Uma Ferramenta para Medição e Caracterização de Tráfego de Protocolos de Alto de Nível e Aplicações em Rede

Débora Pandolfi Alves, Lucio Braga, Ricardo Sanchez, Luciano Gaspary

Programa Interdisciplinar de Pós-Graduação em Computação Aplicada (PIPCA)
Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos 950 – 93022-000 – São Leopoldo – RS – Brasil

{debora,lbraga,rsanchez,paschoal}@exatas.unisinos.br

Abstract. *This paper presents a tool consisted of (i) a RMON2 agent which allows to measure and characterize high-layer protocol traffic in a network and (ii) a web-based management application, which makes possible the visualization of data obtained from the agent, in a simple and easy-to-analyze way. The tool provides the manager with conditions to identify and quantify the impact that users and/or protocols, as well as certain communications among peers, cause in the network.*

Resumo. *Este artigo apresenta uma ferramenta compreendida por (i) um agente RMON2 que permite medir e caracterizar o tráfego de protocolos de alto nível em uma rede e (ii) uma aplicação de gerenciamento, baseada na web, que torna possível a visualização de dados obtidos junto ao agente, de forma simples e de fácil análise. A ferramenta provê ao gerente condições de identificar e quantificar o impacto que usuários e/ou protocolos, bem como determinadas comunicações entre pares, causam na rede.*

1 Introdução

Os investimentos realizados na expansão e na manutenção das redes de computadores têm crescido de forma surpreendente nos últimos anos. Sua popularização acarretou o surgimento de um elevado número de aplicações distribuídas e protocolos, levando projetistas e gerentes a investigar soluções efetivas de gerenciamento que permitissem reduzir custos, prover alta disponibilidade e, pelo menos, manter a qualidade de serviço percebida anteriormente.

Num primeiro momento, estes objetivos foram alcançados através de uma imediata adesão a novas tecnologias. Um exemplo real foi a recente migração, em muitas organizações, do padrão de rede local *Ethernet* para *Fast* e *Gigabit Ethernet*. Como na maioria das vezes os usuários encaram a rede como uma fonte inesgotável, acabam incorporando mais e mais aplicações e protocolos ao seu cotidiano o que, para o gerente, acaba gerando a necessidade de constantes alterações na infra-estrutura da rede.

Essas modificações envolvem custos e, portanto, precisam ser justificadas. Isto é possível se o gerente tiver condições de responder a questões simples como: que usuários ou departamentos estão utilizando a rede? Quando ela está sendo mais utilizada? Que aplicações estão sendo executadas? Quais as atividades de um determinado usuário? Os usuários estão percebendo um nível adequado de serviço? Os recursos adquiridos estão corretamente alocados?

Respostas a essas questões podem ser obtidas com a utilização de mecanismos de contabilização. Existem várias ferramentas destinadas a esse propósito. Entre elas destacam-se `ntop`, `NetFlow` e `NeTraMet`. `ntop` é uma aplicação de gerenciamento de código aberto, baseada na *web*, destinada à medição e caracterização de tráfego de rede [Deri 2004]. Foi desenvolvida para suprir necessidades de gerenciamento não atendidas pelas ferramentas que acompanham os sistemas operacionais. Sua arquitetura exige um acoplamento da aplicação de gerenciamento e o módulo de monitoração, ou seja, se houver três pontos de medição serão necessárias três consoles de visualização. `NetFlow` [Netflow 2004] e `NeTraMet` [Netramet 2004] são ferramentas voltadas à monitoração de fluxos e, em geral, são adotadas para monitorar tráfego de borda, ou seja, o tráfego de entrada e saída da rede. A primeira constitui-se de uma tecnologia desenvolvida pela Cisco e deve ser utilizada com *software* e *hardware* fabricado pela empresa (ou compatível), tornando o gerenciamento da rede dependente dos mesmos.

Alternativamente às ferramentas recém mencionadas, há o padrão RMON2 (*Remote Network Monitoring Management Information Base version 2*) que é uma tecnologia padronizada pelo IETF para monitoração de protocolos de alto nível [Waldbusser 1997]. Uma das vantagens do emprego de RMON2 em relação às demais ferramentas mencionadas é ser padronizado, o que facilita sua adesão a plataformas baseadas em SNMP (*Simple Nework Management Protocol*) já em uso pelas organizações. Outro benefício reside na sua adequação para monitorar tanto tráfego de borda, quanto corporativo (interno). Soma-se a isso o fato de que é possível ter agentes RMON2 espalhados em vários pontos de uma rede e uma única aplicação de gerenciamento requisitando e processando, de forma integrada, os dados obtidos.

Nesse contexto, este artigo apresenta uma ferramenta para medição e caracterização de tráfego de protocolos de alto nível, baseada em RMON2, que é organizada em duas partes: o agente de monitoração e a aplicação de gerenciamento. Ao agente de monitoração RMON2 cabe a função de monitorar a rede e prover estatísticas sobre sua utilização. O formato das informações geradas pelo agente é textual. Embora possa ser compreendido pelo gerente da rede, o volume dessas informações aumenta rapidamente, dificultando cada vez mais sua interpretação. Como o tipo de informações oferecido pelo padrão RMON2 não é próprio para uso humano, torna-se conveniente o uso de uma aplicação que processe essas informações textuais e gere informações de mais fácil e rápida interpretação pelo gerente da rede. Para esse fim, foi desenvolvida a aplicação de gerência, que gera gráficos a partir de consultas a informações geradas pelo agente. Os gráficos a serem criados pela aplicação são configurados pelo gerente da rede de acordo com as suas necessidades.

O agente RMON2 age independentemente da aplicação de gerenciamento e pode ser usado com outras aplicações ou ferramentas de visualização fornecidas pela plataforma em uso na organização. Da mesma forma, a aplicação de gerenciamento pode operar consultando agentes RMON2 disponíveis em dispositivos de rede.

O artigo está organizado da seguinte forma: a seção 2 apresenta o agente RMON2 desenvolvido, abordando sua arquitetura e desempenho. A seção 3 trata da aplicação de gerenciamento. O artigo encerra na seção 4 com as considerações finais.

2 Agente RMON2

O padrão RMON2 define uma MIB (*Management Information Base*) para monitoração remota de redes, que é uma base de dados de gerenciamento que fornece informações estatísticas sobre o tráfego de protocolos de alto nível e aplicações em rede. A MIB é organizada em dez grupos [Waldbusser 1997]. O agente desenvolvido implementa seis desses grupos, os quais foram escolhidos a partir de uma pesquisa do que se pode obter da MIB RMON2 especificamente no monitoramento de aplicações e protocolos de alto-nível [Gaspary 1999]:

- *protocol directory* (`protocolDir`): composto por uma única tabela que indica todos os encapsulamentos de protocolos que o agente é capaz de interpretar;
- *protocol distribution* (`protocolDist`): fornece estatísticas sobre a quantidade de tráfego gerado por cada encapsulamento de protocolo observado pelo agente;
- *network-layer host* (`nlHost`): coleta estatísticas sobre a quantidade de tráfego de entrada e saída de acordo com o endereço do nível de rede;
- *network-layer matrix* (`nlMatrix`): provê estatísticas sobre o volume de tráfego entre pares de estações com base no endereço do nível de rede;
- *application-layer host* (`alHost`): agrega estatísticas sobre o volume de tráfego de entrada e saída das estações com base em endereços do nível de rede e encapsulamentos de protocolos de aplicação (transporte e aplicação);
- *application-layer matrix* (`alMatrix`): coleciona estatísticas sobre o volume de tráfego entre pares de estações com base no endereço do nível de rede e encapsulamentos de protocolos de aplicação (transporte e aplicação).

2.1 Arquitetura do Agente

O agente executa em estações GNU/Linux e foi desenvolvido como uma extensão do agente SNMP Net-SNMP [Net-SNMP 2004], utilizando a linguagem `C`, a biblioteca de *threads* POSIX e a biblioteca de captura de pacotes *libpcap* [Libpcap 2004]. A figura 1, a seguir, ilustra a arquitetura do agente.

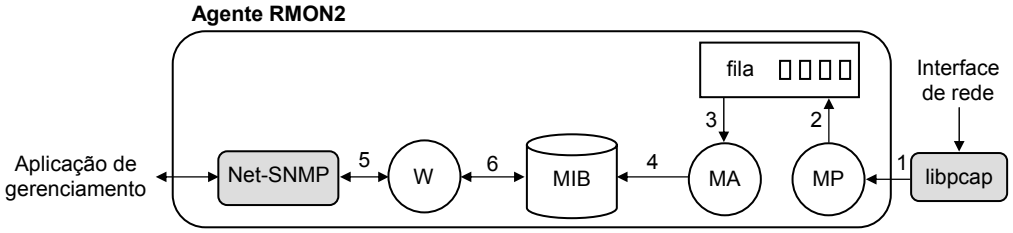


Figura 1. Organização interna do agente

O módulo de processamento (MP) é responsável por receber e analisar os pacotes capturados pela *libpcap* (fluxos 1 e 2 na figura). Apenas os pacotes cujos encapsulamentos estão registrados na tabela *protocolDir* são contabilizados; desse modo o custo de processamento de pacotes cujas informações não serão utilizadas é reduzido. As informações essenciais dos pacotes analisados (endereços de rede e portas de aplicação, por exemplo) são armazenadas em uma fila circular de tamanho fixo. A partir das informações obtidas na fila (3), o módulo de atualização (MA) atualiza as

tabelas que armazenam estatísticas que constituem a MIB RMON2 (4), implementadas usando estruturas *hash*. O módulo *wrapper* (W), por fim, possibilita ao Net-SNMP acessar os dados armazenados na MIB RMON2 (5,6).

2.2 Desempenho

Esta sub-seção apresenta o resultado de uma análise de desempenho realizada junto ao agente RMON2 visando avaliar a sua capacidade sustentada de monitoração. A estação onde o mesmo foi instalado possuía um processador Pentium 4 de 1,7GHz, 512MB de RAM, uma placa de rede 3COM 3c905C-TX/TX-M Tornado e sistema operacional GNU/Linux (Slackware Linux 8.1, *kernel* 2.4.21). O experimento de medição foi realizado na velocidade máxima de transmissão suportada pela rede (100Mbps), apenas variando-se o tamanho dos pacotes, a fim de encontrar o limite da capacidade de monitoração do agente [Sanchez 2003]. Os resultados revelaram que o nosso agente RMON2 é capaz de sustentar a taxa de monitoração de 100Mbps se os pacotes analisados forem de 212 bytes ou maiores (52.100 pacotes por segundo). Nesse cenário o uso de CPU ficou em torno de 95% (75% pelo agente e 20% pelo *kernel* Linux).

2.3 Localização do Agente na Rede

Um fator de grande importância para a monitoração adequada da rede é a localização do agente RMON2. A estação que possui o agente instalado deve ser conectada à rede através de um *hub* ou *switch*. Ao utilizar um *switch*, será necessário configurá-lo para realizar espelhamento de portas, direcionando todo o tráfego para a porta onde a estação com o agente RMON2 estiver conectado. Dessa forma, um único agente poderá fazer uma análise em tempo real do tráfego de vários segmentos de rede. Em ambientes maiores, compostos por roteadores, agentes devem ser espalhados pelas diversas subredes para que se tenha uma monitoração que possibilite obter um detalhamento do tráfego global da rede.

3 Aplicação de Gerenciamento

Obter estatísticas de um agente RMON2 apenas através de consultas SNMP é uma tarefa complicada pela grande quantidade de dados e variáveis disponíveis. Por exemplo, sem o apoio de uma aplicação, obter estatísticas sobre a quantidade de pacotes do encapsulamento *ether2.ipv4.tcp.http* que foram observados pelo agente requer que o gerente faça duas consultas a ele. A primeira, que é uma consulta à tabela *protocolDir*, tem o intuito de descobrir o índice do respectivo encapsulamento e a segunda, que consulta a tabela *protocolDist* levando em conta o índice obtido na *protocolDir*, busca obter o dado propriamente dito. Esse resultado, por sua vez, é devolvido ao gerente em formato textual (ex: “Gauge32: 74302”), e sua compreensão e interpretação em relação ao comportamento da rede estão sujeitas a atrasos e erros por parte do gerente. A fim de minimizar os erros e o tempo de análise dos dados pelo gerente, a aplicação de gerenciamento tem por objetivo consultar agentes RMON2, processar as informações obtidas e gerar gráficos.

3.1 Arquitetura da Aplicação

A arquitetura da aplicação de gerenciamento está ilustrada na figura 2, onde são destacados seus componentes e as relações entre os mesmos. Nela pode ser vista que a

interação do gerente de rede com a aplicação se dá por meio de um navegador *web*, onde o gerente acessa a aplicação disponível em um servidor *web* (Apache) com suporte a PHP (*Hypertext Preprocessor*).

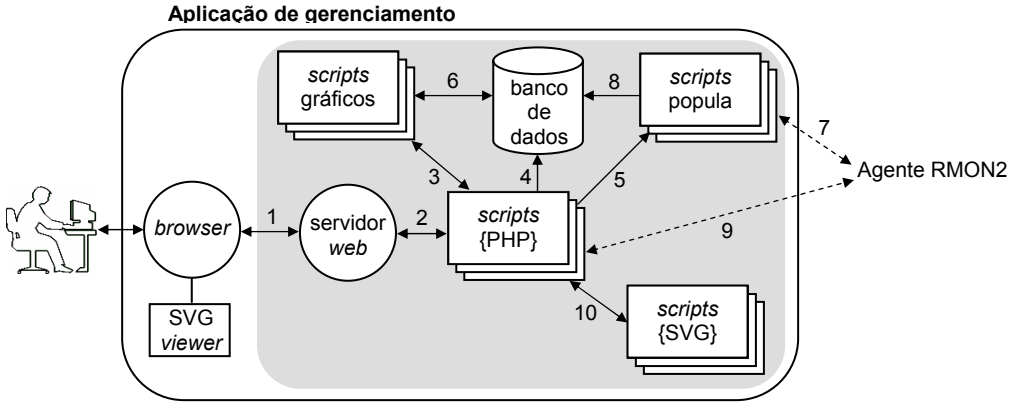


Figura 2. Estrutura da aplicação de gerenciamento

Os dados obtidos a partir dos grupos *protocolDist*, *nlHost* e *alHost* da MIB RMON2 são armazenados pelo *software* RRDtool [Oetiker 2004], que também é responsável pela criação dos gráficos. Quando a geração de um gráfico é solicitada (fluxos 1 e 2 na figura), ocorre a criação de: um *script* com a função de gerar os gráficos (3), uma base de dados contendo as variáveis que serão monitoradas (4) e um *script* (5) que realiza consultas ao agente a cada 5 minutos (7) e atualiza a base de dados (8). Para executar o *script* em intervalos de cinco minutos, utiliza-se o comando "`at`" disponível na plataforma GNU/Linux.

Para visualizar um gráfico previamente criado a partir de consultas a um dos grupos mencionados acima, um *script* PHP executa um *script* gráfico (fluxo 3) e esse, por sua vez, cria os gráficos necessários requisitando os dados à respectiva base (6).

Gráficos gerados a partir dos grupos *nlMatrix* e *alMatrix* seguem uma abordagem diferenciada. Os gráficos são criados a partir do padrão SVG (*Scalable Vector Graphics*) [Ferraiolo 2003]. Quando se solicita um gráfico desse tipo, ocorre a criação de um *script* PHP que tem a função de consultar o agente (fluxo 9) e criar o arquivo SVG (10). A consulta ao agente e a criação do arquivo SVG são realizadas apenas no momento em que o gerente requisita a visualização do gráfico.

3.2 A Aplicação em Operação

Serão apresentados nesta seção dois exemplos de criação de gráficos utilizando a aplicação de gerenciamento. O primeiro demonstra um gráfico criado a partir do grupo *protocolDist*, que informa a quantidade de octetos observados pelo agente para um grupo de aplicações durante um período de tempo. O processo de criação é compreendido por um *wizard* dividido em três etapas:

- Indicação do agente RMON2 sobre o qual deseja-se obter estatísticas e a respectiva comunidade SNMP de leitura configurada no agente;
- Seleção dos encapsulamentos de protocolo a monitorar;

- Configuração de aspectos visuais como cores que informações terão no gráfico, unidade de medida (octetos, pacotes, bits) e períodos de tempo dos gráficos (diários, semanais e/ou mensais), como ilustrado na figura 3.

Ao término da terceira etapa, o processo de criação dá-se por encerrado e o gráfico passa a estar disponível para a visualização na área destinada na barra de *menu* (vide figura 3).

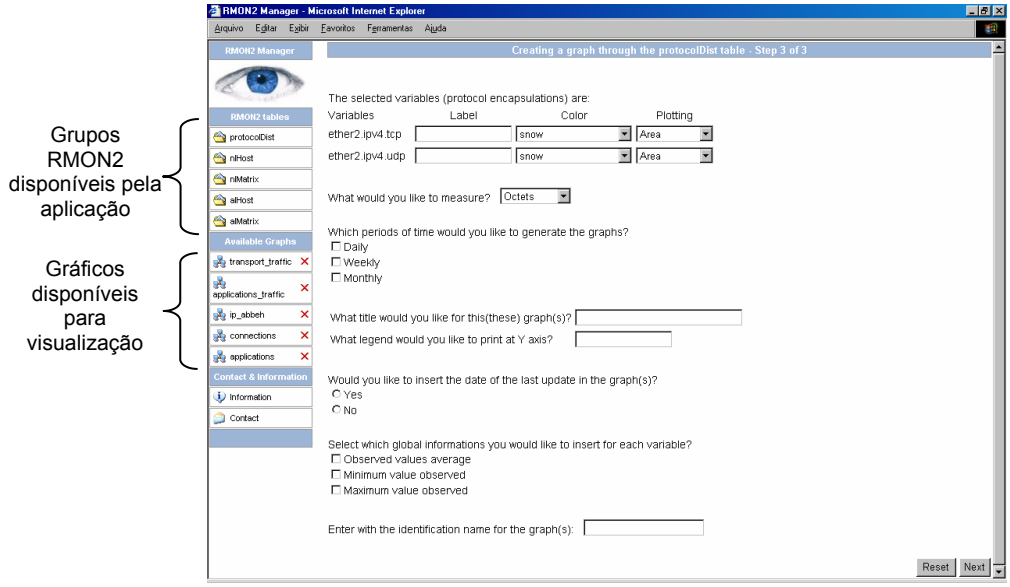


Figura 3. Aplicação no último passo de criação de gráfico para o grupo *protocolDist*

O gráfico criado a partir do primeiro exemplo pode ser visualizado na figura 4. Gráficos dessa natureza têm como característica apresentar os dados em função do tempo. No exemplo, ele ilustra o tráfego total, em octetos, dos protocolos de aplicação SSH, HTTP, SFTP, FTPS, DNS e SNMP. Embora o exemplo demonstre a criação para o grupo *protocolDist*, o processo de criação para os grupos *nlHost* e *alHost* segue o mesmo padrão; o que o diferencia é a informação monitorada.

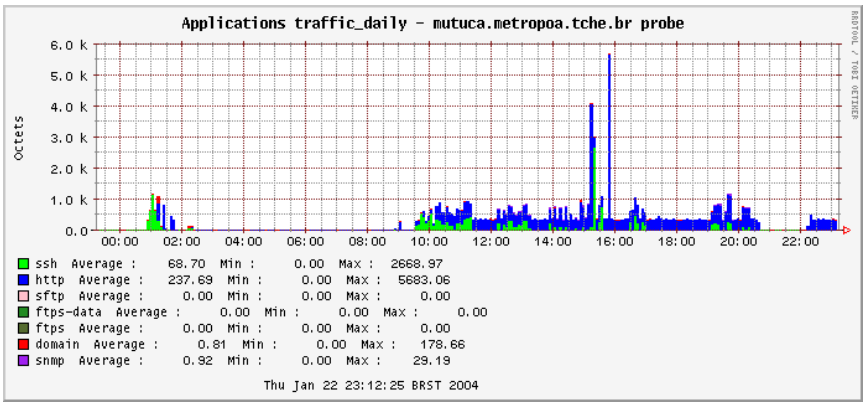


Figura 4. Tráfego diário de protocolos de aplicação

Outra funcionalidade agregada à aplicação e que pode ser utilizada para a geração de gráficos similares ao anterior é o *aberrant behavior* [Brutlag 2003]. Essa funcionalidade indica a ocorrência de algum comportamento anômalo em relação ao padrão comportamental da rede ao longo do tempo. Isso pode ser verificado através da

extrapolação do tráfego do protocolo em estudo diante de limiares que são calculados por uma média padrão do tráfego obtido do histórico. A figura 5 ilustra um exemplo de gráfico que utiliza a funcionalidade *aberrant behavior* e monitora o tráfego do protocolo *IPv4*. Observa-se que o tráfego *IPv4* está dentro dos limiares aceitáveis e portanto o seu comportamento se encontra dentro do padrão.

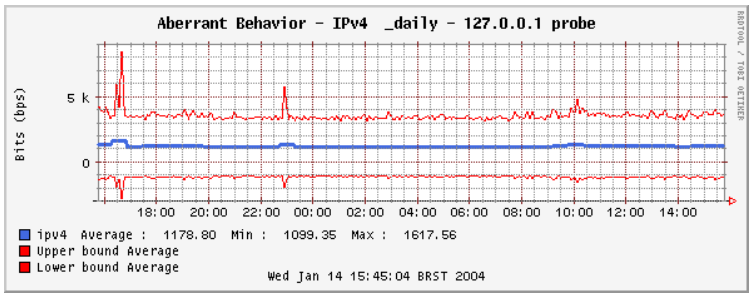
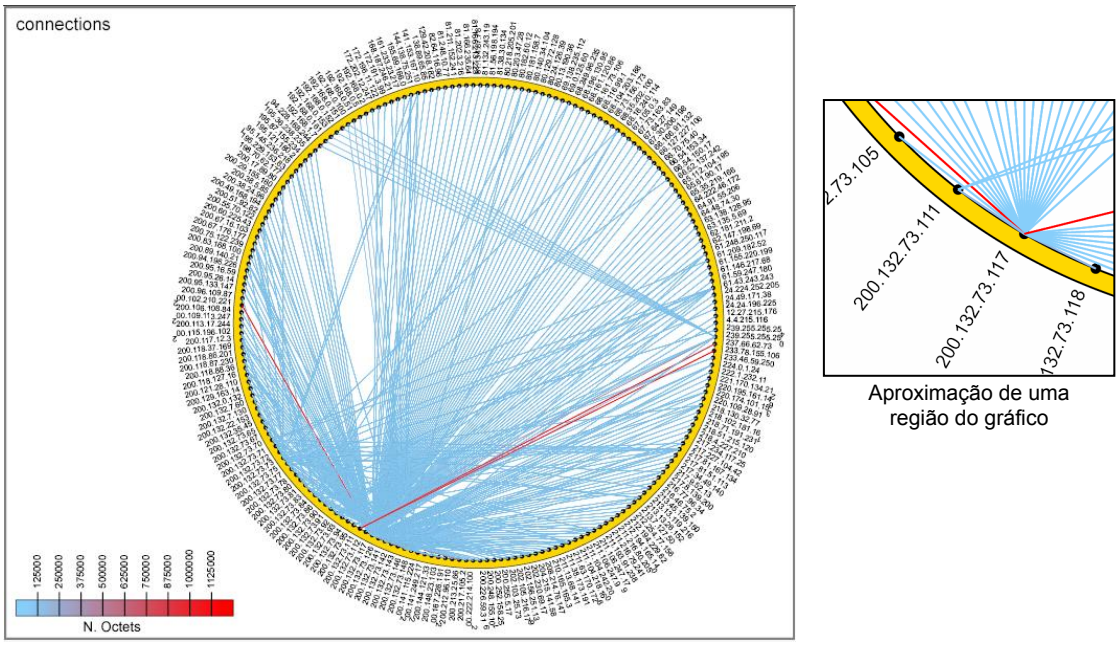


Figura 5. *Aberrant behavior* diário do protocolo ipv4

O segundo exemplo ilustra a criação de um gráfico no qual os dados são oriundos do grupo *nlMatrix*. Esse gráfico mostrará todos os pares de *host* que se comunicaram juntamente com a taxa de octetos transferida. Assim como no primeiro exemplo, o processo de criação é realizado através de um *wizard*, mas com duas etapas. A primeira etapa é a mesma do exemplo anterior. Já a segunda, requisita se o gerente deseja visualizar todas as comunicações ou apenas àquelas que apresentam pelo menos um dos *hosts* selecionados.

Um exemplo de gráfico resultante é apresentado na figura 6. Esses gráficos utilizam o formato SVG e podem receber *zoom* sem perda de qualidade ou deformações. Além disso, podem ser feitas pesquisas por determinados endereços IP.



Aproximação de uma região do gráfico

Figura 6. Comunicações observadas por um agente

4 Conclusões

Este trabalho apresentou uma ferramenta formada por um agente RMON2 e uma aplicação de gerenciamento, implementados pelo nosso grupo de pesquisa, para medição e caracterização de tráfego de protocolos de alto nível. Através da ferramenta é possível controlar atividades de usuários, traçar um perfil global de utilização da rede, otimizar a localização de usuários e recursos, entre outros. A principal contribuição desse trabalho é a disponibilização de uma implementação gratuita e de código aberto da ferramenta, o que (a) permite à comunidade usá-la como base para outras implementações e (b) torna desnecessária, em muitos casos, a aquisição de equipamentos e aplicações comerciais dedicados à monitoração. A ferramenta e o tutorial de instalação podem ser obtidos em `http://mutuca.metropoa.tche.br/`.

Referências

Brutlag J. D. (2003) "Aberrant Behavior Detection in Time Series for Network Monitoring", http://www.usenix.org/events/lisa2000/full_papers/brutlag/brutlag_html/, Novembro.

Deri L. (2004) "Ntop Home Page", http://www.ntop.org/ntop.html, Janeiro.

Ferraiolo J., Fujisawa J. e Jackson D. (2003) "Scalable Vector Graphics (SVG) 1.1 Specification", http://www.w3.org/TR/SVG11/, Novembro.

Gaspary, L. e Tarouco, L. (1999) "Characterization and Measurements of Enterprise Network Traffic with RMON2", In: International Workshop on Distributed Systems: Operations & Management, DSOM, Switzerland.

Libpcap (2004) "Libpcap project Home Page", http://sourceforge.net/projects/libpcap/, Janeiro.

Net-SNMP (2004) "Net-SNMP Home Page", http://www.net-snmp.org/, Janeiro.

Netflow (2004) "NetFlow Home Page", http://www.cisco.com/go/netflow, Janeiro.

Netramet (2004) "NeTraMet Home Page", http://www2.auckland.ac.nz/net/NeTraMet/, Janeiro.

Oetiker T. (2004) "RRDtool Home Page", http://www.rrdtool.com/, Janeiro.

Sanchez R., Pereira, R. e Gaspary, L. (2003) "On the Development of IETF-based Network Monitoring Probes for High Speed Networks", In: Latin American Network Operations and Management Symposium, Iguassu Falls.

Waldbusser, S. (1997) "Remote Network Monitoring Management Information Base Version 2", IETF Request for Comments 2021.