Um Ambiente de Gerenciamento de Medições por Fluxo de Tráfego Baseado na utilização de Mapas em árvore

Leobino Sampaio, Marcio Almeida, José A. Suruagy Monteiro, Manoel Mendonça

Núcleo Interdepartamental de Pesquisa em Redes de Computadores (NUPERC), UNIFACS
R. Agnelo de Brito, 116, Salvador, Ba, Brasil, 40171-100
{leobino,marcioalmeida,suruagy,mgmn}@unifacs.br

Abstract. *Traffic flow measurements are very useful for identifying the characteristics and distribution of network traffic in a backbone. However, the amount of collected data from these measurements is too large what makes it difficult to analyze and manage. Many of the tools used to assist in this task are very limited and don't allow a more detailed analysis of many important variables that could be correlated in order to have a more precise network diagnostic . This work shows how the use of the tree-map visualization technique combined with traffic flow measurements can contribute to a better network management.*

Keywords. *Netflow, Flow-tools, TreeMap, Measurements, Network management*

Resumo. *As medições por fluxo de tráfego são bastante úteis quando se deseja identificar as características e distribuição do tráfego das redes de um backbone. Porém, o volume de dados coletados a partir destas medições é muito grande o que dificulta a sua análise e gerência. Muitas das ferramentas utilizadas para auxiliar neste trabalho são bastante limitadas e não permitem uma análise mais detalhada de diversas variáveis importantes e que poderiam ser correlacionadas a fim de se ter um diagnóstico mais preciso da rede. Este trabalho mostra como a utilização da técnica de visualização Mapas em Árvore em conjunto com as medições por fluxo de tráfego pode contribuir para uma melhor gerência da rede.*

Palavras-Chave: *Netflow, Flow-tools, Mapa em Árvore, Medições, Gerenciamento de redes*

1. Introdução

As redes IP modernas possuem diversos problemas de infra-estrutura, tais como o congestionamento das filas dos equipamentos, a falta de priorização de serviços, dentre outros. Em função disto é necessário se ter informações relevantes sobre o tráfego a fim de saber como resolver ou amenizar estes problemas. Com o uso de ferramentas de coleta, armazenamento e visualização dos dados sobre a rede, torna-se possível à elaboração de diagnósticos mais ricos e precisos, facilitando, assim, o processo de tomada de decisão.

Não resta dúvidas quanto à utilização e permanência das redes IP nos backbones da Internet. Sua imensa base instalada e o conjunto de aplicações dos usuários finais fazem com que esta solução seja a tendência natural dos próximos anos. O IP atende muito bem às aplicações convencionais. Porém, as novas aplicações (ex. multimídia) possuem outros requisitos de QoS para os quais estas redes não foram projetadas. Em função desta limitação, através da arquitetura Diffserv, foi proposta a solução de fornecer tratamento diferenciado aos diversos fluxos de pacotes que trafegam nos roteadores do backbone. Nesta solução, os serviços prestados são contratados pelos acordos de nível de serviço, ou SLAs (*Service Level Agreement*), que fornecem garantias mínimas sobre o serviço prestado.

Neste cenário, surge a necessidade de se obter mecanismos que monitorem os serviços prestados de forma que possam ser verificados se os parâmetros estabelecidos na SLA estão sendo realmente atendidos. Outro fator importante é que para se realizar um contrato é preciso saber se a rede suporta suas exigências. Informações sobre o número de *hosts*, volume do tráfego e a distribuição dos serviços são exemplos de informações que irão ajudar a identificar as condições mínimas da rede para prover serviços a novos usuários.

Em função destes fatores, percebe-se a necessidade de ferramentas de medições que ajudem na coleta dos dados sobre as métricas de interesse relacionadas a QoS das aplicações. Para isso, é necessário levar em consideração, além das métricas desejadas, as técnicas de medição e as ferramentas existentes. Existem basicamente dois tipos de medições: passivas e ativas. Nas medições passivas são coletadas informações sobre todos os pacotes que trafegam na rede sem provocar nenhuma interferência no tráfego, enquanto que nas medições ativas são gerados pacotes de teste que terão os seus desempenhos monitorados através da rede. Cada um desses tipos possui um propósito específico, e a sua utilização varia de acordo com as métricas escolhidas e as tecnologias de hardware ou software disponíveis.

Nas medições passivas, principalmente nos *links* de alta velocidade, o volume do tráfego se torna um problema, na medida em que exige uma boa capacidade de armazenamento e gerenciamento dos dados coletados. Neste contexto, a Cisco propõe a utilização do Netflow para reduzir parte do volume de dados coletados [6]. Isso é feito através da criação de regras na definição de fluxos[1] nos próprios roteadores da rede, ao invés de trabalhar diretamente com cada pacote individual. Estes fluxos são coletados por uma ferramenta específica, armazenados em sistema de arquivos e depois processados de acordo com a necessidade identificada de análise dos dados.

Ainda assim, essas medições geram conjuntos volumosos de informações, que mesmo quando bem estruturados são difíceis de serem explorados. Na maioria das vezes são utilizados *scripts* para extração de informações de arquivos texto e a análise é feita apenas em função de uma única variável (ex. serviço, endereço de origem, octetos, etc.). O problema persiste na parte de visualização dos dados, quando são gerados gráficos de poucas dimensões dificultando as análises mais específicas e o gerenciamento do desempenho das redes.

---

[1] Pode ser considerado como um conjunto de pacotes IP que possuem atributos em comum (ex: IP fonte, IP destino, porta fonte, porta destino, protocolo, etc.).

Para extrair informação útil desses conjuntos são necessárias técnicas e ferramentas que explorem de forma eficiente os dados disponíveis. Entre os meios que os seres humanos podem usar para explorar dados, a visualização é talvez o mais intuitivo. Isto se deve ao fato do homem possuir uma memória de curto prazo bastante limitada que não é adequada à memorização de grandes listas e tabelas, como as apresentadas na maioria dos relatórios das ferramentas de medições atuais.

Algumas ferramentas como o MRTG [4] e o *Flowscan* [5] apresentam os dados coletados a partir de gráficos bastante limitados, pois utilizam poucas variáveis de análise e não permitem interação em tempo real.

Diante disso, os computadores vêm sendo usados cada vez mais para promover a comunicação visual de informações e, segundo Shneiderman [8], o uso dos computadores é também muito útil para a representação visual de dados abstratos. Com o uso dos princípios propostos por Tufte [9] é possível apresentar centenas, milhares ou até milhões de registros de dados em uma única cena visual, criando assim um eficiente meio de interpretação de grandes volumes de dados. Isso se torna bastante conveniente ao se tratar de uma visualização de um *backbone* formado por diversas redes menores em que se tem mais de uma variável de análise.

Nesse universo de tipos de dados, as estruturas hierárquicas de informação são extremamente comuns e estão presentes nos dados gerados pelos fluxos, onde existe muita informação sobre a característica do tráfego e a sua distribuição na rede ao longo do tempo. Apesar disto, atualmente esta característica não é muito explorada pelas ferramentas de visualização de fluxos onde são geradas informações de difícil interpretação. As ferramentas e plataformas de gerência de redes são mais focadas em detecção e sinalização de falhas e identificação de problemas, não cobrindo necessariamente a rede como um todo e possuindo uma visibilidade muito limitada.

É com base no exposto acima que este trabalho mostra como a utilização da técnica de mapas em árvore pode facilitar o gerenciamento das medições por fluxo de tráfego.

Este trabalho, que se insere dentro do escopo das atividades de medições do grupo de trabalho de Qualidade de Serviço da RNP, é validado através da implementação de um protótipo em que são utilizados o Netflow para criação dos fluxos, o pacote *flow-tools* [7] para a coleta e processamento de alguns dados e por fim a utilização do TreeMiner[2] como ferramenta de visualização e análise.

Este artigo está organizado da seguinte forma: a seguir, são apresentadas algumas ferramentas de medição com ênfase nas voltadas para medições por fluxo. Na seção 3 são apresentados os conceitos básicos de visualização de dados hierárquicos através de mapas em árvore, na seção 4 são apresentados os experimentos realizados com o protótipo. Por fim, a seção 5 apresenta as considerações finais e trabalhos futuros.

[2] Ferramenta de exploração visual baseada em mapas em árvore em desenvolvimento no Nuperc

2. Ferramentas de Medições

Como citado anteriormente, a escolha de uma ferramenta de medição depende do tipo de medição a ser realizada e das métricas de interesse. Em termos de medições ativas, ideais para o monitoramento de medidas como atraso, variação do atraso e conectividade, existem diversas infra-estruturas de medições que em sua grande maioria utiliza o programa *ping* e suas variantes para obter os dados da rede através das estatísticas do RTT (*round-trip-time*) dos pacotes de teste. Destacam-se nesta área as iniciativas do AMP (*Active Measurement Project*) [10], Surveyor [12] e TTM-RIPE [11]. Nas medições passivas, algumas ferramentas como o Coralreef [13] possuem *drivers* que dão suporte à utilização de placas para captura do tráfego em redes ópticas, bem como Ethernet com o propósito de fazer o monitoramento sem interferir no meio. Em função do objeto de estudo deste trabalho, será dada maior ênfase nas ferramentas de medições passivas por fluxo de tráfego.

Para este tipo de medição, o IETF propõe a padronização do RTFM (*Realtime Traffic Flow Measurement*) [1][2] que possui, basicamente, três componentes: o medidor, o coletor e o gerente, de acordo com a Figura 1. O primeiro converte os pacotes coletados e os associam às tabelas de fluxos. O segundo recebe as tabelas que posteriormente serão utilizadas por uma aplicação. O terceiro gerencia os outros dois. Com base neste modelo, o NeTraMet (*Network Traffic Meter*) [3] foi implementado com o propósito de desempenhar as funções dos três componentes. Trata-se de um software de código aberto, que tem a vantagem de permitir ao usuário a possibilidade de definir regras que identificam fluxos de dados através da programação de *scripts*, permitindo uma maior flexibilização e dinamismo no trabalho de quantificar e qualificar os tipos de fluxos. O pacote ainda possui o NetFlowMet que obtém os seus dados a partir dos fluxos identificados e exportados pelos roteadores Cisco. Além do NetraMet, outras ferramentas destacam-se nas medições por fluxo e serão descritas nas subseções seguintes.

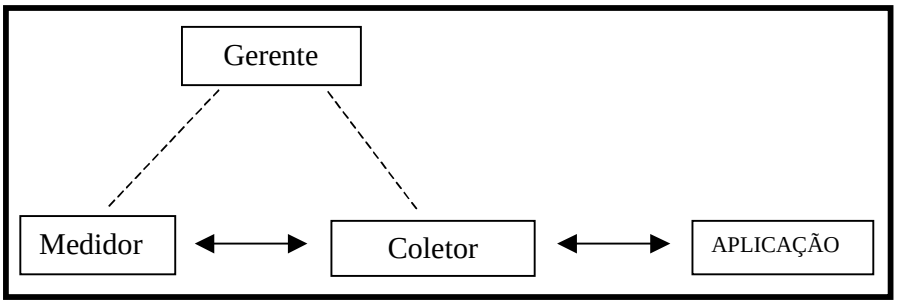


Figura 1. Modelo RTFM

2.1. Netflow

O NetFlow é um produto da Cisco que possibilita a criação de regras para a identificação de fluxos no próprio roteador da rede, exercendo a função de medidor. Os dados coletados sobre estes fluxos, assim definidos devem ser encaminhados para um servidor, a fim de que possam ser tratados por um software específico de coleta. A Figura 2 apresenta uma visão genérica do funcionamento do Netflow.

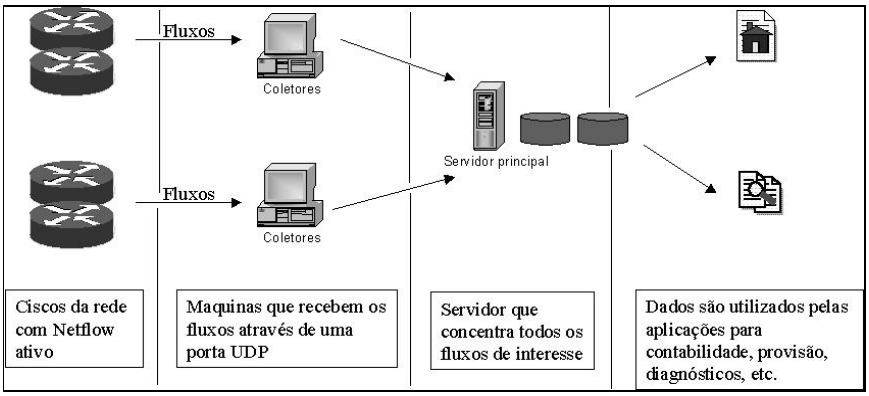


Figura 2. Funcionamento do Netflow

Um fluxo é identificado quando o primeiro pacote chega numa interface de rede configurada com o Netflow. A partir deste momento, todos os outros pacotes com as mesmas características são contabilizados na tabela de fluxos em número de octetos e pacotes. O registro do fluxo permanece na tabela até que uma das seguintes condições ocorra:

- fim da conexão TCP (*TCP FIN ou RST*).
- A tabela atingiu seu limite de tamanho.
- Expiração do tempo de inatividade (tempo que em não chegam pacotes com a característica do fluxo).
- Expiração do tempo de atividade (tempo máximo que um fluxo pode permanecer na tabela).

Os dados do Netflow são exportados através de pacotes UDP para uma porta configurada no coletor. Cada pacote é formado por um cabeçalho seguido dos fluxos e o seu formato varia de acordo com a versão do Neflow.

Na versão 8 do Netflow são criados fluxos agregados (fluxos de fluxos), ou seja, fluxos contabilizados a partir dos fluxos expirados e com critérios mais genéricos, por exemplo: ToS, AS, rede Destino, rede origem. Para isso, uma outra tabela de fluxos é criada de acordo com a versão que foi configurada (ex: 8.1, 8.2, etc.). Vale lembrar, que no caso de um roteador ser configurado com as versões 5 e 8 e estar enviando os fluxos para o mesmo coletor é preciso que sejam configuradas portas UDP diferentes.

2.2. Flow-tools

O pacote Flow-tools é composto por um conjunto de programas que tem a finalidade de fazer a coleta dos fluxos enviados pelo NetFlow. O pacote foi desenvolvido em C e possui suporte para exportar dados para outros softwares de visualização (Flowscan) e coleta (Cflowd). Em função do uso específico para o Netflow, o mesmo é marcado pela sua simplicidade na coleta, visualização e totalização dos fluxos. O software ainda fornece suporte à coleta distribuída e ao gerenciamento dos fluxos armazenados em disco. A Tabela 1 apresenta as descrições das ferramentas do pacote.

Tabela 1. Algumas das ferramentas do pacote flows-tools

Ferramenta	Finalidade
Flow-capture	Faz a captura dos fluxos exportados pelos roteadores
Flow-cat	Concatena fluxos de diversos roteadores num só arquivo
Flow-dscan	Detecta varredura de rede, utilizado para checar a segurança
Flow-expire	Remove arquivos de fluxos antigos
Flow-export	Exporta os arquivos de fluxos para outros formatos (ex. Cflowd)
Flow-gen	Gera fluxo de teste
Flow-import	Importa dados de outros formatos
Flow-print	Imprime os fluxos no formato texto
Flow-send	Transmite fluxos utilizando o protocolo do Netflow
Flow-stat	Geração de relatórios dos dados dos arquivos de fluxos

3. Visualização de dados hierárquicos

Os dados gerados pelos fluxos identificados em ferramentas de medição, como o Netflow, possuem características que permitem que sejam agrupados de forma hierárquica. Como exemplo, podemos agrupar o tráfego total gerado pelos serviços nas sub-redes de um PoP (ponto de presença), descrito na Tabela 2, em uma estrutura hierárquica visual que demonstra a sua distribuição (Figura 3).

Esta representação visual é feita através de árvores que usam linhas para estabelecer a conexão entre os nós pais e nós filhos de uma hierarquia. Ela apresenta duas grandes desvantagens: (1) uma grande porção do espaço visual disponível é gasto na organização dos nós; e (2) estruturas hierárquicas geram grandes árvores de difícil visualização [17].

Tabela 2. Fluxos em um backbone

PoP	Rede	Serviço	Fluxo (MB)
PoP1	10.0.1.0/24	http	215
PoP1	10.0.1.0/24	ftp	77
PoP1	10.0.1.0/24	Smtp	23
PoP1	10.0.2.0/24	http	317
PoP1	10.0.2.0/24	ftp	83
PoP1	10.0.2.0/24	Smtp	39
PoP2	...	...	...

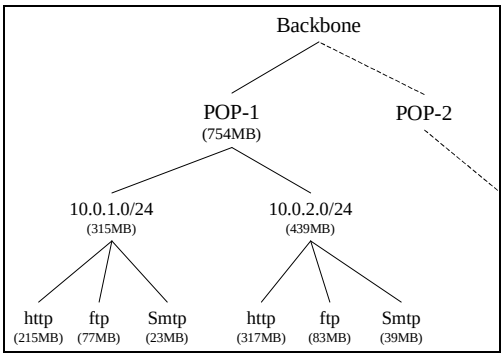


Figura 3. Representação dos fluxos de forma hierárquica.

Shneiderman propôs um método alternativo para visualização de informações estruturadas de forma hierárquica chamado de "Mapa em Árvore" [18]. Este método utiliza 100% do espaço disponível para visualização das informações, mapeando a hierarquia em regiões retangulares, como mostrado na Figura 4.

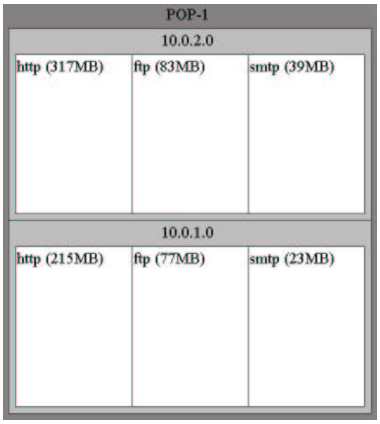


Figura 4. Um mapa em árvore para a Figura 3

Mapas em Árvore é um método de visualização de preenchimento de espaço utilizado em estruturas hierárquicas. Seu principal ponto forte é conseguir mostrar de forma eficiente grandes hierarquias, que podem chegar a centenas de milhares de itens [16]. Ele é também bastante eficiente em mostrar os atributos dos nós a partir da codificação de tamanho e cores. O atributo visual "tamanho" é especialmente útil na representação de variáveis que podem ser decompostas hierarquicamente. Como mostrado na Figura 5, ele pode ser usado para fazer com que os nós que contenham informações de maior importância sejam colocados em regiões maiores que aqueles de menor importância. Isto permite aos usuários comparar os tamanhos dos nós e das sub-árvores, ajudando a mostrar padrões hierárquicos incomuns.

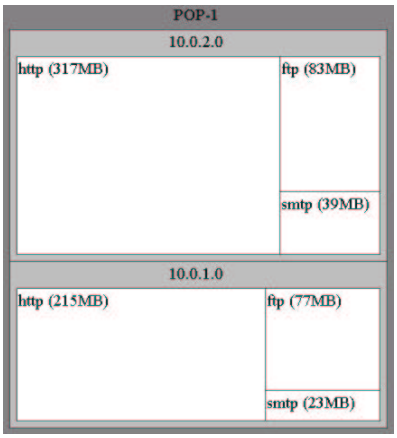


Figura 5. Um mapa em árvore com retângulos de tamanho variado

A Figura 4 e a Figura 5 estão representando a mesma estrutura hierárquica. Suas diferenças se devem ao uso, no segundo caso, do atributo visual "tamanho". Outros atributos podem ser usados para a criação de muitas variantes na aparência visual dos mapas em árvores (ex., cor, altura dos retângulos em 3D, brilho, taxa em que um retângulo pisca, etc.). Isto permite que diversas variáveis (além da estrutura hierárquica) possam ser codificadas numa única cena visual.

4. Protótipo do ambiente

4.1. Descrição do ambiente de testes

O ambiente de testes foi iniciado com a utilização do Netflow, para identificação dos fluxos, no PoP-Ba da Rede Nacional de Ensino e Pesquisa (RNP) entre os dias 10 e 17 de novembro de 2002, com a sua configuração na principal interface de entrada do tráfego do roteador (cisco série 7500). Na configuração realizada, os fluxos foram enviados para um servidor instalado no Nuperc / UNIFACS através de um link Gigabit Ethernet, conforme apresentado na Figura 6. O servidor, da marca Gateway modelo 8400 server, possui 4 processadores Pentium III, 2Gb de memória e 7 discos SCSI de 36Gb e o sistema operacional Linux RedHat 7.3 (kernel 2.4.18-3). Para a coleta dos fluxos, foi utilizado o pacote flow-tools versão 0.62.

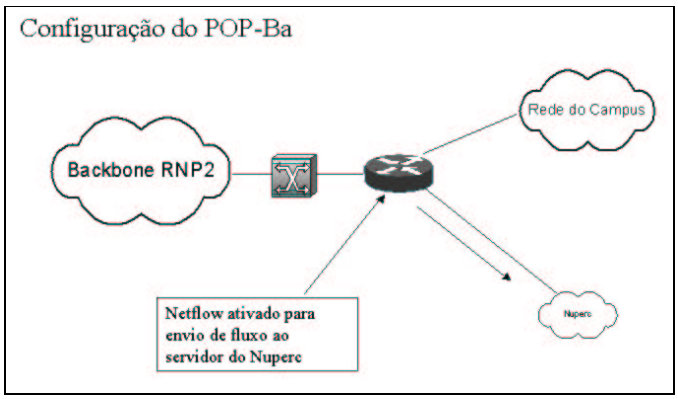


Figura 6. Configuração do Netflow no PoP-Ba da RNP

Para análise dos dados gerados pelo ambiente proposto foi utilizado um aplicativo protótipo que utiliza uma interface de exploração visual [14]. Este aplicativo utiliza o conceito de *Consultas Dinâmicas* [15], utilizados para interação em tempo real, e um método de representação visual dos dados baseado em mapas em árvore, explicado na seção 3, criando um ambiente sofisticado para se explorar e comparar dados hierárquicos.

Através deste ambiente é possível realizar uma análise dinâmica dos fluxos na medida em que podem ser aplicados filtros em diversas variáveis do conjunto estudado, bem como mudança de cores, trocas de hierarquias e isolamento de uma única variável de análise.

4.2. Experimento 1: Utilização da Rede por Serviço e Sub-rede

O objetivo desse experimento é mostrar como a combinação das técnicas de coleta e visualização apresentadas pode facilitar o entendimento das características do tráfego e a sua distribuição pelas suas sub-redes ao longo do tempo.

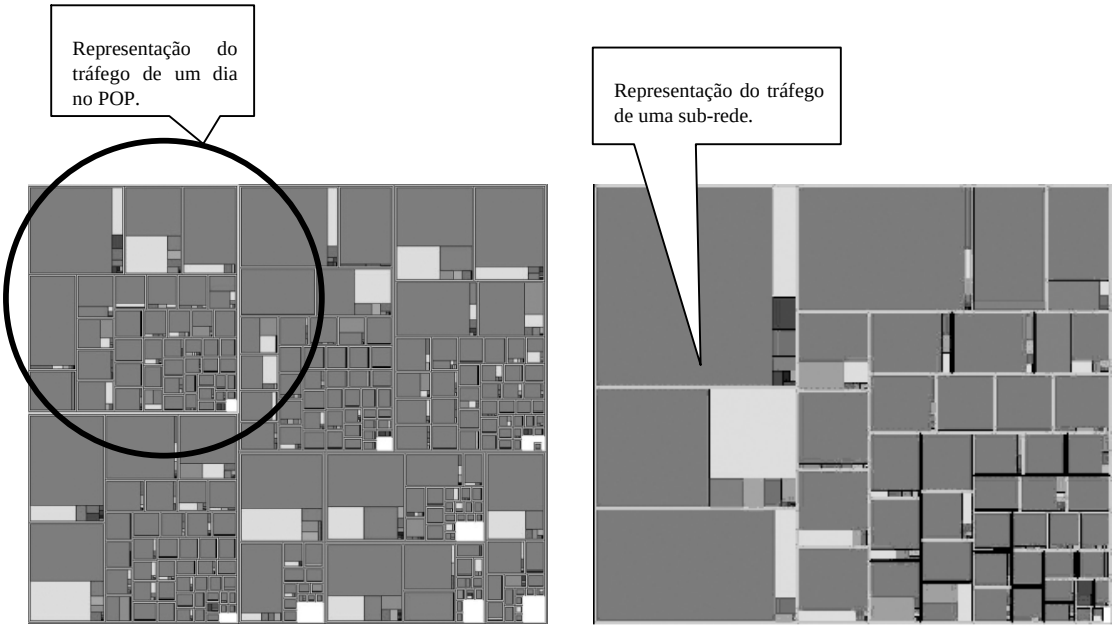
A fim de diminuir o volume de dados e fazer uma análise por sub-redes foram criados agregados de fluxos baseados no VLSM (*Variable-length subnet mask*) /24 dos IPs e contabilizados em número de fluxos e bytes, e foram consideradas apenas as portas TCP mais conhecidas.

Neste experimento foram utilizados os atributos tipo de serviço, sub-rede, tráfego total e dia, que representam um item de informação indicado por apenas um retângulo na Figura 7. A partir desses atributos é possível definir diversas hierarquias de acordo com a necessidade de análise.

No exemplo mostrado na Figura 7 (a), foi definida a hierarquia “Data->Sub-rede” onde toda a cena visual representa o tráfego do PoP, cada grupo de retângulos circunscritos pelas bordas mais externas representa um dia do experimento (1º nível da hierarquia), cada grupo possui sub-grupos de retângulos que representam as sub-redes (2º nível da hierarquia), as cores representam os serviços e o tamanho de cada retângulo representa o volume de tráfego gerado em bytes. Desta forma, 4 variáveis estão sendo avaliadas, bem como, as suas relações entre si.

Com esse tipo de representação é possível verificar a distribuição de todo o tráfego nas sub-redes durante a semana do experimento. Nesta cena visual, Figura 7 (a), podemos identificar facilmente os dias de menor uso da rede (sábado e domingo), representados pelos grupos menores (do 1º nível). Na mesma cena, as cores identificam a predominância do serviço de http, e os tamanhos dos sub-grupos (2º nível) representam o tráfego das sub-redes.

Através da utilização de funções que permitem a obtenção de detalhes sob demanda (como zoom e dicas textuais), pode-se analisar mais detalhadamente cada parte da cena visual. Como pode ser observado na Figura (b), foi feita a análise de um único dia no qual foi possível verificar a distribuição do tráfego pelas sub-redes em maiores detalhes.



a b

Figura 7. Visualização dos serviços ao longo de oito dias através das sub-redes (a) e apenas 1 dia (b).

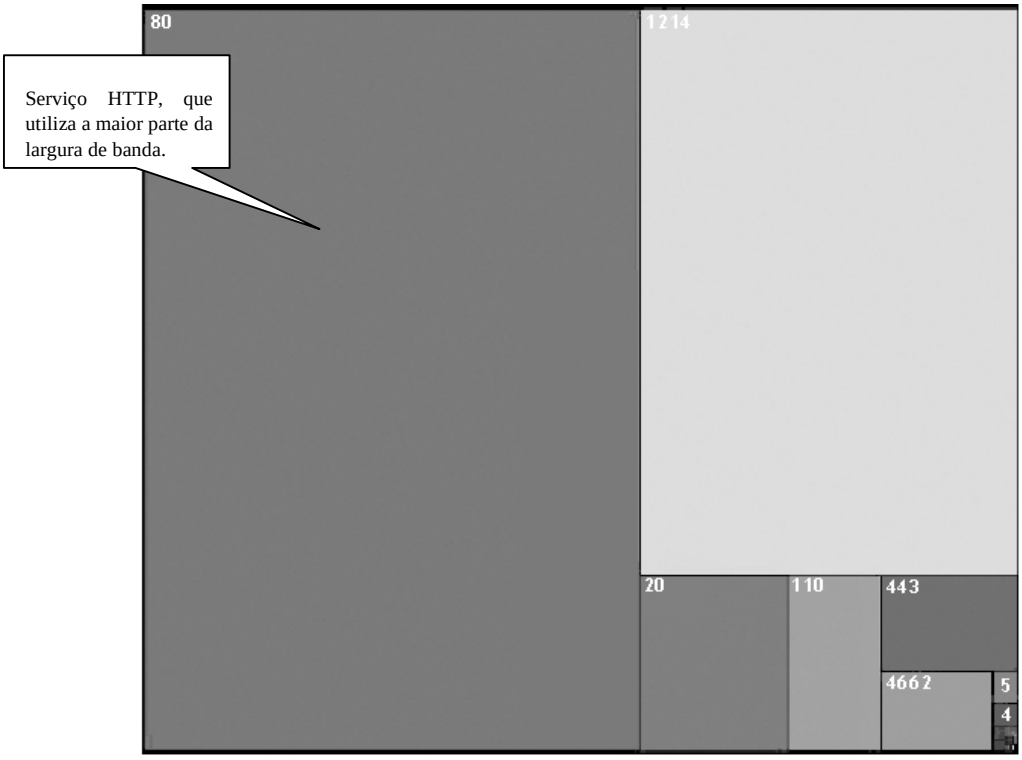


Figura 8. Visualização dos serviços de uma sub-rede.

Além da visualização de um dia, pode-se também ser visualizada uma sub-rede com maiores detalhes. No exemplo da

Figura 8, percebe-se que a maior parte do tráfego, na sub-rede analisada, foi de http (porta 80), seguida pelo serviço de compartilhamento de arquivos Kazaa (porta 1214).

Da mesma forma que o tráfego do PoP pode ser representado numa única cena visual, o mesmo pode ser feito com o tráfego de todo um backbone. Neste caso, seria adicionado um nível na hierarquia, onde o primeiro nível representaria um PoP e toda a cena visual o *backbone*.

Este experimento mostra que nas situações em que o tráfego estiver sendo distribuído incorretamente na rede, o ambiente de gerenciamento proposto vai facilitar a identificação da origem do problema e o redimensionamento da rede. Além disto, com a utilização de filtros, também vai ser possível à identificação dos serviços não conhecidos que estiverem consumindo banda acima do normal.

4.3. Experimento 2: Identificação de Anomalias

Este segundo experimento está voltado para a identificação das anomalias que ocorrem na rede que ajudam na detecção de uso indevido e de tentativa de ataques às máquinas. Para estes testes foram considerados apenas os dados de um dia de medições. Antes do detalhamento dos testes é preciso abordar alguns conceitos básicos sobre tentativas de varreduras em redes.

Uma tentativa de varredura de portas em redes se caracteriza quando ocorrem tentativas de conexão de um IP de origem para vários IPs de destinos na mesma porta ou um IP de origem para o mesmo IP de destino em portas diferentes. Quando um invasor faz tentativas de ataques deste tipo geralmente são utilizadas ferramentas que geram um conjunto volumoso de conexões que enviam muitos pacotes pequenos e isto faz com que existam diversos fluxos. Com isso, chega-se à conclusão que se existem muitos fluxos com pacotes pequenos partindo de uma mesma origem pode ser um indicador de problemas de segurança.

A fim de dar um maior direcionamento à aplicabilidade deste ambiente na identificação de falhas de segurança, foram selecionados os registros de fluxos que tivessem como destino à porta TCP 25 de qualquer máquina da rede. A escolha desses fluxos deveu-se ao fato de o serviço de SMTP ser um dos mais procurados pelos invasores de rede em busca de falhas de segurança. O total de registros selecionados foi 12.360.

Para auxiliar a identificação destes fluxos foi criado um campo nos registros dos fluxos que faz a relação entre fluxos e quantidade de bytes. Através desta relação são identificadas as anomalias da seguinte forma: Quanto mais se aproximar do valor 1 (que significa 1 fluxo para cada byte) significa que mais pacotes pequenos foram enviados, quanto mais se aproxima de zero (1 fluxo para diversos bytes) significa mais possibilidade de ser uma conexão normal.

Para visualização foi atribuída a variável cor à relação mencionada acima. Para a formação da hierarquia foi considerada a formação “IP-Origem -> IP-Destino”. Desta forma, os retângulos maiores representam que um IP de origem foi utilizado para muitas

conexões e a tonalidade mais escura representa muitos fluxos com pacotes pequenos. Com isso já é possível ter dois indicadores de problemas numa única cena visual de toda a rede, conforme pode ser observado na Figura 9.

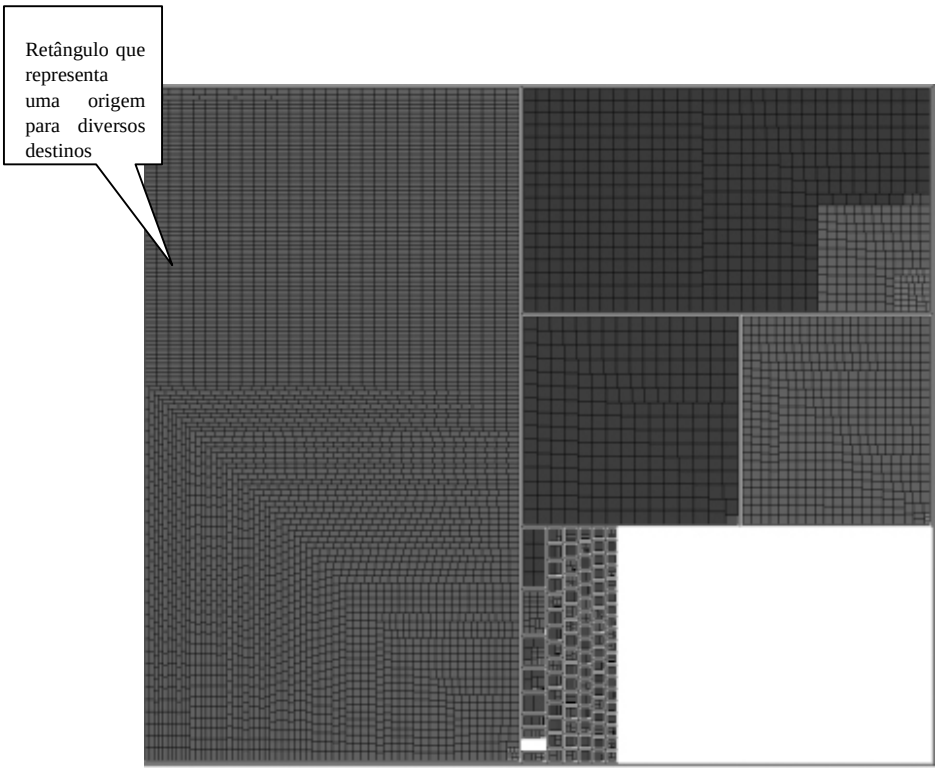


Figura 9. Visualização dos fluxos com porta 25 de destino.

Na Figura 9 pode-se perceber que houve cinco IPs de origem, representados pelos retângulos maiores, que realizaram num número excessivo de conexões para diversos IPs de destino da rede estudada, representados pelos sub-grupos de cada grupo. As cores em tonalidade mais escura mostram que foram enviados muitos pacotes com as mesmas características dos pacotes gerados pelas ferramentas de varreduras de portas. O quadro branco representa a parte da rede em que teve um comportamento normal (com tonalidade mais clara e que foram agrupados para facilitar o entendimento). Conforme demonstrado no experimento 1, é possível obter uma visão ainda mais detalhada dos fluxos desejados.

Com a utilização deste ambiente para identificação de anomalias, pode-se ter mecanismos automáticos de gerenciamento de falhas bem como um acompanhamento da rede com um todo.

5. Conclusão e Trabalhos Futuros

A complexidade das redes vem aumentando a cada dia, dificultando cada vez mais a tarefa da engenharia de tráfego para planejar as redes tendo em vista fornecer QoS para os usuários. Somente com as ferramentas de medições é possível se ter um perfil da rede

e realizar um planejamento da sua capacidade. Dentro das ferramentas de medição, destacam-se as de medição por fluxo de tráfego que possibilitam, dentre outras coisas, medir a distribuição do tráfego e seus serviços. Os fluxos identificados por essas ferramentas podem ser organizados hierarquicamente e com isso são adequados à utilização da técnica de mapas em árvores, facilitando o gerenciamento dos dados.

Neste trabalho foi proposto um ambiente de medições por fluxo de tráfego com o auxílio da utilização do método de visualização Mapas em Árvore, tendo em vista a obtenção de uma melhor caracterização do tráfego das redes IP e dando mais uma contribuição em torno do esforço de se obter um gerenciamento efetivo do desempenho das redes IP.

Os resultados obtidos com a implantação do protótipo mostram que com o uso deste ambiente é possível se ter todo o perfil de uma rede através de uma única cena visual. Sendo possível, de acordo com a necessidade, verificar uma rede com maiores detalhes. Nos experimentos realizados, por exemplo, foi possível verificar as condições de uma rede em função dos serviços mais conhecidos, volume de tráfego, dia e as sub-redes, além de ajudar a identificar as anomalias que podem representar tentativas de invasão na rede.

Como trabalhos futuros, tem-se a idéia de identificar e incluir mais fluxos neste ambiente e verificar as informações que podem ser extraídas tendo em vista uma melhor caracterização do tráfego. Também é de interesse fazer mais testes direcionados para a área de segurança, onde é plenamente possível chegar a diversas conclusões de uso indevido da rede. Além disso, pode-se fazer um ambiente de coleta e visualização em tempo real e disponibilizar através da *web* para consultas dinâmicas. Por fim, a realização de testes com outras técnicas de visualização que se adeqüem aos dados de fluxos gerados pelas ferramentas de medições utilizadas neste trabalho bem como outras similares de forma que se obtenha um ambiente de gerenciamento eficiente.

Agradecimentos: Agradecemos todo o apoio que a RNP vem dando ao GT-QoS com o fornecimento da infra-estrutura técnica necessária para a realização dos experimentos apresentados neste trabalho.

6. Referências

[1]Brownlee, N., Mills, C., and Ruth, G., Traffic Flow Measurement: Architecture, RFC 2722, IETF, October 1999.

[2]RTFM. Real-time Traffic Flow Monitoring.

http://www.auckland.ac.nz/net/Internet/rtfm/

[3]NeTraMet website, http://www.auckland.ac.nz/net/NeTraMet/

[4]Oetiker, T., MRTG – Multi-Router Traffic Grapher. http://www.mrtg.org

[5]Flowscan, http://www.caida.org/tools/utilities/flowscan/

[6]Cisco Systems. NetFlow Services and Applications. http://www.cisco.com/warp/public/732/Tech/netflow/, 1999.

[7]Flow-tools, http://www.splintered.net/sw/flow-tools/

[8]Shneiderman, B., Dynamic Queries for Visual Information Seeking. IEEE Software. Los Alamitos, v. 6, n. 11, p. 70-77, Novembro.

[9]Tufte, E., The visual display of Quantitative Information. Graphics Press.

[10]NLANR. AMP – Active Measurement Project. http://watt.nlanr.net/

[11]RIPE, TTM – Test Traffic Measurements, http://www.ripe.net/test-traffic/

[12]Surveyor Project. http://www.advanced.org/surveyor/

[13]CAIDA. CoralReef. http://www.caida.org/tools/measurement/coralreef/, November 2001

[14]Mendonça, M. e Almeida, M. (2001) Uso de Interfaces Abundantes em Informação para Exploração Visual de Dados. In: IHC, 2001, Florianópolis – IV Workshop sobre Fatores Humanos em Sistemas Computacionais. p.256-268.

[15]Shneiderman, B. (1994) Dynamic Queries for Visual Information Seeking. IEEE Software. Los Alamitos, v. 6, n. 11, p. 70-77, Novembro.

[16]Fekete, J. e Plaisant, C. (2001) Interactive Information Visualization to the Million. [on line] http://www.cs.umd.edu/hcil/VisuMillion/million-viz.pdf.

[17]Babaria, K. (2001) Introduction to Treemap. University of Maryland. [on line] http://www.cs.umd.edu/hcil/treemap3/TreemapIntroduction.pdf.

[18]Shneiderman, B. Tree visualization with tree-maps: 2-d space-filling approach. ACM Transactions on Graphics, v. 11 , n. 1, p. 92-99, Jan. 1992.