NeTCollector: Uma Ferramenta para o Monitoramento Distribuído de Fluxos de Tráfego em redes IP

Rafael Costa, Leobino N. Sampaio, José A. S. Monteiro

[1]Núcleo Interdepartamental de Pesquisas em Redes de Computadores – NUPERC
Universidade Salvador (UNIFACS)
Rua Ponciano de Oliveira, 126 - Rio Vermelho 41950-275 – Salvador – BA – Brazil
rafael.costa@cc.unifacs.br, leobino@unifacs.br, suruagy@unifacs.br

Abstract. *The increased demand for network monitoring environments covering several administrative domains have motivated research groups to create and adapt tools which use a standard data representation format using Web services. Although a large number of traffic flow measurement tools are already available, little have been done in adapting them to Web services. This paper presents the NeTCollector tool. It consists of a solution for traffic flow measurements which provides a set of Web services used for filtering rule management and NeTraMet collected data recovery. Furthermore, this application provides a very friendly interface to the end users.*

Resumo. *A crescente demanda por ambientes de monitoração de redes que abrangem domínios administrativos diferentes tem motivado diversos grupos de pesquisa a envidar esforços na criação e adaptação de ferramentas que utilizem um formato padrão para representação de informações através do uso de Serviços Web. Apesar do grande número de ferramentas existentes para as medições de fluxos de tráfego, pouco trabalho foi realizado nesta direção. Este artigo apresenta a ferramenta NeTCollector que consiste em uma solução para medições de fluxos de tráfego que disponibiliza um conjunto de Serviços Web utilizados na manutenção de regras de filtragem e recuperação de dados coletados pela ferramenta NeTraMet. Além disso, a aplicação fornece uma interface bastante amigável para os usuários finais.*

1. Introdução

É cada vez maior o número de aplicações na Internet que possuem escopos de funcionamento que ultrapassam as fronteiras dos seus domínios administrativos. Por este motivo, torna-se evidente a necessidade de utilização de infra-estruturas de medições de desempenho que também ultrapassem as barreiras dos seus domínios, possibilitando ao gerente da rede ter um único ambiente de monitoração.

Acontece que desenvolver um ambiente de monitoração que opere entre domínios diferentes torna-se um desafio na medida em que as redes costumam ser constituídas por um diversificado conjunto de soluções tecnológicas que dificultam bastante o desenvolvimento de um ambiente homogêneo e interoperável. São estas as razões que têm levado diversos grupos de pesquisa a despertar o interesse em desenvolver ambientes de monitoramento que têm no uso de Serviços Web (do inglês *Web Services*)[1] o principal mecanismo de comunicação. Dentre os trabalhos já realizados e em andamento que seguem esta

[1]http://www.w3.org/

tendência, destacam-se iniciativas de desempenho fim-a-fim (E2Epi — *End to End performance initiative*) da Internet2 [Internet2 2005] e a atividade de pesquisa em Medição e Monitoração de Desempenho (JRA1) da Géant2 [Géant2 2005b], que buscam encontrar mecanismos de averiguação e acompanhamento que auxiliem no diagnóstico mais preciso dos problemas das redes pertencentes a domínios distintos.

Já no contexto nacional, a RNP, através dos grupos de trabalho GT-Medições [Monteiro 2004] e GT-Medições 2 [Monteiro 2005], vem criando uma infra-estrutura de medições orientada a serviços que possa ter interoperabilidade com outras infra-estruturas através do uso de Serviços Web. A idéia é que ferramentas de monitoração, ao utilizar um padrão de representação de informações, possam ter acesso aos dados sobre o desempenho das redes independentemente dos domínios administrativos em que estejam inseridas. Isso irá permitir que uma aplicação localizada numa rede externa possa obter as informações sobre o desempenho do *backbone* nacional antes de iniciar a sua utilização. Nesta direção foi desenvolvida a arquitetura piPEs-BR que tem módulos responsáveis por funcionalidades relacionadas à publicação, descoberta, autorização e autenticação no uso de Serviços Web; agendamento e gerência de testes; armazenamento de medidas e Interface com os usuários.

Na arquitetura do piPEs-BR está prevista a utilização de diversas ferramentas de medição que serão manipuladas pelas aplicações de gerenciamento através dos Serviços Web desenvolvidos. Cada ferramenta de medição dá contribuições ao ambiente de monitoração de acordo com a métrica de desempenho desejada. Dentre as ferramentas existentes, a NeTraMet [Brownlee 2002] destaca-se por realizar medições de fluxos de tráfego em tempo real, fornecendo informações sobre o volume e a composição do tráfego que trafega nos canais de transmissão. A ferramenta NeTraMet é uma excelente alternativa quando se deseja realizar medições de fluxos de tráfego, já que é bastante flexível ao permitir a utilização de regras na especificação dos fluxos a serem coletados. Apesar dessa ferramenta ser bastante utilizada, poucos trabalhos significativos foram realizados em torno da visualização dos dados medidos. Além disso, nenhum trabalho foi desenvolvido no sentido de criar uma interface padrão que possa ser integrada a outras infra-estruturas de medições.

É no contexto delineado acima que se insere a ferramenta NeTCollector [2], que consiste em uma aplicação desenvolvida em Java que traz uma interface amigável para a visualização dos dados medidos pelo NeTraMet, além da possibilidade de configuração dos medidores através das suas regras de filtragem. A ferramenta é totalmente orientada a Serviços Web, dando contribuições significativas em torno do desenvolvimento de ambientes de monitoração que envolvam diferentes domínios administrativos.

Este artigo está organizado da seguinte forma: na seção 2. será apresentado o contexto da ferramenta NetCollector. Na seção 3. é apresentada a ferramenta, sua arquitetura e um breve detalhamento dos módulos desenvolvidos. Na seção 4. são apresentados os testes realizados e, por fim, na seção 5., as considerações finais.

2. Trabalhos relacionados

A ferramenta NeTCollector foi desenvolvida sob a perspectiva de permitir que infra-estruturas de monitoramento possam acessar informações de desempenho de redes per-

[2] http://www.nuperc.unifacs.br/netcollector/

tencentes a domínios diferentes. Dentre as iniciativas que se destacam, pode-se citar o framework GFD e o piPEs-BR. A seguir, nas próximas subseções, serão descritos brevemente esses trabalhos, elucidando, assim, o contexto no qual a ferramenta NeTCollector está inserida.

2.1. O Framework GFD

O *framework* GFD [Géant2 2005a] foi concebido para permitir a utilização de ferramentas de medições dentro das políticas internas de um domínio administrativo de rede, porém prevendo interoperabilidade com outras infra-estruturas através de um modelo de confiança entre federações. Trata-se de um ambiente de computação distribuída de aplicações relacionadas às medições de desempenho e que tem como requisitos: escalabilidade; extensibilidade; interoperabilidade; utilização de soluções de software de padrão aberto; rápida capacidade de recuperação em casos de falhas; e monitoramento no nível IP.

Dentre os objetivos da infra-estrutura de monitoramento que segue as especificações do *framework*, pode-se citar o fato de a mesma ser flexível o suficiente para operar entre domínios e acomodar diferentes tipos de métricas, ferramentas e abordagem de monitoramento. É diante desta perspectiva que os componentes possuem um baixo grau de acoplamento entre si, expondo as suas funcionalidades através de serviços.

O GFD prevê a existência de produtores e consumidores de serviços que podem ser classificados nos seguintes tipos: Ponto de Medição (MP — *Measurement Point Service*); Publicação/descoberta (LS — *Look-up Service*); Autenticação/Autorização (AS - Authentication Service); Controlador de recursos (RP — *Resource Protector Service*); Armazenamento de medições (MA — *Measurement Archive Service*); Transformação (TS — *Transformation Service*); e Topologia (ToS — *Topology Service*).

2.2. O ambiente piPEs-BR

O ambiente piPEs-BR [Monteiro 2004] é composto por ferramentas já existentes (adaptadas para o ambiente) bem como novas ferramentas desenvolvidas em GTs anteriores. O piPEs-BR visa contemplar funcionalidades de: testes, armazenamento, agendamento, autorização, interface e detecção/aconselhamento. Após a revisão da arquitetura, inicialmente concebida para o piPEs-BR e tendo como base a arquitetura GFD, foi possível se chegar numa segunda versão da arquitetura do piPEs-BR.

Nesta nova arquitetura, os componentes desenvolvidos são adaptados para terem os seus funcionamentos de acordo com a especificação do GFD. Além disso, novos componentes são adicionados, disponibilizando outros serviços necessários para o funcionamento do ambiente. Entre os novos componentes merecem destaque os responsáveis pelos serviços de agendamento e gerência de testes, bem como de publicação, descoberta, autorização e autenticação de serviços.

3. A ferramenta NetCollector

A ferramenta NeTCollector, desenvolvida em Java, é dividida em dois módulos: um cliente que apresenta a interface com o usuário final e um servidor que funciona como um gerente SNMP do NeTraMet e disponibiliza Serviços Web para sua manipulação. As funcionalidades da ferramenta fazem desde a coleta dos dados sobre fluxos medidos

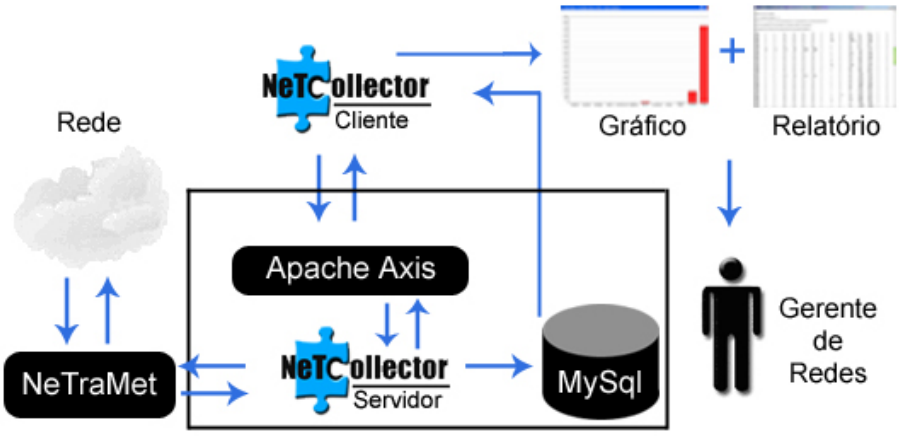

Figura 1. Arquitetura da ferramenta NeTCollector.

pelo NeTraMet até a configuração de regras no medidor. Um resumo da arquitetura da ferramenta é apresentada na Figura 1.

3.1. Módulo Servidor

Para a construção do módulo servidor, foi utilizado o pacote Java SNMP [JavaSNMP 2005], que dá suporte às principais funcionalidades necessárias à obtenção dos dados armazenados no agente SNMP (NeTraMet). Essas informações medidas pelo NeTraMet e coletadas via protocolo SNMP são armazenadas num banco de dados MySQL. Com base nesse banco de dados, Serviços Web foram desenvolvidos para disponibilizar os dados que podem ser utilizados na geração de relatórios pelo cliente. O cliente pode armazenar os dados coletados em arquivos texto em formato de relatórios para referências futuras ou opcionalmente mostrados na tela ao final da coleta definida pelo usuário.

Para o desenvolvimento dos Serviços Web, foi utilizado o pacote do projeto Apache Axis[3] o qual fornece uma boa infra-estrutura para o desenvolvimento de aplicações desta natureza. Isto por que através dele, o desenvolvedor de Serviços Web não precisa se preocupar com o tratamento de mensagens SOAP e o uso de APIs Java mais específicas como JAX-RPC (*Java API for XML-based RPC*) e JAXM (*Java API for XML Messaging*). Na Tabela 1 estão relacionados os principais serviços desenvolvidos no módulo servidor.

Tabela 1. Serviços Web do módulo servidor.

Serviço	Parâmetros de entrada
`coletaFluxosWS`	enderecoMedidor
`setaregraWS`	endereco, selector, mask, matchedvalue, action, parameter
`tiraregradeexecucaoWS`	enderecoMedidor, idDaRegra

3.2. Módulo Cliente

Já no módulo cliente, além dos relatórios, ainda podem ser gerados gráficos estatísticos, tudo de forma integrada. Para que sejam gerados os gráficos, foi utilizado o pacote

[3]http://ws.apache.org/axis/

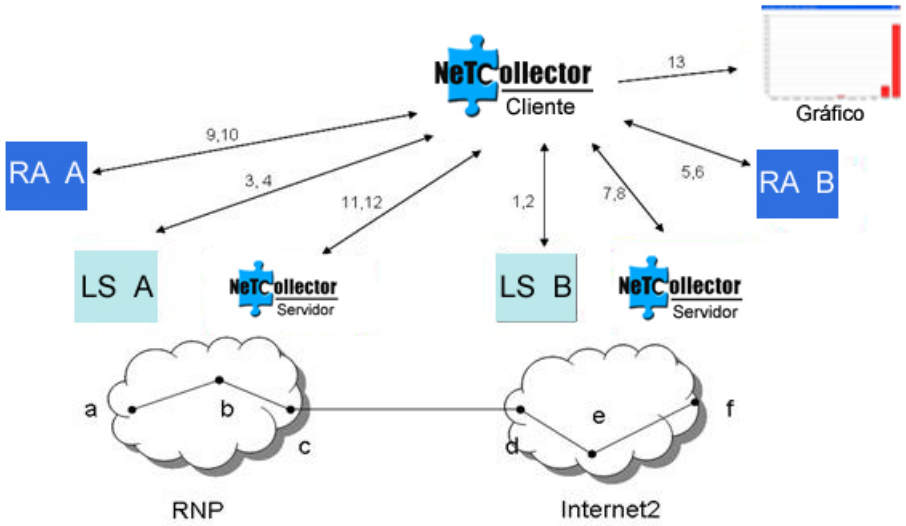

Figura 2. Cenário de utilização da ferramenta NetCollector.

ChartDirector [Engineering 2005], que permite construir gráficos profissionais de diversos tipos, como pizza, barras, etc, podendo ser utilizados tanto para aplicações web como Windows.

O software tem como principal objetivo possibilitar ao gerente da rede a realização de planejamentos e identificação de possíveis problemas que estejam ocorrendo.

Através do NeTCollector foi possível ter um software capaz de integrar o que grande parte das aplicações de medição de fluxos de redes fazem isoladamente: manter uma base de dados consistente com diversos atributos que dizem respeito ao tráfego em uma rede, gerar relatórios técnicos capazes de auxiliar o administrador da rede a diagnosticar e identificar problemas referentes ao ambiente, disponibilizar Serviços Web para acessos remotos, e por fim, construir gráficos com estatísticas acerca do ambiente de rede de um domínio administrativo.

3.3. Cenário de utilização do NetCollector

Ao disponibilizar Serviços Web através do módulo servidor, o NetCollector permite que diversos coletores de fluxos, pertencentes a domínios distintos, possam ser configurados de modo a identificar fluxos de interesse das aplicações de monitoração. Pelo fato de utilizar Serviços Web na comunicação entre os módulos, a probabilidade de acontecer problemas de interoperabilidade em razão das peculiaridade de cada domínio é bastante reduzida. Na Figura 2 é ilustrado um cenário em que o NeTCollector pode ser utilizado com dois domínios distintos, assumindo também a existência de uma infra-estrutura para publicação/descoberta de serviços (LS) e de autenticação (RA).

Neste cenário, o módulo cliente faz acesso aos serviços prestados pelos servidores nos dois domínios (RNP e Internet2). Os serviços acessados são utilizados para configuração de medidores e recuperação de dados coletados. Os passos de 1 a 4 envolvem a busca por informações sobre os serviços prestados pelos módulos servidor. Nos passos 5, 6, 9 e 10 o cliente requisita a autorização para acesso aos serviços disponibilizados que, posteriormente, são solicitados nos passos 7, 8, 11 e 12. Por fim, o cliente após obter as informações necessárias gera o gráfico de interesse ou recebe a confirmação de

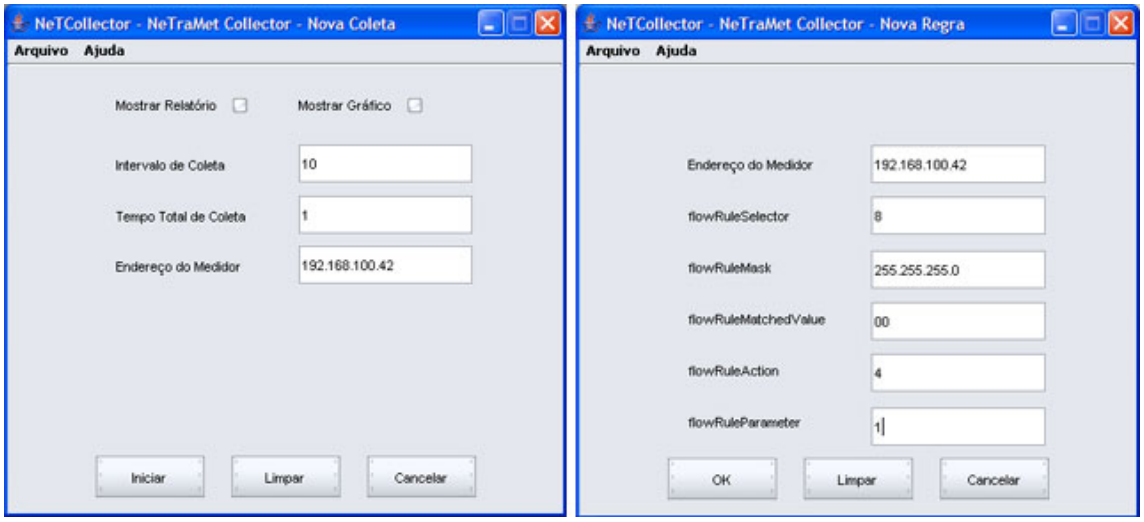

Figura 3. Interface de coleta e configuração de regras do cliente.

uma solicitação de configuração no passo 13.

4. Testes realizados

Diversos testes experimentais foram realizados no laboratório do CEPERC - UNIFACS, composto por uma média de 40 máquinas conectadas em rede, com o objetivo de buscar informações sobre os fluxos que trafegam no ambiente como um todo.

Para que isso fosse possível, um ambiente de medições teve que ser montado, de acordo com a arquitetura apresentada na Figura 1.

Para composição do módulo servidor, foram utilizadas duas estações IBM Pentium 4 com o sistema operacional Red Hat Linux 9.0. A primeira estação foi utilizada para a instalação do NeTraMet 5.0 e do Apache Axis, enquanto que a segunda serviu para a instalação do SGBD MySql. No módulo Cliente, foi utilizada uma estação Pentium 4 com o sistema operacional Windows XP. Essa aplicação poderia funcionar ainda em outros sistemas, graças à portabilidade da linguagem Java.

O usuário ao interagir com a ferramenta deve especificar no cliente, o endereço do medidor, tempo total da coleta de informações e intervalo (periodicidade) em que se quer coletar tais fluxos (Figura 3). Esses parâmetros são passados ao módulo servidor pelo Apache Axis e então o servidor se conecta ao NeTraMet via protocolo SNMP e obtém os fluxos coletados de acordo com o que foi especificado pelo usuário. Após a obtenção dessas informações, o módulo servidor se conecta à base de dados MySql e armazena os dados relevantes.

Após a conclusão da coleta (final do tempo total estipulado pelo usuário), o módulo cliente oferece como opções a geração de gráficos e relatórios técnicos sobre as informações coletadas na rede (Figuras 4 e 5).

5. Considerações finais e trabalhos futuros

Apesar dos trabalhos na área que relacionam as medições por fluxo de tráfego aos Serviços Web [Sampaio et al. 2004, da Rosa et al. 2004], pouco foi feito em relação ao

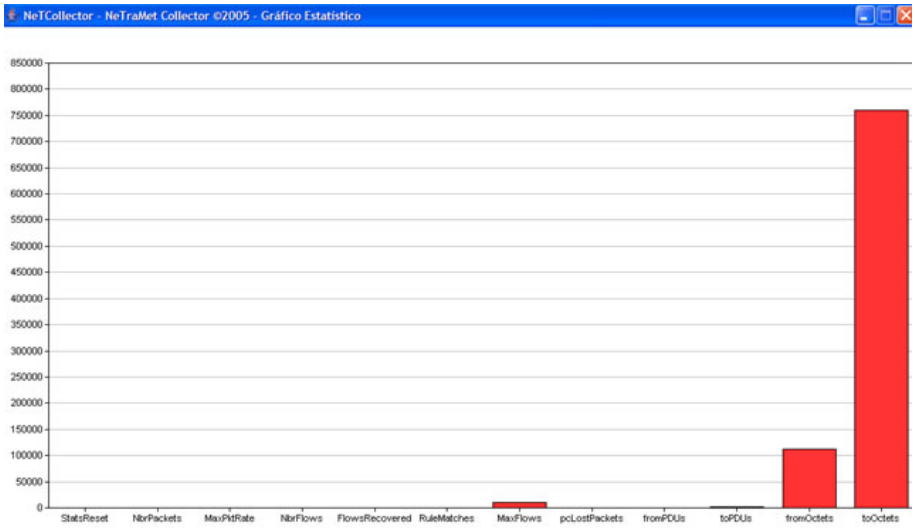

Figura 4. Gráfico gerado no módulo cliente.

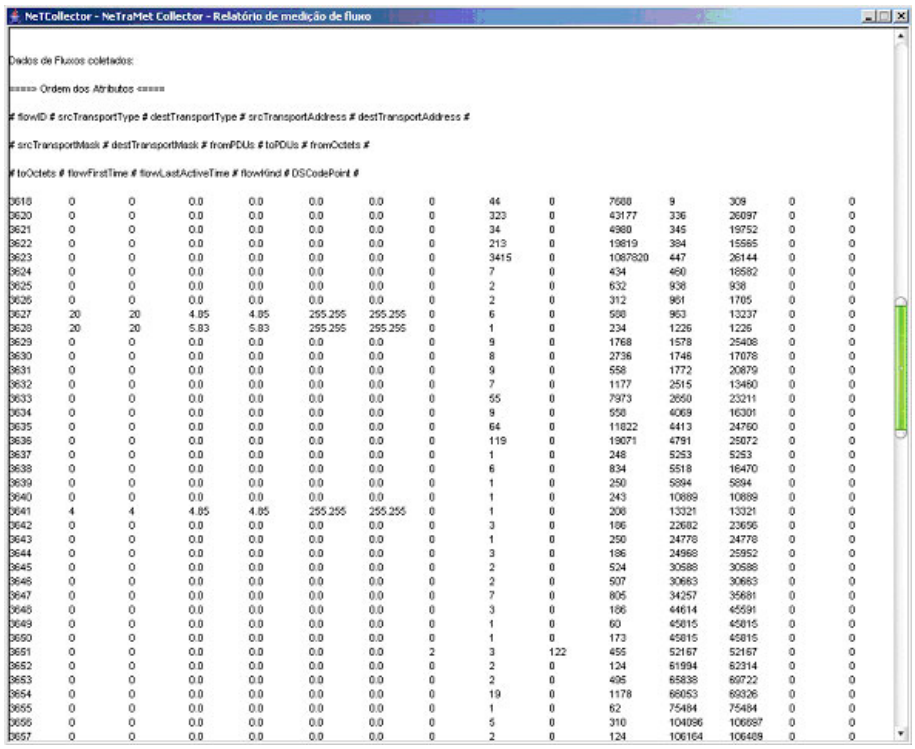

Figura 5. Relatório gerado no módulo cliente.

NeTraMet que possibilita a definição de regras mais específicas para identificação de fluxos de tráfego. Se por um lado esta ferramenta permite a utilização de regras, por outro tem uma interface com o usuário muito pobre em recursos, o que dificulta bastante a sua utilização. Além disso, a única forma de utilização desta ferramenta é através da linha de comando, utilizando o gerente NeMac.

Portanto, a ferramenta NeTCollector traz importantes contribuições em torno do desenvolvimento de um ambiente distribuído de monitoração de fluxos de tráfego que, através do seu módulo servidor, disponibiliza um conjunto de Serviços Web para configuração de regras da ferramenta NeTraMet. Além disso, através do módulo cliente tem-se uma interface gráfica bastante amigável, facilitando bastante a configuração de regras e a visualização dos dados coletados sobre os fluxos.

Os trabalhos futuros com a ferramenta serão na direção do desenvolvimento de uma infra-estrutura que facilite o gerenciamento e utilização dos serviços desenvolvidos por parte de outras ferramentas, por meio da utilização de infra-estruturas de publicação, descoberta, autenticação e gerenciamento de configurações dos medidores.

Agradecimentos

Os autores agradecem todo o apoio que a RNP vem dando ao GT-Medições 2 com o fornecimento da infra-estrutura técnica necessária para a realização deste trabalho.

Referências

Brownlee, N. (2002). Using netramet for production traffic measurement. Conference/Journal: Integrated Network Management Proceedings.

da Rosa, D. M., Pereira, E. D. V., Granville, L. Z., Almeida, M. J. B., and Tarouco, L. M. R. (2004). Uma Solução Baseada em Web Services para o Gerenciamento de Coletores NetFlow Distribuídos. In *IX WGRS*, pages 3–14, Gramado, RS. Anais do SBRC 2004.

Engineering, A. S. (2005). Chartdirector. `http://www.advsofteng.com/index.html/`.

Géant2 (2005a). Deliverable D.J.1.2.1: General Framework Design. `http://www.geant2.net`.

Géant2 (2005b). Géant2. http://www.geant2.net.

Internet2 (2005). Internet2. `http://www.internet2.edu`.

JavaSNMP (2005). Java snmp package. `http://edge.mcs.drexel.edu/GICL/people/sevy/snmp/snmp_package_introduction.html`.

Monteiro, J. A. S. (2004). GT-Medições: Documento de Diagnóstico e Alternativas. Technical Report P2.1, RNP.

Monteiro, J. A. S. (2005). GT-Medições2 (GT-Med2): Proposta para Grupo de Trabalho. Technical report, RNP.

Sampaio, L., Granville, L. Z., and Monteiro, J. A. S. (2004). Gerenciamento de Medições por Fluxo de Tráfego: Uma abordagem baseada no uso de Banco de Dados e Serviços Web. In *IX WGRS*, pages 15–26, Gramado, RS. Anais do SBRC 2004.