# Arquitetura de uma Ferramenta e Técnicas de Visualização para Medições sobre Tráfego SNMP

**Ewerton Monteiro Salvador, Lisandro Zambenedetti Granville**

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre, RS – Brasil

{emsalvador, granville}@inf.ufrgs.br

***Abstract.*** *In march 2006 the IRTF proposed an approach for the measurement of SNMP traffic. However, this approach has some limitations, such as: absence of data visualization techniques and lack of integration among the necessary tools for supporting the approach. This paper proposes an architecture for a Web-based tool that automates, in an integrated fashion, the execution of the IRTF approach's steps. Visualization techniques have been also developed in order to properly present the results of the analyses of SNMP traffics. An implementation of this architecture, named Management Traffic Analyzer, has been used for studying SNMP traffic samples from the Brazilian National Education and Research Network (RNP).*

***Resumo.*** *Em março de 2006 o IRTF propôs uma metodologia para medição de tráfego SNMP. Contudo, essa metodologia possui algumas limitações, tais como: ausência de técnicas para visualização de dados e falta de integração entre as ferramentas necessárias para a execução da metodologia. Este artigo apresenta uma proposta de arquitetura para uma ferramenta Web que automatiza, de forma integrada, a execução das etapas da metodologia do IRTF. Também foram desenvolvidas técnicas de visualização para os resultados gerados a partir de análises de tráfegos SNMP. Uma implementação dessa arquitetura, denominada Management Traffic Analyzer, foi utilizada para o estudo de amostras de tráfego SNMP da Rede Nacional de Ensino e Pesquisa (RNP).*

## 1. Introdução

O *Simple Network Management Protocol* [Case et al. 1990] (SNMP) foi proposto há mais de 15 anos, e atualmente é tido como o protocolo padrão *de facto* para o gerenciamento de redes TCP/IP. Apesar de ser amplamente utilizado, muito pouco se sabe de fato sobre os padrões de uso desse protocolo nas redes em produção.

Em março de 2006, o *Network Management Research Group* (NMRG), pertencente ao *Internet Research Task Force* (IRTF), publicou um documento no formato *internet draft* intitulado "*SNMP Traffic Measurements*" [Schoenwaelder 2006], o qual propunha uma metodologia sistemática para medições e geração de estatísticas sobre o uso do SNMP. O objetivo dessa metodologia é identificar padrões de utilização do SNMP a fim de poder se descobrir características deste protocolo que atualmente ainda não são efetivamente conhecidas. Algumas das questões que estão sendo investigadas neste contexto são, por exemplo: quais recursos do protocolo (versões, operações, MIBs, etc.) estão sendo utilizados, como o uso do SNMP difere nos vários tipos existentes de redes de

computadores e organizações, quais informações são mais freqüentemente requisitadas e quais são as interações mais típicas que estão sendo empregadas utilizando o protocolo [Schoenwaelder et al. 2007].

Apesar da metodologia proposta pelo IRTF ser de grande relevância para a área de gerenciamento de redes, a mesma ainda possui algumas limitações. Os estudos sobre o SNMP baseados nessa metodologia certamente irão gerar uma grande quantidade de novos dados sobre esse protocolo. Essa nova massa de dados também precisará ser interpretada pelas pessoas que estiverem conduzindo o estudo, de forma a responder às questões que ainda se encontram em aberto sobre o SNMP. Uma forma de aumentar a eficiência desse processo de interpretação dos dados é a utilização de técnicas de visualização de informação, as quais permitem que pessoas obtenham *insights* sobre os dados que estão sendo analisados (e.g., detecção de padrões, descoberta de características interessantes, etc.) de uma forma mais rápida e natural, graças às capacidades únicas do sistema visual humano. Contudo, nenhuma técnica de visualização de informação é descrita pela metodologia original apresentada pelo NMRG.

Outra característica da metodologia original do IRTF é a necessidade de se empregar um conjunto de ferramentas específicas para certas fases do estudo sobre o tráfego SNMP, o que dificulta a utilização da metodologia em si. O desenvolvimento de um framework que possa integrar todos esses softwares numa única ferramenta é algo bastante desejável, uma vez que simplificaria consideravelmente a execução desse tipo de estudo. Por fim, também não é fornecida pela metodologia do IRTF nenhuma forma de se comparar os resultados de análises realizadas sobre dois ou mais tráfegos distintos. Essas comparações teriam por objetivo apresentar, para a pessoa que está realizando o estudo, as variações de uma amostra de tráfego SNMP com relação à outra amostra, permitindo se identificar as diferenças entre as possíveis estratégias de gerenciamento que podem ser empregadas na administração de uma rede.

Neste artigo propomos algumas soluções para essas deficiências da metodologia do IRTF através do desenvolvimento da arquitetura de uma ferramenta Web para automatizar, de forma integrada, a execução das etapas da abordagem. As principais contribuições deste trabalho são: especificação de uma nova arquitetura, baseada em tecnologias Web, voltada à investigação sobre tráfego SNMP segundo as definições do IRTF; desenvolvimento de técnicas de visualização de informação específicas para o contexto onde está inserido o SNMP; e apresentação dos primeiros resultados acerca das investigações sobre o tráfego SNMP da Rede Nacional de Ensino e Pesquisa (RNP). O restante deste artigo está organizado da seguinte maneira. A seção 2 apresenta os trabalhos que estão relacionados com este artigo. A seção 3 apresenta os principais conceitos relacionados à área de investigação de tráfego de gerenciamento, enquanto que a seção 4 apresenta a arquitetura de uma ferramenta Web para automatizar a execução da metodologia do IRTF. A seção 5 descreve as técnicas de visualização desenvolvidas para serem utilizadas em conjunto com a metodologia proposta pelo IRTF. Os primeiros resultados das análises de um tráfego SNMP da RNP são apresentados na seção 6. Por fim, a seção 7 apresenta conclusões e trabalhos futuros.

## 2. Trabalhos Relacionados

Ainda são poucos os trabalhos que tratam da investigação de tráfego de gerenciamento nas redes em produção. Um desses trabalhos é o de Schönwälder *et al.* [Schoenwaelder et al. 2007], que apresenta os primeiros resultados sobre o uso do SNMP nas redes em produção. Nele são publicadas informações obtidas através da aplicação direta da metodologia do IRTF sobre diversas amostras de tráfego SNMP. Contudo, o estudo descrito pelo trabalho de Schönwälder ainda está em andamento, e os resultados apresentados são apenas preliminares.

Os trabalhos sobre técnicas de visualização de dados aplicados à área de gerenciamento de redes também são escassos. De acordo com o conhecimento dos autores deste artigo, o trabalho que mais se aproxima dos objetivos desta pesquisa é o artigo de Seong Jin Ahn *et al.* [Ahn et al. 1999]. O objetivo do trabalho de Seong Jin Ahn *et al.* é definir uma ferramenta Web destinada a analisar o desempenho de redes TCP/IP, através da análise dos dados gerados pela monitoração da rede, utilizando o SNMP.

Oberheide *et al.* [Oberheide et al. 2006] descreveu uma ferramenta para auxiliar a tarefa de gerenciar uma rede através de visualizações sobre *Netflow feeds*. Um dos aspectos dessa ferramenta que se assemelha à proposta dos autores deste trabalho é a preferência pelo uso de um conjunto de técnicas de visualização e ferramentas de manipulação associadas, ao invés da utilização de uma técnica de visualização única.

Conforme se pode observar, todos os trabalhos sobre visualização de dados descritos nesta seção lidam com tráfego de rede de uma forma geral, sem levar em consideração as particularidades do tráfego de gerenciamento e, mais especificamente, do SNMP. O grande problema disso é que as técnicas de visualização para tráfego de rede não específicos não levam em consideração características intrínsecas do protocolo SNMP, como versão utilizada, elementos na *varbind list* e o comportamento de operações básicas como `get-next-request` e `set-request`. Dessa forma, se faz necessária uma adaptação das técnicas de visualização de informações sobre redes de computadores para o contexto onde está inserido o protocolo SNMP.

## 3. Metodologia para Análise de Tráfego de Gerenciamento

Conforme já afirmado anteriormente, a primeira metodologia sistemática para análise de tráfego de gerenciamento foi proposta pelo IRTF em março de 2006 [Schoenwaelder 2006]. Essa metodologia é composta de etapas bem definidas e sua relativa simplicidade facilita a sua implementação. Entretanto, conforme também já foi afirmado anteriormente, a metodologia do IRTF e suas ferramentas auxiliares apresentam uma série de restrições, tais como: não especificar técnicas para a visualização dos dados obtidos, exigir o uso de um determinado conjunto de softwares e não especificar formas de comparação entre resultados de análises. A seguir, serão descritas brevemente as etapas que compõem a metodologia do IRTF para medições de tráfego SNMP.

1. **Captura do tráfego de gerenciamento** – A captura do tráfego de gerenciamento a ser analisado pode ser realizada através do uso de *sniffers* de rede convencionais, como o Wireshark;
2. **Conversão dos arquivos `pcap`** – A necessidade de se converter o arquivo de tráfego no formato `pcap` para um outro formato (XML ou CSV) vem da

constatação de que o formato `pcap` não é suficientemente legível, nem para humanos nem para máquinas. Fazer com que o arquivo de tráfego seja "legível por seres humanos" permite que um operador verifique se dados confidenciais não estão presentes nos dados analisados. Já a expressão "legível por máquinas" refere-se à facilidade com que um arquivo em um determinado formato tem de ser processado pelo computador. Um arquivo de fácil processamento permite que a análise de seus dados seja realizada de forma eficiente. Dois possíveis formatos para armazenar os tráfegos SNMP que atendem a esses pré-requisitos são XML (*eXtended Markup Language*) e CSV (*Comma Separated Values*);

3. **Filtragem dos arquivos XML/CSV** – Um dos problemas existentes em se publicar tráfegos de gerenciamento para pesquisa é o fato de que comumente são encontradas nos mesmos informações sensíveis (e.g., senhas, nomes de usuários, informações sigilosas) que não podem ser divulgadas. Devido a isso, é necessária a utilização de um meio para proteger as fontes que estejam fornecendo amostras de tráfego de gerenciamento através de uma filtragem nos dados desses tráfegos, a fim de se remover e/ou anonimizar essas informações sensíveis;
4. **Armazenamento do arquivo `pcap` e de sua representação XML/CSV** – Durante o período em que a metodologia aqui proposta estiver sendo aplicada, ou até mesmo após esse período, poderão ser descobertos problemas em algum processo realizado durante a obtenção, conversão ou análise dos dados, de forma que será necessário verificar e/ou repetir um ou mais passos da metodologia. Por causa disso, os dados originais (arquivo `pcap` "bruto" e arquivos XML/CSV filtrados) devem ser armazenados e preservados de forma a possibilitar a recuperação dessas informações numa eventual necessidade futura;
5. **Análise dos arquivos filtrados** – O último passo da metodologia consiste na análise dos arquivos filtrados, a fim de se agregar os dados do tráfego de gerenciamento contidos nesses arquivos e, a partir deles, extrair informações que ajudem a responder às questões em aberto sobre a utilização prática do SNMP. A análise dos dados se dá através da execução de programas ou *scripts* que procuram agregar os dados do tráfego de gerenciamento de forma a fornecer informações úteis, como predominâncias e/ou tendências dentro desses tráfegos (e.g., qual versão do protocolo é mais utilizada, qual a relação entre o tráfego periódico e o aperiódico e quais os objetos mais acessados).

## 4. Arquitetura de uma Ferramenta para Medições sobre Tráfegos SNMP

Conforme já foi apresentado na introdução deste artigo, a metodologia do IRTF para medições sobre tráfego SNMP possui uma série de limitações que dificultam a sua utilização e diminuem a eficiência da análise dos resultados. Com o intuito de abordar essas limitações, será apresentada nesta seção a arquitetura de uma ferramenta Web para automatizar a execução da metodologia para medições sobre tráfego SNMP. As principais contribuições provindas dessa arquitetura para os estudos sobre tráfego SNMP são as seguintes:

- Utilização de um módulo gerador de visualizações, destinado a facilitar o processo de interpretação dos resultados das análises executadas sobre tráfego SNMP;
- Eliminação da necessidade de se utilizar um conjunto de ferramentas para realizar todos os passos da metodologia do IRTF. A arquitetura supre todas as necessidades de software fundamentais para a realização das medições sobre o tráfego SNMP;

- Inclusão de um módulo voltado para comparação de resultados de análises de tráfego SNMP. A metodologia original do IRTF não especifica nenhuma forma para se comparar resultados de análises distintas.

A Figura 1 apresenta os principais componentes que formam a arquitetura.

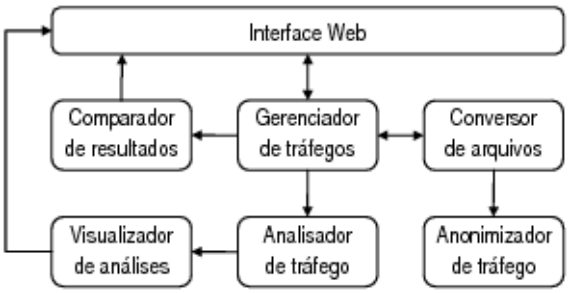


**Figura 1. Arquitetura de uma ferramenta para medições de tráfego SNMP**

O primeiro elemento que compõe a arquitetura do software é a sua **interface Web**. É somente através dela que o usuário poderá interagir com o sistema para executar operações como: criação de conta de usuário, login no sistema, inclusão de novo tráfego, análise e visualização de resultados, etc.

O **gerenciador de tráfego** é a parte da arquitetura responsável por manter registro de todos os tráfegos que o usuário submete à ferramenta Web. A entidade "tráfego", na arquitetura que está sendo desenvolvida, é a junção de um conjunto de metadados que descreve um tráfego em si (i.e., a rede onde o monitoramento foi realizado, o período em que se deu esse monitoramento, o nome de uma pessoa responsável pela administração da rede monitorada, etc.), e os arquivos que se relacionam àquele tráfego, que podem estar no formato `pcap`, XML ou CSV.

Uma vez que já existam arquivos submetidos para um determinado tráfego, o usuário terá à sua disposição uma "sub-ferramenta" – o **conversor de formato de arquivos**. Com isso o usuário poderá, por exemplo, converter um arquivo gerado a partir de uma seção de monitoramento de uma rede, originalmente no formato `pcap`, para os formatos XML ou CSV. Esse tipo de conversão é necessária para permitir que esses arquivos de tráfego possam ser analisados posteriormente, pois a ferramenta não será capaz de analisar arquivos no formato `pcap`, conforme já discutido anteriormente.

Durante o processo de conversão de um arquivo, o usuário poderá informar para a ferramenta parâmetros a serem utilizados na anonimização de informações que ele não deseja que sejam divulgadas. A parte da arquitetura responsável por tratar esses parâmetros e coordenar o processo de anonimização é chamada de **anonimizador de tráfego**.

Os parâmetros que poderão ser informados durante o processo de anonimização estão organizados na ferramenta na forma de *perfis de anonimização*. Dessa forma, primeiramente um usuário define um perfil de anonimização, especificando um nome para o mesmo e um conjunto de itens que se deseja ocultar com a utilização daquele perfil.

Após os arquivos terem sido devidamente registrados e adequadamente convertidos na ferramenta, os mesmos estarão aptos a serem analisados. A parte da arquitetura responsável por executar essa operação é o **analisador de tráfego**. Para isso, o usuário

poderá selecionar um dos tipos de análise disponíveis na ferramenta, e aplicá-la sobre os arquivos disponíveis no formato XML ou CSV. Os dados resultantes da análise são armazenados em tabelas específicas da base de dados, para serem utilizados posteriormente em visualizações ou comparações com outras análises. Ao final do processo, o sistema informa ao usuário que os dados resultantes daquela análise estão disponíveis, e apresenta ao mesmo uma lista com todas as visualizações possíveis para aquele resultado.

O módulo analisador de tráfego foi desenvolvido de forma a possuir baixo acoplamento com o restante da ferramenta, permitindo que outras análises possam ser desenvolvidas sem que sejam necessárias modificações no restante do código do sistema. Dessa forma, uma vez que novas análises tenham sido desenvolvidas, é suficiente que sejam feitas algumas poucas modificações na base de dados, como adição de linhas em tabelas ou criação de novas tabelas, para que a nova análise seja reconhecida pelo sistema.

As técnicas de visualização a serem utilizadas na ferramenta Web devem ser desenvolvidas de forma a recuperar os dados resultantes de uma análise diretamente do banco de dados, processar esses dados e exibir a visualização. O módulo da arquitetura que gerencia esse processo é denominado de **visualizador de resultados de análises**.

Uma análise na ferramenta pode ter uma ou mais técnicas de visualização associadas à mesma para que o usuário possa escolher, dentre as técnicas disponíveis, a que melhor se aplica ao seu caso. De modo análogo ao que ocorre com as análises na ferramenta, também é possível se adicionar novas visualizações. Para isso, também será suficiente a manipulação de determinadas tabelas da base de dados para que o sistema possa reconhecer e disponibilizar uma nova técnica de visualização de dados.

Por fim, o usuário terá a opção de realizar comparações entre duas ou mais análises já realizadas. Essa comparação é gerenciada pelo **comparador de resultados de análises**. Uma determinada análise sobre uma amostra de tráfego pode ser comparada com a mesma análise realizada sobre outras amostras de tráfego, pertencentes ao próprio usuário ou a outras amostras disponíveis no sistema (com o devido consentimento de seus respectivos proprietários). Também de modo análogo aos casos das análises e visualizações, também é possível se adicionar novas formas de comparação de resultados à ferramenta.

## 5. Técnicas de Visualização de Informação para os Resultados das Análises

Atualmente, tanto a academia quanto a indústria estão cada vez mais interessadas no desenvolvimento de técnicas de visualização de dados específicas para a área de gerenciamento de redes. Os trabalhos de Oberheide *et al.* [Oberheide et al. 2006] e Papadopoulos *et al.* [Papadopoulos et al. 2004] são exemplos de estudos que objetivaram o desenvolvimento de técnicas de visualização para tráfegos de redes de computadores. Entretanto, todos esses trabalhos lidam com tráfegos de redes de um modo geral, ou seja, sem levar em consideração as finalidades específicas de cada tipo de tráfego.

Os primeiros trabalhos sobre técnicas de visualizações de tráfego SNMP foram apresentados no trabalho de Salvador e Granville [Salvador and Granville 2008]. Essas técnicas também estão implementadas na ferramenta *Management Traffic Analyzer* e serão descritas brevemente nas próximas subseções.

### 5.1. Visualização da Topologia da Rede de Gerenciamento

Técnicas de visualização baseadas em grafos são amplamente utilizadas para representar determinados aspectos de uma rede de computadores, como a sua topologia [Becker et al. 1995]. Para adaptarmos essa técnica a fim de que ela possa produzir uma visualização da topologia de uma rede de gerenciamento, é necessário identificarmos no tráfego SNMP quais terminais atuam como gerentes, quais atuam como agentes, e quais atuam como ambos. Essa identificação deve ser feita através da análise dos fluxos de mensagens SNMP que compõem o tráfego. Esses fluxos são definidos como o conjunto de mensagens que partiu de uma determinada origem até um determinado destino. Além disso, os fluxos de mensagens SNMP pertencem à duas classes de relacionamento: *Command Generator* (CG) / *Command Responder* (CR) e *Notification Originator* (NO) / *Notification Receiver* (NR). O nó de origem em um relacionamento do tipo CG/CR atua como gerente e o destino atua como agente. Por outro lado, em um relacionamento do tipo NO/NR, a fonte atua como agente e o destino como gerente.

Uma vez que gerentes e agentes tenham sido identificados, esses elementos serão representados na visualização através de círculos. O tamanho dos círculos indica o papel que um determinado terminal desempenhou no tráfego estudado. Se um terminal atuou apenas como agente ao longo de todo o tráfego, ele será representado por um círculo menor. Por outro lado, se um terminal atuou como um gerente em qualquer um dos fluxos de mensagens SNMP, ele será representado por um círculo maior, mesmo que este tenha atuado como agente em algum outro fluxo de mensagens. O tamanho do círculo também dependerá do número de mensagens enviadas/recebidas que sejam características de um gerente da rede: quanto maior o número de mensagens desse tipo, maior será o tamanho do círculo na visualização. Isso indica que, quanto maior o círculo, maior é a atuação do nodo como gerente na rede representada.

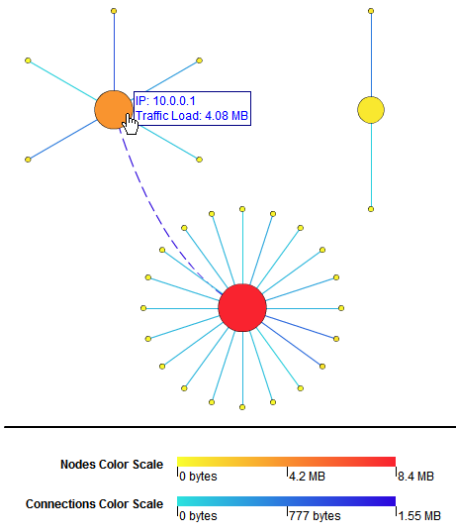


**Figura 2. Visualização da Topologia da Rede de Gerenciamento**

Uma linha sólida ligando dois nós representa uma conexão entre um nó gerente e um nó estritamente agente (i.e., que atuou como agente em todos os fluxos de mensagens do tráfego). Já uma linha tracejada representa a conexão entre um nó gerente e um nó

que está atuando naquele relacionamento específico como agente, mas que atuou também como gerente em outros fluxos de mensagens.

Tanto os nós quando as conexões possuem uma determinada cor que carrega consigo informações sobre carga do tráfego. No caso dos nós, a cor representa a quantidade de tráfego recebido por aquele determinado terminal. Por outro lado, a cor das conexões representa a quantidade de tráfego trocado entre os dois terminais conectados. Na parte inferior da visualização existem 2 barras coloridas, que são as escalas de cores utilizadas para coloris nós e conexões. Foram utilizadas escalas de cores distintas devido à diferença entre as ordens de grandeza dos tráfegos dos nós e das conexões. O resultado dessa análise pode ser observado na Figura 2.

Por fim, foram utilizados dois mecanismos de interação nessa visualização: legendas interativas para nós e conexões, e barra de rolagem. As legendas informam para o usuário algumas informações relevantes sobre nós (e.g., endereço IP e carga no nó) e conexões (e.g., tipo de relacionamento do fluxo e carga de tráfego). O usuário irá visualizar essas legendas quando posicionar o ponteiro do mouse sobre um nó ou uma conexão. Por sua vez, a barra de rolagem é o mecanismo que evita que a representação topológica seja truncada quando uma rede de grande porte estiver sendo representada.

### 5.2. Visualização de Objetos SNMP em uma *MIB Tree*

Uma das análises sobre tráfegos SNMP previstas pela metodologia do IRTF é o cálculo do número de vezes em que um determinado objeto SNMP é visto em um tráfego. Através desta análise, é possível se elaborar uma série de estatísticas sobre os objetos SNMP presentes no tráfego, como o conjunto de objetos mais acessados, os menos acessados, as MIBs (*Management Information Bases*) mais importantes, etc. Contudo, uma resposta textual desse tipo de análise possui algumas limitações. Provavelmente a principal delas é a dificuldade que um usuário teria de identificar o relacionamento hierárquico entre dois ou mais objetos, observando apenas seus nomes ou seus OIDs (Objects Identifiers). Uma vez que os objetos SNMP são organizados em uma árvore conhecida como *MIB tree*, é desejável que o resultado desse tipo de análise também apresente o conjunto de objetos encontrados no tráfego nesse tipo de estrutura. Devido a isso, foi desenvolvida uma técnica que mistura duas técnicas de visualização bastante conhecidas: visualização de árvores e histogramas. Dessa forma, o processo de análise dos resultados desse tipo de estatística se tornará mais eficiente, pois se assume que os administradores de rede estão potencialmente familiarizados com a organização de objetos SNMP em *MIB trees*.

Uma vez que a *MIB tree* contendo os objetos SNMP encontrados no tráfego tenha sido desenhada, será necessário representar o número de mensagens relacionadas com cada um dos objetos SNMP em um histograma. As barras do histograma são dese-nhadas do lado direito dos nós folhas da árvore, os quais representam os objetos SNMP. O tamanho da barra é baseado numa escala criada em tempo real, onde o valor mínimo é 0 e o máximo é o maior número de mensagens contendo um determinado objeto SNMP, dentre todos os objetos listados nos resultados da análise. Por fim, foi empregada uma barra de rolagem como mecanismo de interação para essa visualização, pois muito freqüentemente existe um grande número de objetos distintos em um tráfego SNMP. A Figura 3 mostra um exemplo dessa técnica sendo aplicada sobre um tráfego SNMP.

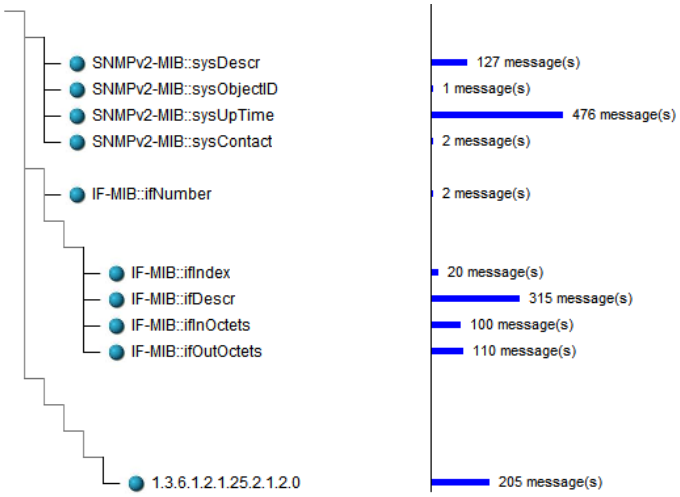


**Figura 3. Visualização de Objetos do SNMP em uma *MIB Tree***

## 5.3. Visualização da Quantidade de Mensagens SNMP em Intervalos de 1 Hora

Uma das análises disponibilizadas na ferramenta *Management Traffic Analyzer* é o cálculo da quantidade de mensagens encontradas no tráfego em intervalos de 1 hora. Esse tipo de análise é útil para se identificar o comportamento da quantidade dos diversos tipos de mensagens de gerenciamento trocadas na rede ao longo de um dia.

Os resultados desse tipo de análise são representados em uma visualização que emprega histogramas para apresentar o número de mensagens SNMP transmitidas em cada intervalo de 1 hora do tráfego analisado. Por isso, cada histograma possui 24 barras, onde cada uma dessas barras representa um intervalo de 1 hora. Por exemplo, a primeira barra do histograma representa o intervalo entre 00h00min e 00h59min. O tamanho das barras do histograma é baseado em uma escala que vai de 0 ao número máximo de mensagens encontradas em uma única hora, ao longo de todo o tráfego analisado. Além disso, cada barra é dividida em várias seções, onde cada seção possui uma cor distinta, conforme mostra a Figura 4. Existem duas formas de se seccionar as barras do histograma: por versões ou por operações do protocolo SNMP. Dessa forma, o usuário poderá identificar as versões e operações predominantes no seu tráfego, além de ter conhecimento sobre o comportamento da quantidade total de mensagens por hora.

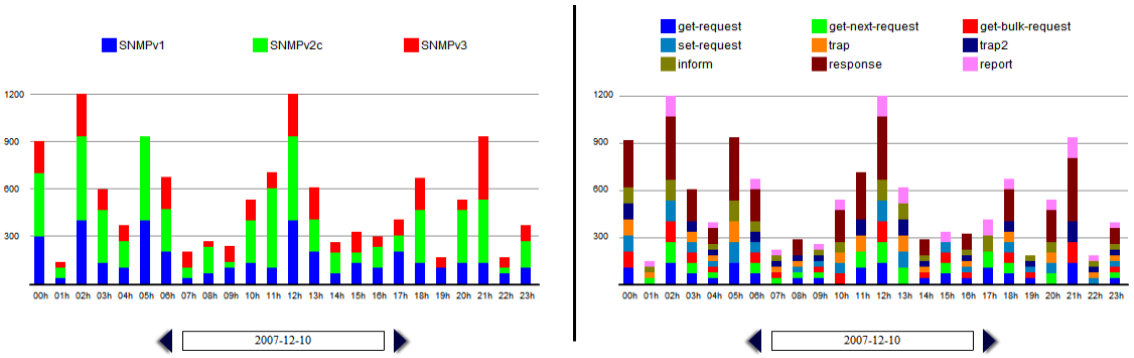


**Figura 4. Histogramas seccionados por versões e por operações do SNMP**

Um mecanismo de interação permite que o usuário saiba à qual dia o histograma

que está sendo apresentado se refere, assim como fornece a possibilidade do usuário navegar por esses dias, de modo a conhecer as quantidades de mensagens em intervalos de 1 hora referentes ao dia selecionado.

## 6. Resultados das Análises de Tráfegos SNMP

Como forma de validar as propostas deste artigo, foi implementada uma ferramenta Web de acordo com as especificações da arquitetura apresentada anteriormente. A ferramenta, chamada *Management Traffic Analyzer*, automatiza a execução da metodologia de medições sobre tráfego SNMP do IRTF, desde o processo de conversão de arquivos até as análises dos tráfegos submetidos e visualização dos resultados.

Para o desenvolvimento da mesma, foram aproveitadas as funcionalidades da ferramenta SNMPDUMP, desenvolvida em conjunto com a metodologia do IRTF para converter arquivos `pcap` para os formatos XML ou CSV e remover ou anonimizar informações sensíveis que possam estar presentes no tráfego. Dessa forma, se faz necessário que o SNMPDUMP esteja instalado no mesmo computador que irá receber a instalação do *Management Traffic Analyzer*. O núcleo da ferramenta foi desenvolvido na linguagem PHP, enquanto os scripts de análise de tráfego foram desenvolvidos em Perl, e as visualizações implementadas como aplicações Macromedia Flash através da linguagem ActionScript. Para armazenamento dos dados das análises foi utilizado o MySQL.

Já para validar as análises e visualizações implementadas no *Management Traffic Analyzer*, submetemos amostras de tráfego SNMP coletadas da Rede Nacional de Ensino e Pesquisa (RNP) à ferramenta, a fim de analisarmos os resultados gerados pela mesma. Essas amostras consistem num conjunto de 13 arquivos anonimizados, no formato CSV, com capturas de tráfegos realizadas entre os dias 22 de junho e 5 de julho de 2007.

Nas próximas subseções apresentaremos alguns dos resultados das análises sobre os tráfegos cedidos pela RNP. Foram escolhidos os resultados mais relevantes, uma vez que não seria possível a inclusão de todos os resultados devido à restrições de espaço.

### 6.1. Topologia da Rede de Gerenciamento

Ao se observar a topologia da rede de gerenciamento encontrada nos 13 arquivos de tráfego SNMP analisados, percebe-se que a mesma permanece relativamente invariável no intervalo de tempo onde esse tráfego foi monitorado. Tomando como exemplo a topologia observada no dia 22 de junho de 2007, identificamos que a rede possui um gerente principal que gerencia a maior quantidade de nós, e que também é o terminal que concentra a mais alta carga de tráfego (148,26 MB). Existe também um segundo nó que atua como um gerente menos importante da rede. A quantidade de nós conectados a esse gerente é bem menor do que a quantidade de nós conectados ao gerente principal, assim como a carga de tráfego nesse nó também é inferior (997,46 KB). Destaca-se ainda a existência de dois nós que gerenciam exclusiva e simultaneamente um único nó na rede.

A diferença mais perceptível que pode ser encontrada analisando-se os outros arquivos de tráfego SNMP da RNP é a aparição de um grupo de terminais formado por 1 nó gerente e cerca de 6 nós agentes conectados a esse gerente. Esse grupo aparece pela primeira vez no arquivo de tráfego relativo ao dia 27 de junho de 2007. A Figura 5 apresenta a visualização resultante das análises dos tráfegos da RNP relativos aos dias 22 e 27 de junho de 2007 (da esquerda para a direita, respectivamente).

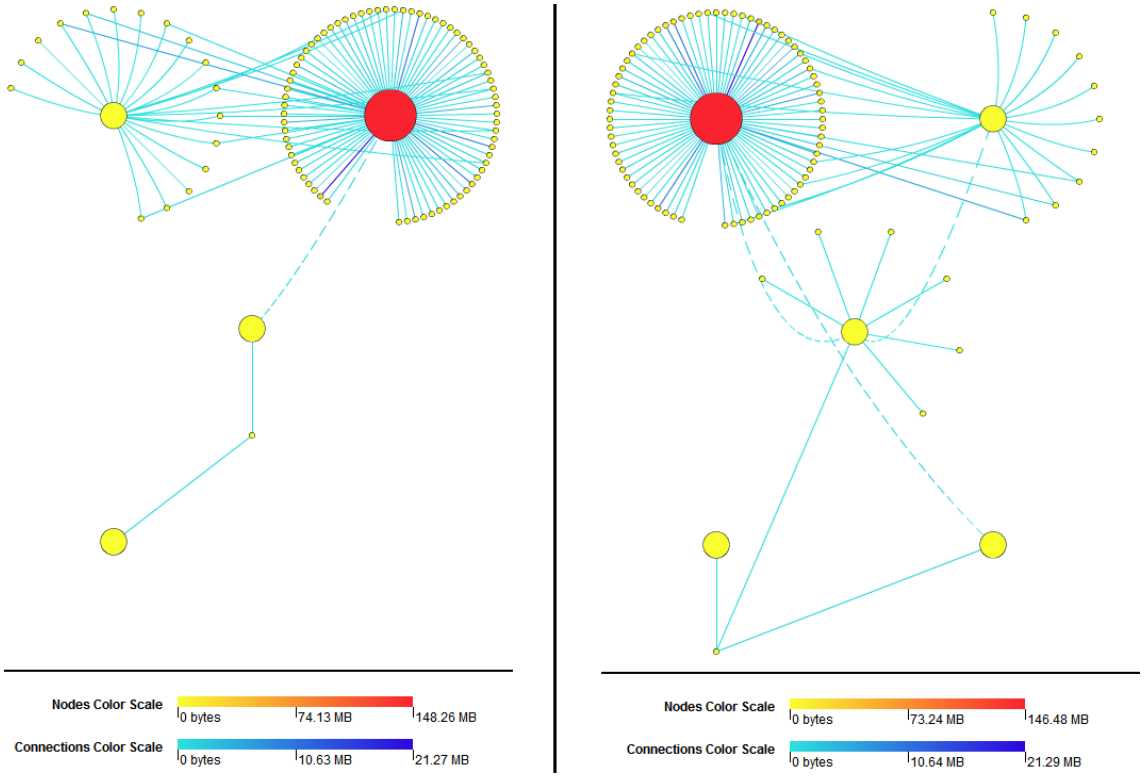


**Figura 5. Topologias da rede de gerenciamento da RNP**

Com relação às conexões representadas na topologia, percebemos que aquelas onde passa a maior quantidade de tráfego são as que conectam o principal nó gerente da rede com determinados nós agentes. A maior quantidade de tráfego registrada em uma conexão foi de 21,29 MB. No geral, cerca de 80% das conexões são do tipo CG/CR, enquanto cerca de 20% são do tipo NO/NR. Isso mostra uma preferência por parte dos administradores de rede em realizar *polling* nos dispositivos gerenciados, ao invés de utilizar notificações (*traps*).

## 6.2. Objetos SNMP Utilizados

Após a análise para identificação dos objetos SNMP encontrados nos tráfegos ter sido executada, observou-se que os objetos e a quantidade de mensagens associadas a estes são relativamente invariáveis nos arquivos de tráfego estudados. Devido a essa constância, será apresentada nesse artigo a árvore de objetos SNMP (*MIB Tree*) de apenas um dos arquivos de tráfego. Além disso, reduzimos o tamanho dessa árvore de modo a exibir apenas os 15 objetos SNMP mais representativos. O resultado dessa visualização pode ser observado na Figura 6.

A observação da árvore da Figura 6 mostra que os objetos SNMP mais utilizados são: IF-MIB::ifDescr (250.241 mensagens) e IF-MIB::ifType (245.464 mensagens). Provavelmente esses objetos são acessados para se verificar se o dispositivo consultado está operacional ou não, o que indicaria uma grande preocupação em testar o funcionamento dos dispositivos gerenciados da rede. Outros objetos que são intensivamente utilizados fornecem dados sobre o tráfego da rede. São eles: IF-MIB::ifOutUcastPkts (217.491 mensagens), ifInUcastPkts (217.479 mensagens), IF-MIB::ifHCOutOctets (203.737 men-

sagens) e IF-MIB::ifHCInOctets (203.730 mensagens). Muito provavelmente algum software de monitoramento de rede como o MRTG é o responsável pelos *pollings* feitos sobre esses objetos.

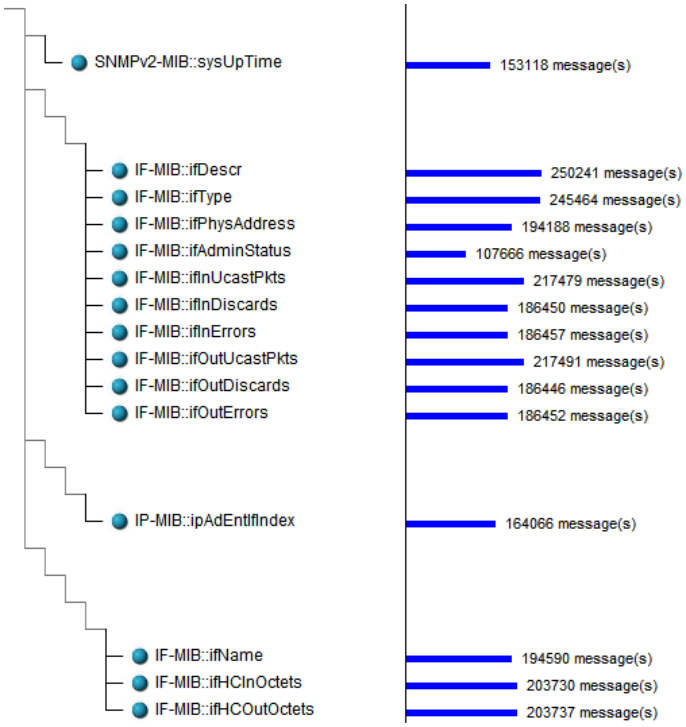


**Figura 6. Os 15 objetos SNMP mais acessados na rede da RNP**

### 6.3. Número de Mensagens SNMP por Intervalos de 1 Hora

De modo análogo à análise dos objetos SNMP presentes no tráfego (discutida na subseção anterior), a análise da distribuição da quantidade de mensagens SNMP em intervalos de 1 hora também se mostrou relativamente constante nos arquivos de tráfego estudados. Portanto, mais uma vez serão representados apenas os histogramas gerados a partir de apenas um dos arquivos fornecidos, correspondente ao monitoramento na RNP realizado no dia 28 de junho de 2007. Os histogramas resultantes dessa visualização podem ser vistos na Figura 7, seccionados por versões e por operações do protocolo SNMP (da esquerda para a direita, respectivamente).

A quantidade de mensagens é praticamente constante ao longo das horas completas em que houve monitoramento de tráfego. A última barra do histograma é menor devido à interrupção do processo de monitoração do tráfego de gerenciamento, que ocorreu em meados das 22h. O maior tráfego SNMP na rede registrado em 1 hora é de 101185 mensagens, observado às 6h do dia 28 de junho de 2007. Essa constância observada na quantidade de mensagens em todas as horas completas onde houve monitoramento mostra uma preferência dos sistemas de gerenciamento por consultas (*polling*) realizadas periodicamente nos dispositivos. Isso é confirmado também pelo grande número de mensagens do tipo *get-request*, *get-next-request* e *get-bulk-request*.

O histograma seccionado de acordo com as versões encontradas do protocolo SNMP mostram que o SNMPv2c é a versão predominante no tráfego. Em menor quantidade, encontra-se mensagens SNMPv1. Não foram encontradas mensagens SNMPv3, o

que constitui um fato interessante, pois teoricamente as versões SNMPv1 e SNMPv2c são históricas, enquanto que a versão SNMPv3 é considerada como o padrão em vigência.

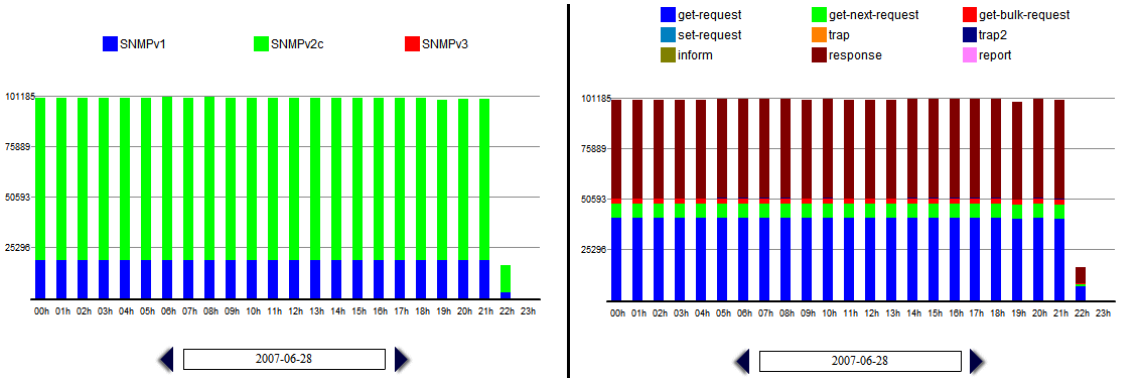


**Figura 7. Histogramas do tráfego SNMP na RNP**

Já o histograma seccionado de acordo com as operações do SNMP mostra que o tráfego é formado em sua maior parte por mensagens `response`. Em seguida aparecem as mensagens `get-request` e `get-next-request`, respectivamente. Em menor quantidade temos mensagens `get-bulk-request` e `trap2`. Mensagens de `trap` podem ser encontradas no tráfego, mas em quantidade insignificante, sendo esse o motivo de elas não serem representadas no histograma. O fato de mensagens `response` serem maioria no tráfego é justificável, pois esse tipo de mensagem sempre é emitida quando um dispositivo responde à consultas `get-request`, `get-next-request` ou `get-bulk-request`. Não foram observadas mensagens `set-request`, o que indica que o protocolo está sendo utilizado exclusivamente para monitoramento da rede, e não para configuração da mesma.

De um modo geral, podemos concluir que o tráfego SNMP da RNP é formado quase que em sua totalidade por mensagens periódicas de *polling* geradas pelos sistemas de gerenciamento utilizados na rede. O uso de notificações é raro, e praticamente não exerce influência sobre o tráfego como um todo. Por fim, o SNMP é utilizado exclusivamente para a realização do monitoramento sobre os dispositivos e serviços da rede. Muito provavelmente esse protocolo não é utilizado para configuração de dispositivos por questões de segurança.

## 7. Conclusões e Trabalhos Futuros

Atualmente, várias abordagens de gerenciamento de redes de computadores estão bem consolidadas, tais como as que empregam o protocolo SNMP, e algumas outras já se encontram em um estado avançado de desenvolvimento, como as que fazem uso de Web Services. Entretanto, a indústria e a academia ainda não conhecem de maneira satisfatória as características da utilização dessas abordagens no “mundo real”, ou seja, nas redes em produção.

Contudo, certamente existe espaço para melhorias no que diz respeito à metodologia de medições sobre o protocolo SNMP. A arquitetura de uma ferramenta Web proposta neste trabalho apresenta uma forma de integrar os vários softwares que anteriormente eram necessários para a execução dessa metodologia, acrescentar novas funcionalidade e, com isso, aumentar a acessibilidade e a eficiência desse tipo de estudo.

O emprego das três técnicas de visualização de informação propostas neste artigo tornou o trabalho de interpretação dos resultados das análises mais eficiente e eficaz. A partir dessas técnicas, o usuário da ferramenta poderá analisar os dados obtidos de forma mais natural, pois graças às características do sistema visual humano a descoberta de padrões e características interessantes se dará de forma simplificada.

Através da implementação da ferramenta *Management Traffic Analyzer*, demonstrou-se a viabilidade da implementação da arquitetura proposta. Além disso, a ferramenta implementada foi utilizada para realizar um estudo sobre arquivos de tráfego SNMP pertencentes à Rede Nacional de Ensino e Pesquisa (RNP), segundo a metodologia proposta pelo IRTF. Algumas características interessantes puderam ser confirmadas através desse estudo, tais como: preferência pela utilização de *polling* ao invés de notificações (*traps*), não utilização da versão 3 do protocolo SNMP e utilização de operações de forma predominantemente periódica.

Como trabalhos futuros, pretende-se ampliar o conjunto de técnicas de análise, visualização e comparação de tráfegos SNMP disponibilizadas na ferramenta *Management Traffic Analyzer*. Além disso, planeja-se buscar amostras de tráfegos SNMP oriundas de outras redes em produção, a fim de tornar os resultados obtidos mais representativos quanto à utilização atual do protocolo SNMP em outros contextos.

## Referências

Ahn, S. J., Yoo, S. K., and Chung, J. W. (1999). Design and Implementation of a Web-based Internet Performance Management System Using SNMP MIB-II. *International Journal of Network Management*.

Becker, R. A., Eick, S. G., and Wilks, A. R. (1995). Visualizing Network Data. *IEEE Transactions on Visualization and Computer Graphics*, 1(1):16–28.

Case, J. D., Fedor, M. L., and Schoffstal, J. D. (1990). Simple Network Management Protocol (SNMP). RFC 1157. [S.l.]: Internet Engineering Task Force, Network Working Group.

Oberheide, J., Goff, M., and Karir, M. (2006). Flamingo: Visualizing Internet Traffic. In *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, pages 150–161, Vancouver, Canada.

Papadopoulos, C., Kyriakakis, C., Sawchuk, A., and He, X. (2004). CyberSeer: 3D audio-visual immersion for network security and management. In *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 90–98, New York, NY, USA. ACM Press.

Salvador, E. M. and Granville, L. Z. (2008). An Investigation of Visualization Techniques for SNMP Traffic Traces. In *IEEE/IFIP Network Operations and Management Symposium, 2008. NOMS '08. (aceito como short-paper)*.

Schoenwaelder, J. (2006). SNMP Traffic Measurements. *Internet Draft*.

Schoenwaelder, J., Pras, A., Harvan, M., Schippers, J., and van de Meent, R. (2007). SNMP Traffic Analysis: Approaches, Tools, and First Results. *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management*.