol.com.br	753	2.136.143
49	www.msd-brazil.com	752	8.619.534
50	email-logs.ig.com.br	745	201.921
51	login.yahoo.com	727	5.703.572
52	a248.e.akamai.net	710	1.172.346
53	groups.msn.com	702	20.228.145
54	ads.globo.com	692	4.613.979
55	arvoredobem.ig.com.br	686	1.280.148
56	h.msimg.com	678	235.478
57	images.google.com.br	677	2.273.016
58	ad.br.doubleclick.net	653	1.403.148
59	www.selecoes.com.br	645	749.398
60	www.jb.com.br	639	249.334
61	shopp.img.uol.com.br	600	881.875
62	www.muitafesta.com.br	594	1.280.194
63	img.ibestmail.com.br	580	372.809
64	www.mercadolivre.com	576	960.526
65	www.scielo.br	575	7.757.478
66	www.caixa.gov.br	572	2.253.524
67	by18fd.bay18.hotmail.msn.com	555	7.730.140
68	www.bol.uol.com.br	537	2.122.091
	LOCAL ACESSADO	**CONEXÃO**	**BYTES**
69	www.doctum.com.br	527	1.800.632
70	voxcards.com	516	191.234
71	imagens.oi.com.br	506	3.209.528
72	plasticaebeleza.terra.com.br	506	574.088
73	by1fd.bay1.hotmail.msn.com	501	8.035.837
74	jbonline.terra.com.br	499	1.537.828
75	www.tim.com.br	498	1.304.296
76	www.clicmar.com.br	496	2.241.217
77	images.americanas.com.br	496	878.879
78	home.img.uol.com.br	490	921.246
79	www.cvo.com.br	469	2.456.636
80	www.submarino.com.br	465	13.911.722
81	search.msn.com.br	457	742.850
82	by13fd.bay13.hotmail.msn.com	456	5.314.959
83	www.faseh.com.br	452	1.368.782
84	uv.terra.com.br	434	216.150
85	www.abril.com.br	433	840.231
86	www.joaobidu.com.br	420	1.889.446
87	help.msn.com	420	1.507.249
88	www.piranga.com.br	414	2.866.873
89	www.cancaonova.com	409	1.397.764
90	www.acessa.com.br	409	1.192.603
91	www.bol.com.br	409	202.247
92	www.timmaxitel.com.br	406	1.734.086
93	www.popupad.net	403	552.355
94	somlivre.globo.com	402	785.161
95	maisvoce.globo.com	389	1.629.646

96	par.ad.uol.com.br	367	413.257
97	login.passport.net	366	3.427.482
98	by22fd.bay22.hotmail.msn.com	364	5.252.769
99	www.cobradevidro.com.br	364	2.187.388
100	by10fd.bay10.hotmail.msn.com	362	4.489.804

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:22

Figura 20 - Relatório dos 100 *Sites* com Maior Conexão.

Assim como o anterior, este relatório apresenta como período de 18 de outubro de 2004 a 28 de outubro de 2004, onde os dados são apresentados pelos 100 *sites* que tiveram maior número de conexão. Neste relatório são encontradas as seguintes informações:

- ✓ LOCAL ACESSO: endereço de acesso aos servidores (*sites*).
- ✓ CONEXÃO: quantidade de conexões efetuadas, não confundir com número de *sites* acessados.
- ✓ *BYTES*: quantidade de *Bytes* baixados.

Para ilustrar o entendimento das informações apresentadas acima utilizaremos como exemplo o item de número 2 e 66 que contém a seguintes informações

	LOCAL ACESSADO	CONEXÃO	BYTES
2	www.unipac.br	14.806	35.611.840
66	www.caixa.gov.br	572	2.253.524

Figura 21 - Dados Específicos do Relatório dos 100 Locais de Acesso Com Maior Conexão

A Figura 21 acima nos possibilita identificar o 2º (segundo) *site* pelo "endereço" *www.unipac.br*, este endereço efetuou um total de 14.806 conexões, e baixando 33.611.840 *Bytes*. Da mesma forma podemos visualizar o 66º (sexagésimo sexto) *site*, através de seu "endereço" *www.caixa.gov.br*, o qual efetuou 572 conexões baixando 2.253.524 *Bytes*.

4.2.1.3. Relatório de *Sites* e Usuários Que Acessaram Esses *Sites*

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004

Sites & Users

	LOCAL ACESSADO	USUÁRIOS
1	.www.oi.com.br	192.168.1.95

2	1001cartasdeamor.terra.com.br	192.168.1.93
3	171.66.124.80	192.168.1.51
4	192.168.0.1	192.168.0.5
5	194.192.82.253	192.168.1.76
6	200.154.151.17	192.168.1.93
7	200.157.211.198	192.168.1.71 192.168.1.98
8	200.162.196.5	192.168.1.63
9	200.168.231.201	192.168.1.24 192.168.1.28 192.168.1.95
10	200.175.198.195	192.168.1.80 192.168.1.93 192.168.1.96
11	200.181.132.144	192.168.1.53 192.168.1.65 192.168.1.72 192.168.1.81 192.168.1.96
12	200.182.48.138	192.168.0.7
13	200.189.160.25	192.168.1.71 192.168.1.80
14	200.189.178.36	192.168.1.70
15	200.189.189.2	192.168.1.95 192.168.1.99
16	200.190.254.202	192.168.1.96
17	200.198.90.75	192.168.1.98 192.168.1.99
18	200.202.193.135	192.168.1.93
19	200.202.207.2	192.168.1.98
20	200.202.247.25	192.168.0.21 192.168.1.93
21	200.205.125.211	192.168.1.95
22	200.212.63.19	192.168.1.66 192.168.1.99
23	200.219.198.116	192.168.1.97
24	200.226.126.20	192.168.1.72
25	200.226.127.8	192.168.1.97
26	200.229.32.3	192.168.1.93
27	205.180.85.40	192.168.1.80
28	207.46.110.11	192.168.0.5
	LOCAL ACESSADO	**USUÁRIOS**
29	207.46.110.13	192.168.0.5
30	207.46.110.15	192.168.0.5
31	207.46.110.2	192.168.0.5
32	207.46.110.20	192.168.0.5
33	207.46.110.26	192.168.0.5
34	207.46.110.30	192.168.0.5
35	207.46.110.32	192.168.0.5
36	209.130.45.94	192.168.1.98
37	212.26.221.41	192.168.1.80
38	212.26.221.42	192.168.1.80
39	216.200.145.8	192.168.1.96
40	216.21.229.207	192.168.1.54
41	216.21.232.20	192.168.1.54
42	216.221.138.105	192.168.1.56
43	216.35.213.236	192.168.1.96
44	216.98.142.114	192.168.1.79
45	4mg.com	192.168.1.12
46	64.236.10.217	192.168.1.93
47	64.237.33.182	192.168.1.77
48	64.237.33.98	192.168.1.77
49	64.246.10.150	192.168.1.99
50	64.255.164.70	192.168.1.77 192.168.1.78
51	64.4.16.250	192.168.1.37 192.168.1.63
52	64.4.18.250	192.168.1.93 192.168.1.96
53	64.4.22.250	192.168.1.72
54	64.4.26.250	192.168.1.75
55	64.4.30.250	192.168.1.68 192.168.1.98
56	64.4.34.250	192.168.1.38 192.168.1.93 192.168.1.98
57	64.4.36.250	192.168.1.67
58	64.4.43.250	192.168.1.27
59	64.4.46.250	192.168.1.95
60	64.4.48.250	192.168.1.93 192.168.1.96 192.168.1.97 192.168.1.98
61	64.4.53.250	192.168.1.78 192.168.1.93

62	64.4.55.109	192.168.1.11 192.168.1.124 192.168.1.27 192.168.1.36 192.168.1.37
63	64.4.55.45	192.168.1.101 192.168.1.27 192.168.1.52 192.168.1.58 192.168.1.59
64	65.54.184.250	192.168.1.70 192.168.1.80 192.168.1.97
65	65.54.186.250	192.168.1.81 192.168.1.93 192.168.1.99

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:29

Figura 22 - Relatório de *Sites* relacionado aos Usuários Que os Acessaram

Este relatório também apresenta como período de 18 de outubro de 2004 a 28 de outubro de 2004, onde os dados apresentados são: locais de acesso e os usuários que acessaram estes locais. Neste relatório são encontradas as seguintes informações:

- ✓ LOCAL DE ACESSO: *site* ou "endereço" do servidor que foi acessado.
- ✓ USUÁRIOS: nome do usuário (IP) que acessou a página.

Para ilustrar o entendimento das informações apresentadas acima utilizaremos como exemplo o item de número 7 e 13 que contém as seguintes informações

	LOCAL ACESSADO	USUÁRIOS
7	200.157.211.198	192.168.1.71 192.168.1.98
13	200.189.160.25	192.168.1.71 192.168.1.80

Figura 23 - Dados Específicos do Relatório de *Sites* e Usuários Que Acessaram Esses *Sites*

Tomando como base os *sites* acessados pelo mesmo usuário utilizado na Figura 19 - Especificação de Dados do Relatório de Ordem Decrescente de *Bytes* temos que a Figura 23 acima nos possibilita identificar as suas posições 7 (sétima) e 13 (décima terceira), tendo como acesso em primeiro lugar o *site* ou local de acesso (IP) 200.157.211.198 e 200.189.160.25 respectivamente, juntamente com este usuário, o primeiro local de acesso também foi acessado pelo usuário 192.168.1.98 e o segundo *site* pelo usuário 192.168.1.80.

4.2.1.4. Relatório de *Sites* Negados

Relatório do Proxy Squid - Do Dia

eriodo: 18Oct2004-28Oct2004
NEGADO Relatorio

USUÁRIO	IP/NOME	DATA/HORA	LOCAL ACESSADO
192.168.0.22	192.168.0.22	28/10/2004-21:31:13	http://image.ig.com.br/RealMedia/ads/Creatives/selomercadolivre_ros_051004/selos_webcam.gif
		28/10/2004-16:51:06	http://www.rumo.com.br/Redir.asp?

192.168.0.32	192.168.0.32	28/10/2004-17:23:03	http://br.i1.yimg.com/br.yimg.com/i/br/shopping_mantel/041007_2_playboy.jpg
192.168.0.37	192.168.0.37	28/10/2004-13:42:45	http://br.i1.yimg.com/br.yimg.com/i/br/shopping_mantel/041007_2_playboy.jpg
		28/10/2004-19:22:10	http://br.i1.yimg.com/br.yimg.com/i/br/shopping_mantel/041007_2_playboy.jpg
		28/10/2004-19:37:10	http://br.i1.yimg.com/br.yimg.com/i/br/shopping_mantel/041007_2_playboy.jpg
		28/10/2004-19:37:25	http://br.wrs.yahoo.com/;_ylt=AmgZn9DgmhcrweuUWUPrTJTz6Qt.;_ylu=X3oDMTA2bTQ0OXZjBHNlYwNzcg--/**http%3A%2F%2Fwww.floridareview.com%2Fnovelas.htm
		28/10/2004-19:38:13	http://br.wrs.yahoo.com/;_ylt=ApoqLvTrMeRqpTNNDbHZaADz6Qt.;_ylu=X3oDMTA2bTQ0OXZjBHNlYwNzcg--/**http%3A%2F%2Fwww.rumbora.com.br%2Fnovela
		28/10/2004-19:38:24	http://br.wrs.yahoo.com/;_ylt=Auk0oBlWEIMutZl7NCOl__Tz6Qt.;_ylu=X3oDMTA2bTQ0OXZjBHNlYwNzcg--/**http%3A%2F%2Fwww.horahnews.com%2Ftv%2Fnovelas.htm
USUÁRIO	**IP/NOME**	**DATA/HORA**	**LOCAL ACESSADO**
		28/10/2004-19:35:21	http://cabocla.globo.com/
		28/10/2004-19:35:21	http://cabocla.globo.com/_vti_bin/owssvr.dll?
		28/10/2004-19:34:11	http://comecardenovo.globo.com/Comecardenovo/0,22059,VYP0-3716-20041102-pc,00.html
		28/10/2004-19:34:11	http://comecardenovo.globo.com/_vti_bin/owssvr.dll?
		28/10/2004-19:33:40	http://gmc.globo.com/GMC/0,,2465-p-M216525-MC13,00.html
		28/10/2004-19:33:40	http://gmc.globo.com/_vti_bin/owssvr.dll?
		28/10/2004-13:46:26	http://maisvoce.globo.com/imagens/globo_videochat.gif
		28/10/2004-19:21:29	http://maisvoce.globo.com/imagens/globo_videochat.gif
		28/10/2004-19:21:34	http://maisvoce.globo.com/imagens/globo_videochat.gif
		28/10/2004-19:33:24	http://maisvoce.globo.com/imagens/globo_videochat.gif
		28/10/2004-19:33:58	http://maisvoce.globo.com/imagens/globo_videochat.gif
		28/10/2004-13:46:23	http://maisvoce.globo.com/js/lib_tvgChat.js
		28/10/2004-19:21:19	http://maisvoce.globo.com/js/lib_tvgChat.js
		28/10/2004-19:21:28	http://maisvoce.globo.com/js/lib_tvgChat.js
		28/10/2004-19:21:33	http://maisvoce.globo.com/js/lib_tvgChat.js
		28/10/2004-19:33:23	http://maisvoce.globo.com/js/lib_tvgChat.js
		28/10/2004-19:33:57	http://maisvoce.globo.com/js/lib_tvgChat.js
		28/10/2004-19:33:25	http://senhoradodestino.globo.com/
		28/10/2004-19:33:26	http://senhoradodestino.globo.com/_vti_bin/owssvr.dll?
		28/10/2004-19:33:37	http://www.globo.com/gcom3/tit_videoChat.gif
		28/10/2004-19:34:02	http://www.globo.com/gcom3/tit_videoChat.gif
		28/10/2004-19:34:15	http://www.globo.com/gcom3/tit_videoChat.gif
192.168.0.7	192.168.0.7	28/10/2004-13:51:08	http://cache.unicast.com/upload/production/139804/124400/124402/ibm_brand.wmv
		28/10/2004-13:51:08	http://cache.unicast.com/upload/production/139804/124400/124402/ibm_brand.wmv
		28/10/2004-17:47:29	http://image.ig.com.br/RealMedia/ads/Creatives/selomercadolivre_ros_051004/selos_webcam.gif
		28/10/2004-17:47:29	http://image.ig.com.br/RealMedia/ads/Creatives/selomercadolivre_ros_051004/selos_webcam.gif
		28/10/2004-13:50:06	http://jbonline.terra.com.br/images/cab_colunista_boechat_p.gif
		28/10/2004-13:51:23	http://jbonline.terra.com.br/images/cab_colunista_boechat_p.gif
		28/10/2004-13:51:23	http://jbonline.terra.com.br/images/cab_colunista_boechat_p.gif
		28/10/2004-18:38:23	http://oglobo.globo.com/audios/wma/041028_medico.wma

		28/10/2004-18:38:24	http://oglobo.globo.com/audios/wma/041028_medico.wma
		28/10/2004-18:39:11	http://oglobo.globo.com/audios/wma/romario1410_01.wma
		28/10/2004-18:39:11	http://oglobo.globo.com/audios/wma/romario1410_01.wma
		28/10/2004-17:45:57	http://server.iad.liveperson.net/hc/53111712/x.js?
		28/10/2004-17:45:59	http://server.iad.liveperson.net/hc/53111712/x.js?
		28/10/2004-17:46:01	http://server.iad.liveperson.net/hc/53111712/x.js?
USUÁRIO	**IP/NOME**	**DATA/HORA**	**LOCAL ACESSADO**
		28/10/2004-17:27:46	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:34:45	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:34:50	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:34:50	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:35:16	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:35:16	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:35:56	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:35:56	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:36:19	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:36:19	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:36:33	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:36:33	http://www.doctum.com.br/servicos/images_foco/ctga_computacao_salvador.jpg
		28/10/2004-17:35:29	http://www.doctum.com.br/unidades/gpi/hebert/galeria.jpg
		28/10/2004-13:45:57	http://www.parperfeito.com.br/imagens/pt/btao_procurar.gif
		28/10/2004-18:37:47	http://www.parperfeito.com.br/imagens/pt/btao_procurar.gif
		28/10/2004-13:45:57	http://www.parperfeito.com.br/maestro/logoppoglobobox.gif
		28/10/2004-18:37:47	http://www.parperfeito.com.br/maestro/logoppoglobobox.gif
192.168.1.101	192.168.1.101	28/10/2004-18:29:52	http://chat11.globo.com/jsp/Chat/includes/scripts/valida_box.js
		28/10/2004-18:31:53	http://ipanorama.globo.com/zumzumzum
		28/10/2004-18:38:08	http://ipanorama.globo.com/zumzumzum
192.168.1.102	192.168.1.102	28/10/2004-13:29:23	http://auto.search.msn.com/response.asp?
		28/10/2004-13:29:45	http://auto.search.msn.com/response.asp?
		28/10/2004-13:29:55	http://auto.search.msn.com/response.asp?
		28/10/2004-10:02:02	http://www.yahoo.com.br/
		28/10/2004-10:02:09	http://www.yahoo.com.br/
192.168.1.11	192.168.1.11	28/10/2004-20:45:23	http://br.i1.yimg.com/br.yimg.com/i/br/shopping_mantel/041007_2_playboy.jpg
		28/10/2004-21:01:03	http://senhoradodestino.globo.com/
		28/10/2004-17:58:23	http://tools.hpg.com.br/newxxx/hot_site/imagens/novo_plano01a.gif
		28/10/2004-18:03:30	http://tools.hpg.com.br/newxxx/hot_site/imagens/novo_plano01a.gif
		28/10/2004-18:04:26	http://tools.hpg.com.br/newxxx/hot_site/imagens/novo_plano01a.gif
		28/10/2004-17:58:23	http://tools.hpg.com.br/newxxx/hot_site/imagens/novo_plano02a.gif
		28/10/2004-18:03:30	http://tools.hpg.com.br/newxxx/hot_site/imagens/novo_plano02a.gif
		28/10/2004-18:04:26	http://tools.hpg.com.br/newxxx/hot_site/imagens/novo_plano02a.gif

USUÁRIO	IP/NOME	DATA/HORA	LOCAL ACESSADO
		28/10/2004-21:00:52	http://www.globo.com/gcom3/tit_videoChat.gif
		28/10/2004-17:58:54	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-17:59:18	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:04:59	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:05:17	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:06:12	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:06:43	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:07:39	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:08:05	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:08:25	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:08:40	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:08:56	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:09:13	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:09:33	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:09:49	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:10:02	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:10:12	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:10:28	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:10:43	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:11:01	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:11:24	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:12:02	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:12:34	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:13:17	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:14:32	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:15:03	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:17:07	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:17:31	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:17:48	http://www.hpg.com.br/newxxx/imagens/pixel.gif
		28/10/2004-18:18:27	http://www.hpg.com.br/newxxx/imagens/pixel.gif

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 24 - Relatório de *Sites* Negados

Este relatório apresenta assim como os anteriores o período de 18 de outubro de 2004 a 28 de outubro de 2004, onde o dado apresentado será o “endereço” completo do *site* negado solicitado pelo usuário. Neste relatório são encontradas as seguintes informações:

- ✓ USUÁRIO: nome (IP) ou *login* do usuário
- ✓ IP/NOME: número do IP da máquina ou nome da mesma.
- ✓ DATA/HORA: data e horário em que esse acesso se realizou.
- ✓ LOCAL ACESSADO: “endereço” completo do *site* que foi negado.

Para ilustrar o entendimento das informações apresentadas acima utilizaremos como exemplo o usuário 192.168.1.101 que contém a seguinte informação

USUÁRIO	IP/NOME	DATA/HORA	LOCAL ACESSADO
192.168.1.101	192.168.1.101	28/10/2004-18:29:52	http://chat11.globo.com/jsp/Chat/includes/scripts/valida_box.js
		28/10/2004-18:31:53	http://ipanorama.globo.com/zumzumzum
		28/10/2004-18:38:08	http://ipanorama.globo.com/zumzumzum

Figura 25 - Especificação de Dados Apresentados no Relatório de *Sites* Negados

A Figura 25 acima nos possibilita identificar os locais acessados pelo usuário 192.168.1.101 utilizando o computador 192.168.1.101 que foram negados como é o caso do *site* http://chat11.globo.com/jsp/Chat/includes/scripts/valida_box.js, acessado no dia 28 de outubro de 2004 as 18 horas 29 minutos e 52 segundos, esse mesmo usuário ainda requisitou outro *site* duas vezes, o qual também foi negado, sendo ele http://ipanorama.globo.com/zumzumzum, a primeira foi no dia 28 de outubro de 2004 as18 horas 31 minutos e 53 segundos e há outro pouco depois as 18 horas 38 minutos e 08 segundos.

4.2.1.5. Relatório de *Sites* Acessados por Cada Usuários (Computadores) Ordenados por *Bytes*

Os relatórios abaixo, são semelhantes ao primeiro relatório, com a diferença de que o primeiro relatório apresentava os dados de todos os usuários juntos, este entretanto, apresenta um relatório individual de usuário (IP) sobre cada *site* que este acessou.

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Usuario: 192.168.0.35
Ordem: BYTES, reverse
Usuario Relatorio

LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO	MILISEG	%TEMPO
www.windowsupdate.com	9	26.525	52.53%	3.62%	96.38%	00:00:10	10.827	42.98%
v4.windowsupdate.microsoft.com	6	23.301	46.14%	0.00%	100.00%	00:00:10	10.561	41.92%
wustat.windows.com	3	672	1.33%	0.00%	100.00%	00:00:03	3.805	15.10%
TOTAL	**18**	**50.498**	**0.00%**	**1.90%**	**98.10%**	**00:00:25**	**25.193**	**0.02%**
MÉDIA	**0**	**15.073.128**				**00:26:51**	**1.611.032**	**1.20%**

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 26 - Relatório dos *Sites* Acessados Pelo Usuário (Computador) 192.168.0.35

Este relatório apresenta como período de 18 de outubro de 2004 a 28 de outubro de 2004, onde os dados são apresentados em ordem decrescente de *Bytes* baixados por um determinado usuário. Neste relatório são encontradas as seguintes informações:

- ✓ LOCAL DE ACESSO: apresenta o *site* ao qual o usuário acessou.
- ✓ CONEXÃO: apresenta o número total de conexões efetuadas pelo usuário.
- ✓ *BYTES*: quantidade total de *Bytes* baixados pelo usuário.
- ✓ %*BYTES*: porcentagem referente ao total de *Bytes* baixados para um determinado servidor.
- ✓ *IN-CACHE*: porcentagem do que foi pego em *cache*.
- ✓ *OUT-CACHE*: porcentagem no que foi pego for a do *cache* (servidor de destino).
- ✓ TEMPO GASTO: tempo que levou para baixar todos os seus *Bytes*.
- ✓ MILISEG: tempo que levou para baixar os seus *Bytes*, porém este é apresentado em milesegundos.
- ✓ %TEMPO: porcentagem referente ao total de tempo gasto

Para ilustrar o entendimento das informações apresentadas acima utilizaremos como exemplo o usuário 192.168.1.101 que contém a seguinte informação

LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
www.windowsupdate.com	9	26.525	52.53%	3.62%	96.38%	00:00:10	10.827	42.98%

Figura 27 - Especificação de Dados Gerados Pelo Usuário 192.168.0.35

A Figura 27 acima nos possibilita identificar os locais acessados pelo usuário 192.168.0.35 e os dados gerados neste acesso.

Este usuário acessou o *site www.windowsupdate*, efetuando um total de 9 conexões, baixando 26.525 *Bytes* o que representa 52,53% dos *Byte*s total baixados no período de 18 de outubro de 200 a 28 de outubro de 2004 o percentual *cahe-in* representa que 3.62% dos dados baixados, estavam disponíveis no *Proxy*, ou seja, não sendo necessário buscá-lo na *Internet*.

em contrapartida o *cache-out* representa que 96.38% dos dados baixados não estavam disponíveis no *Proxy*, desta forma, sendo necessário buscá-lo na *Internet*. para efetuar as 9 conexões e baixar 26.525 *Bytes* gastou-se um tempo de 10 segundos, o que representa 10.827 milesegundos que equivale a 42,98% do tempo total dos *Bytes* total baixados.

Estas regras e este exemplo devem ser seguidos como um modelo para a interpretação da Figura 28 posteriormente.

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Usuario: 192.168.0.21
Ordem: BYTES, reverse
Usuario Relatorio

LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE	OUT	TEMPO GASTO	MILISEG	%TEMPO
www.98fm.com.br	174	1.509.037	12.96%	0.69%	99.31%	00:00:53	53.251	6.30%
www.universo.br	436	1.435.626	12.33%	44.01%	55.99%	00:00:23	23.323	2.76%
www.faseh.com.br	452	1.368.782	11.75%	10.82%	89.18%	00:02:06	126.082	14.93%
www.guarani.com.br	130	1.035.730	8.89%	0.09%	99.91%	00:02:21	141.609	16.77%
www.unifenas.br	84	778.055	6.68%	31.33%	68.67%	00:00:17	17.458	2.07%
wm53.ig.com.br	43	764.836	6.57%	0.03%	99.97%	00:00:42	42.556	5.04%
www.superesportes.com.br	99	565.660	4.86%	12.26%	87.74%	00:00:30	30.686	3.63%
www.unipac.br	206	532.530	4.57%	10.14%	89.86%	00:00:44	44.373	5.25%
www.pseletivo.unincor.br	11	462.747	3.97%	0.00%	100.00%	00:00:15	15.649	1.85%
morango.ig.com.br	72	417.905	3.59%	0.00%	100.00%	00:00:15	15.169	1.80%
image.ig.com.br	300	371.650	3.19%	83.52%	16.48%	00:00:04	4.194	0.50%
200.202.247.25	55	354.001	3.04%	0.33%	99.67%	00:00:21	21.103	2.50%
mmads1.mmonline.com.br	28	341.533	2.93%	0.06%	99.94%	00:00:26	26.394	3.13%
www.uai.com.br	33	318.170	2.73%	0.95%	99.05%	00:00:10	10.281	1.22%
www.caixa.gov.br	65	282.542	2.43%	12.18%	87.82%	00:00:07	7.722	0.91%
www.unincor.br	36	146.054	1.25%	0.26%	99.74%	00:00:10	10.889	1.29%
www.ufmg.br	77	125.395	1.08%	0.43%	99.57%	00:00:17	17.825	2.11%
cam.ponte.com.br	6	109.257	0.94%	0.00%	100.00%	00:00:26	26.938	3.19%
site.unibh.br	16	96.888	0.83%	0.00%	100.00%	00:00:11	11.987	1.42%
www.mec.gov.br	20	96.860	0.83%	19.55%	80.45%	00:00:01	1.572	0.19%
www1.caixa.gov.br	49	84.997	0.73%	5.38%	94.62%	00:00:03	3.476	0.41%
www.ig.com.br	18	81.650	0.70%	30.86%	69.14%	00:00:01	1.304	0.15%
www.meioemensagem.com.br	64	79.928	0.69%	0.00%	100.00%	00:00:26	26.868	3.18%
LOCAL ACESSADO	**CONEXÃO**	**BYTES**	**%BYTES**	**IN-CACHE**	**OUT**	**TEMPO GASTO**	**MILISEG**	**%TEMPO**
www.uaimail.com.br	30	37.026	0.32%	0.00%	100.00%	00:00:04	4.506	0.53%
adserver.ig.com.br	14	34.111	0.29%	0.00%	100.00%	00:00:01	1.739	0.21%
search.msn.com.br	20	22.222	0.19%	11.65%	88.35%	00:00:04	4.055	0.48%
banners3.estaminas.com.br	36	17.042	0.15%	12.65%	87.35%	00:00:14	14.128	1.67%
www8.estaminas.com.br	35	16.942	0.15%	12.68%	87.32%	00:00:10	10.783	1.28%
abril.assineabril.com	23	15.617	0.13%	0.00%	100.00%	00:00:01	1.269	0.15%
br.cade.busca.yahoo.com	4	15.124	0.13%	0.00%	100.00%	00:00:13	13.356	1.58%
afiliados.submarino.com.br	2	13.128	0.11%	94.74%	5.26%	00:00:00	221	0.03%
banners.estaminas.com.br	19	12.303	0.11%	84.60%	15.40%	00:00:00	877	0.10%
www.pa.uai.com.br	6	9.597	0.08%	61.47%	38.53%	00:00:00	843	0.10%
us.i1.yimg.com	6	9.020	0.08%	100.00%	0.00%	00:00:00	30	0.00%
www.windowsupdate.com	3	8.832	0.08%	0.00%	100.00%	00:00:15	15.122	1.79%
www.mmonline.com.br	45	8.695	0.07%	0.00%	100.00%	00:00:21	21.813	2.58%
webmail.ig.com.br	2	8.590	0.07%	0.00%	100.00%	00:00:00	369	0.04%
br.cade.yahoo.com	2	8.437	0.07%	0.00%	100.00%	00:00:04	4.204	0.50%

v4.windowsupdate.microsoft.com	2	7.767	0.07%	0.00%	100.00%	00:00:04	4.917	0.58%
images.ig.com.br	21	6.831	0.06%	100.00%	0.00%	00:00:00	56	0.01%
www.update.fundac.org.br	6	5.175	0.04%	0.00%	100.00%	00:00:02	2.773	0.33%
www.morango.com.br	9	5.051	0.04%	0.00%	100.00%	00:00:03	3.958	0.47%
mmonline.ad.adnetwork.com.br	6	3.903	0.03%	0.00%	100.00%	00:00:00	991	0.12%
email-logs.ig.com.br	13	3.393	0.03%	0.00%	100.00%	00:00:01	1.642	0.19%
a0.mmonline.isee1.net	8	3.276	0.03%	0.00%	100.00%	00:00:01	1.336	0.16%
www.mercadomineiro.com.br	4	2.492	0.02%	0.00%	100.00%	00:00:00	674	0.08%
www.unibh.br	3	1.608	0.01%	0.00%	100.00%	00:00:14	14.011	1.66%
ad.adnetwork.com.br	2	1.322	0.01%	0.00%	100.00%	00:00:00	260	0.03%
auto.search.msn.com	2	1.204	0.01%	0.00%	100.00%	00:00:01	1.242	0.15%
wrs.yahoo.com	2	1.184	0.01%	0.00%	100.00%	00:00:00	862	0.10%
contamail.ig.com.br	1	1.023	0.01%	0.00%	100.00%	00:00:00	129	0.02%
contaclique.ig.com.br	1	1.009	0.01%	0.00%	100.00%	00:00:00	124	0.01%
cade.drs.yahoo.com	2	919	0.01%	0.00%	100.00%	00:00:02	2.515	0.30%
pa.yahoo.com	2	890	0.01%	0.00%	100.00%	00:00:01	1.000	0.12%
ad.credicard.com.br	2	740	0.01%	0.00%	100.00%	00:00:00	825	0.10%
sc.msn.com	3	722	0.01%	100.00%	0.00%	00:00:00	5	0.00%
www.cade.com.br	2	676	0.01%	0.00%	100.00%	00:00:01	1.895	0.22%
ig.com.br	3	585	0.01%	100.00%	0.00%	00:00:00	3	0.00%
g.msn.com	1	441	0.00%	0.00%	100.00%	00:00:01	1.036	0.12%
us.js1.yimg.com	2	420	0.00%	100.00%	0.00%	00:00:00	2	0.00%
wustat.windows.com	1	224	0.00%	0.00%	100.00%	00:00:11	11.357	1.34%
www.estaminas.com.br	1	171	0.00%	0.00%	100.00%	00:00:00	164	0.02%
www.lancenet.com.br	1	0	0.00%	0.00%	0.00%	00:00:16	16.866	2.00%
igshopping.ig.com.br	1	0	0.00%	0.00%	0.00%	00:00:01	1.925	0.23%
TOTAL	**2.822**	**11.647.545**	**0.93%**	**13.83%**	**86.17%**	**00:14:04**	**844.592**	**0.63%**
MÉDIA	**34**	**15.073.128**				**00:26:51**	**1.611.032**	**1.20%**

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 28 - Relatório dos *Sites* Acessados Pelo Usuário (Computador) 192.168.0.21

4.2.1.6. Relatório de Transmissão de *Bytes* por Hora

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Usuario: 192.168.1.95

	00 BYTES	01 BYTES	02 BYTES	03 BYTES	04 BYTES	05 BYTES	06 BYTES	07 BYTES	08 BYTES	09 BYTES	10 BYTES	11 BYTES	12 BYTES
28/10/2004	0	0	0	0	0	0	0	4.704.138	7.763.974	6.152.406	5.254.464	10.532.810	8.177.045
TOTAL	0	0	0	0	0	0	0	4.704.138	7.763.974	6.152.406	5.254.464	10.532.810	8.177.045

13 BYTES	14 BYTES	15 BYTES	16 BYTES	17 BYTES	18 BYTES	19 BYTES	20 BYTES	21 BYTES	22 BYTES	23 BYTES	TOTAL BYTES
8.733.369	12.532.025	4.707.444	9.438.855	8.065.015	2.957.169	9.622.160	871.619	1.647.592	0	0	101.160.085
8.733.369	12.532.025	4.707.444	9.438.855	8.065.015	2.957.169	9.622.160	871.619	1.647.592	0	0	101.160.085

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 29 - Relatório de Transmissão de *Bytes* por Hora do Usuário (Computador) 192.168.1.95

Este relatório apresenta como período de 18 de outubro de 2004 a 28 de outubro de 2004, onde os dados são apresentados de *Bytes* informados de hora-em-hora. Neste relatório são encontradas as seguintes informações:

- ✓ *BYTES*: esses *Bytes* vem precedido de um número, o qual informa a hora.
- ✓ DIA: está opção não tem por escrito, no entanto, a primeira coluna e a partir da segunda linha encontra-se o dia que estes dados foram criados.
- ✓ TOTAL: informa o total de *Bytes* utilizados, caso houvesse mais dias, somava-se um total de *Bytes* por hora.
- ✓ TOTAL DE *BYTES*: esta opção soma o total de *Bytes* utilizado em um dia e o total de *Bytes* utilizado por todos os dias.

Para ilustrar o entendimento das informações apresentadas acima utilizaremos como exemplo a seguinte informação:

	…	05 BYTES	06 BYTES	07 BYTES	08 BYTES	…	21 BYTES	22 BYTES	23 BYTES	TOTAL BYTES
28/10/2004	…	0	0	4.704.138	7.763.974	…	1.647.592	0	0	101.160.085
TOTAL	…	0	0	4.704.138	7.763.974	…	1.647.592	0	0	101.160.085

Figura 30 - Ilustração Para Entendimento das Informações Apresentadas na Figura 29

A Figura 30 acima nos possibilita visualizar como foi à transferência de *Bytes* durante o dia pelo usuário 192.168.1.95

Podemos perceber que no período que antecede as 7 horas não havia qualquer tráfego de *Bytes*, a partir de 7 horas esse tráfego começa com um entrada e *Bytes* de 4.704.138, seguido por 7.763.974 as 8 horas e indo até as 21 horas com um transmissão de 1.647.592 *Bytes*, após esse horário não há mais qualquer tráfego. Finalizando é apresentado um total de *Bytes* no final do relatório.

Estas considerações servem de orientação para as Figuras 31 e 32 abaixo.

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Usuario: 192.168.1.98

	00 BYTES	01 BYTES	02 BYTES	03 BYTES	04 BYTES	05 BYTES	06 BYTES	07 BYTES	08 BYTES	09 BYTES	10 BYTES	11 BYTES	12 BYTES
28/10/2004	0	0	0	0	0	0	0	3.246.217	8.656.642	15.185.574	7.162.224	3.949.749	4.811.067
TOTAL	0	0	0	0	0	0	0	3.246.217	8.656.642	15.185.574	7.162.224	3.949.749	4.811.067

13 BYTES		15 BYTES	16 BYTES	17 BYTES	18 BYTES	19 BYTES	20 BYTES	21 BYTES	22 BYTES	23 BYTES	TOTAL BYTES
7.982.488	11.159.944	2.324.675	6.908.400	3.725.942	5.225.204	7.201.616	9.437.965	4.308.338	0	0	101.286.045
7.982.488	11.159.944	2.324.675	6.908.400	3.725.942	5.225.204	7.201.616	9.437.965	4.308.338	0	0	101.286.045

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 31 - Relatório de Transmissão de *Bytes* por Hora do Usuário (Computador) 192.168.1.98

Relatório do Proxy Squid - Do Dia

Periodo: 18Oct2004-28Oct2004
Usuario: 192.168.0.21

	00 BYTES	01 BYTES	02 BYTES	03 BYTES	04 BYTES	05 BYTES	06 BYTES	07 BYTES	08 BYTES	09 BYTES	10 BYTES	11 BYTES	12 BYTES
28/10/2004	0	0	0	0	0	0	0	0	0	0	36.186	0	0
TOTAL	0	0	0	0	0	0	0	0	0	0	36.186	0	0

13 BYTES	14 BYTES	15 BYTES	16 BYTES	17 BYTES	18 BYTES	19 BYTES	20 BYTES	21 BYTES	22 BYTES	23 BYTES	TOTAL BYTES
159.321	0	57.821	0	1.842.997	57.731	2.990.482	665.209	5.837.798	0	0	11.647.545
159.321	0	57.821	0	1.842.997	57.731	2.990.482	665.209	5.837.798	0	0	11.647.545

Gerado por sarg-1.2.2.1 13Jun2002 em 29/Oct/2004-14:32

Figura 32 - Relatório de Transmissão de Bytes por Hora do Usuário (Computador) 192.198.0.21

5. CONCLUSÃO

Hoje em dia algumas organizações ainda não provêm de um controle em seus laboratórios e redes quanto ao acesso à *Internet*, podendo estes, serem usados por usuários da forma que bem entendem, tornando assim o local que deveria ser de estudo ou trabalho em um ambiente para pesquisas pessoais. Isso ocorre, porque não há um controle sobre estes sistemas.

As ferramentas SARG e MRTG permitiram, demonstrar que é possível monitorar o que se passa por trás de uma rede de computadores que tem acesso a *internet*.

Após a coleta dos dados, podemos verificar que, foi possível gerenciar a rede de um laboratório, por um período de tempo determinado. Portanto fica provado que qualquer ambiente organizacional pode ser monitorado por um administrador, o qual terá acesso aos relatórios, fazendo com que a rede não fique com um tráfego desnecessário e que o acesso à *internet* passe a ser apenas para fins de pesquisa e trabalho. Contudo, não existe uma configuração específica para o funcionamento das ferramentas, cada uma irá depender da necessidade e dos recursos de cada instituição.

De acordo com os resultados apresentados, concluo que as ferramentas atenderam as necessidades esperadas, dando um suporte à administração da rede, sendo que estas, apresentaram dados concretos em relação ao tráfego da rede e ao conteúdo desse tráfego, sendo eles, *sites* acessados, conexões realizadas, *Bytes* de entrada, entre outros.

Como sugestão para trabalhos futuros, fica como idéia:

- ✓ desenvolver ferramentas de análise de dados, utilizando-se de técnicas de Inteligência Artificial e/ou *Datamining;*
- ✓ Efetuar o gerenciamento da rede utilizando-se de outras ferramentas.

6. BIBLIOGRAFIA

BALL, Bill; PITTS, David. Dominando Red Hat Linux 7: Servidor Apache. Edição única. Rio de Janeiro: Editora Ciência Moderna Ltda. 2002.

CAMPOS, Augusto C. Monitoramento com o MRTG. Linux in Brasil. Disponível em: <http//brlinux.linuxsecurity.com.br/artigos/dicas_mrtg.htm/> Acesso em 20 ago. 2004

CAMPOS, Augusto C. Squid. Linux in Brasil. Disponível em: <http://brlinux.linuxsecurity.com.br/artigos/dicas_squid_nt.htm/> Acesso em 20 ago. 2004

CISNEIROS, Hugo. Utilizando o Crontab. Publicado em 2003, Disponível em: <http://www.devin.com.br/eitch/crontab/> Acesso em 25 nov. 2004

Anônimo. Dicionário de Tecnologia**.** Disponível em <http://www.hostgold.com.br/hospedagem-sites/dicionario15.html> Acesso em 10 nov. 2004

Anônimo. O que é MRTG**.** Disponível em: <http://www.nsite.com.br/oque_mrtg.htm/> Acesso em 22 ago. 2004

OLIVEIRA, Lécia de Souza. O Protocolo SNMP. 18f, (graduação em informática). Universidade Católica de Salvador, Salvador. 2003

SOUZA, Cristhiane. Gerenciamento de Rede Usando SNMP Disponível em: <http://www.dsr.inpe.br/dsr/cristhiane/Gerenciamento%20de%20Redes%20usando %20SNMP.doc> Acesso em 1 ago. 2004