

## **Proposta para Grupo de Trabalho**

GT-BackStreamDB - Monitoramento de Tráfego  
de Backbones Baseado em SGSD

Elias P. Duarte Jr. (Coordenador)

Carmem S. Hara (Coordenadora Adjunta)

2008

## **1. Título**

GT-BackStreamDB: Monitoramento de Tráfego de Backbones Baseado em SGSD (Sistemas Gerenciadores de Streams de Dados)

## **2. Coordenador**

Coordenador: Elias Procópio Duarte Júnior  
Coordenadora Adjunta: Carmem Satie Hara  
Departamento de Informática, Universidade Federal do Paraná  
Centro Politécnico - Jardim das Américas  
Caixa Postal: 19081 CEP: 81531-980 - Curitiba – PR  
Fone: (41) 3361-3656  
Fax: (41) 3361-3205  
E-Mail: {elias, carmem}@inf.ufpr.br  
Web: <http://www.inf.ufpr.br/elias>

## **3. Resumo**

O monitoramento de tráfego de um backbone como um todo apresenta uma série de desafios, especialmente devido ao grande número de componentes e sua distribuição geográfica, além do volume de tráfego. Ferramentas tradicionais, como as baseadas no Netflow, apresentam diversas limitações, em geral não permitindo consultas sobre as condições da rede em tempo real. O objetivo do GT-BackStreamDB é projetar e implementar uma solução distribuída para monitoramento de tráfego capaz de gerar medições arbitrárias requisitadas pelo administrador em tempo real, considerando fluxos de todo o backbone. A utilização de técnicas de gerenciamento de streams de dados permitem que o tráfego do backbone como um todo seja tratado de forma distribuída mas coesa. O projeto prevê integração com o arcabouço MonIPÊ.

## **4. Parcerias**

O GT-BackStreamBD prevê parceria com o PoP-PR, especialmente com Christian Lyra Gomes, que recentemente (22/08/2008) defendeu dissertação de mestrado orientado pelos coordenadores deste projeto no uso de SGSD para Monitoramento de Tráfego de Backbones. Outra parceria importante é representada na integração com o projeto de monitoração MonIPÊ através de colaboração neste projeto com o Prof. José Augusto Suruagy Monteiro (UNIFACS). Além destas, devem ser estabelecidas parcerias ainda na primeira fase com 2 PoPs da RNP e CEO. Em uma segunda fase, o projeto tem por objetivo atingir todos os PoPs da RNP.

## **5. Duração do projeto**

12 meses

## 6. Sumário executivo

O tratamento de grandes volumes de informação de fluxos em um backbone é um desafio. As ferramentas tradicionais para este fim não são facilmente escaláveis e não são capazes de funcionar de forma distribuída. Um método comum utilizado para o monitoramento de redes é através do armazenamento de registros coletados. Porém, a necessidade de armazenamento causada pelo excesso de dados é bastante significativa. Com isso, muitas vezes os dados armazenados são restritos a um período de tempo. A análise dos registros armazenados pode ser feita por *scripts* desenvolvidos especialmente para um determinado sistema ou utilizando ferramentas existentes.

Existe uma grande variedade de ferramentas para monitoramento de tráfego [2], tanto comerciais quanto gratuitas, além de algumas com código aberto. Porém, o grande problema destas ferramentas é a falta de flexibilidade. Normalmente elas já provêm um determinado conjunto de informações que nem sempre são as mais apropriadas para atender às necessidades da rede em questão. No caso das ferramentas com código aberto, alterá-las nem sempre é uma tarefa fácil, exigindo a contratação de profissionais e bastante tempo para tentar adequar a ferramenta para atingir os objetivos que uma determinada rede demanda. Em relação às ferramentas comerciais, além do custo para a compra das ferramentas, muitas vezes não é permitido alterá-las, sendo preciso negociar com o vendedor a adequação específica para um cliente, exigindo investimento e um tempo de espera significativos.

Este projeto propõe o desenvolvimento de um arcabouço e a implementação de uma ferramenta para monitoração do tráfego do backbone da RNP como um todo baseado em um SBSDB (Sistema Gerenciador de Streams de Dados). O objetivo de um SGSD é prover as funcionalidades dos Sistemas Gerenciadores de Banco de Dados (SGBD) tradicionais sobre fluxos contínuos de dados. Estes fluxos de dados (*streams*) podem ser, por exemplo, os pacotes trafegando em uma rede, ou dados de uma rede de sensores, ou de um sistema de monitoramento de chamadas. A característica principal destes sistemas é a existência de um grande volume de dados, o que impossibilita que eles sejam armazenados em sua totalidade para serem processados posteriormente. Assim, os SGSDs são sistemas que, além de outras facilidades, possuem uma linguagem de alto nível para expressar consultas, que são processadas à medida que os dados fluem pelo sistema.

Entre os trabalhos relacionados mais significativos destaca-se o Gigascope [3] da AT&T, uma ferramenta proprietária para o monitoramento de tráfego, cujo funcionamento é baseado no princípio dos gerenciadores de streams de dados. No entanto tal ferramenta não é aberta, sendo de uso exclusivo da AT&T. A vantagem da abordagem de desenvolver de uma ferramenta de monitoramento de redes utilizando um Sistema Gerenciador de Stream de Dados (SGSD) é que tais sistemas têm como objetivo prover as mesmas funcionalidades de um Sistema Gerenciador de Banco de Dados (SGBD), porém sobre fluxos de dados ao invés de dados armazenados. Dessa forma, métricas arbitrárias para o monitoramento de uma rede podem ser expressas

em uma linguagem de consulta de alto nível e os resultados são produzidos em tempo real.

O principal objetivo deste projeto é o desenvolvimento de uma ferramenta de monitoramento de backbones utilizando o SGSD Borealis [1] e sua implantação em forma de projeto piloto no POP-PR. O Borealis é um sistema de código aberto desenvolvido pelas seguintes universidades americanas: MIT, Brandeis e Brown. As principais características deste SGSD é que ele permite a integração dos dados e compartilhamento de recursos, além de dar suporte a mecanismos de tolerância a falhas, processamento distribuído, escalabilidade, e balanceamento e dispersão de carga. Duas dissertações de mestrado foram defendidas na UFPR utilizando este sistema para o desenvolvimento de uma ferramenta de monitoramento de redes. A primeira apresenta a ferramenta *PaQueT*, que tem como foco o monitoramento de uma rede local. Ela faz a captura de todo o tráfego da rede e permite a submissão de consultas que envolvam campos no cabeçalho sobre os protocolos de transporte TCP e UDP [4, 5]. Alguns exemplos de métricas que podem ser obtidas pela ferramenta através do registro de consultas no sistema são listadas abaixo:

- número de pacotes UDP e TCP transmitidos em uma determinada janela de tempo;
- taxa de transmissão por IP;
- média do tamanho dos pacotes trafegando;
- quantidade de bytes trocados em cada conexão.

A segunda dissertação defendida tem como foco o monitoramento de um backbone [6], através do processamento de fluxos do protocolo Netflow [7]. Exemplos de informações que podem ser gerados pelo sistema são listados abaixo.

- matriz de tráfego, que é o conjunto de valores de tráfego medidos dois a dois dentre os participantes de uma determinada rede;
- detecção de varreduras de rede, que acontece quando um host envia pacotes para vários outros hosts de uma rede com objetivo de descobrir quais respondem e quais não; a característica desses tipos de sonda é a grande quantidade de fluxos com apenas 1 pacote (em geral apenas um pacote UDP, ou um pacote ICMP é enviado);
- identificação da fonte de um ataque de negação de serviço após a identificação de um alvo.

A característica principal da ferramenta proposta é que cada uma das métricas listadas acima corresponde a uma consulta, expressa em uma única linguagem de consulta de alto nível, que possui poder de expressão similar ao SQL [8], que é a linguagem padrão para consultas em SGBDs relacionais. Assim, a obtenção de informações em diferentes níveis de monitoramento de uma rede podem ser obtidas utilizando uma única ferramenta. Dentre as outras vantagens que a ferramenta apresenta, podem ser citadas:

- geração de dados de monitoramento em tempo real, possibilitando a escolha dos dados históricos que devem ser armazenados;
- capacidade de processamento distribuído de consultas, permitindo que a

filtragem de dados possa ser realizada próxima às fontes de dados;

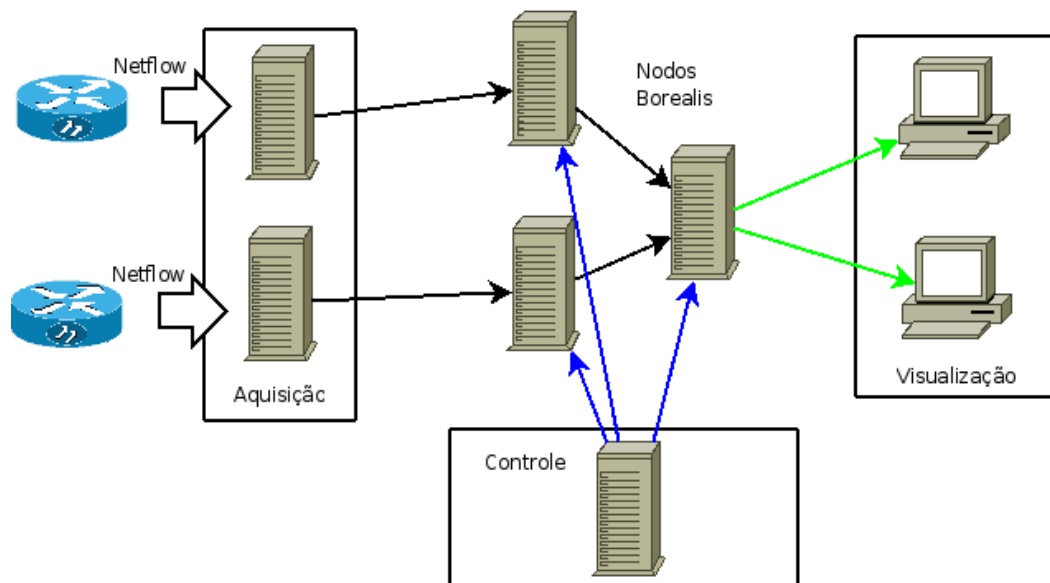
- facilidade de estender a ferramenta para o monitoramento de outros tipos de fluxos, tais como processamento de logs de roteadores, logs de chamadas Voip, requisições Web/vídeo.

Por fim destaca-se que a ferramenta será integrada ao arcabouço de monitoramento de tráfego MonIPÊ [9].

## 7. Descrição da proposta

As atividades a serem escutadas por este GT consistem na implantação de uma rede de processamento de fluxos. Inicialmente serão tratados fluxos de dados Netflow, mas a arquitetura de ferramenta será extensível de forma que no futuro fluxos de outros tipos de dados possam ser considerados.

A figura abaixo mostra uma visão geral da arquitetura:



### 7.1. Rede de nodos de processamento de fluxos

A implementação da rede dos nodos de processamento de fluxos se dará pela instalação de um nodo em cada PoP participante. Tal nodo receberá os fluxos Netflow gerados pelo roteador deste PoP. Caso o roteador do PoP não gere registros Netflow, será necessário espelhar uma porta do switch de distribuição de forma que o próprio nodo possa gerar os registros de netflow através de uma ferramenta como nprobe.

## **7.2. Servidor de controle de nodos**

O servidor de controle de nodos será o responsável pela distribuição de consultas e pelo acesso aos nodos de processamento. As ferramentas atuais baseadas em SGSD possuem um fraco controle de acesso, e portanto essa será uma área onde o grupo de trabalho poderá fazer uma contribuição significativa.

A ferramenta desenvolvida nas dissertações de Mestrado, capturam os dados e realizam as consultas em uma máquina central, a qual é responsável por executar todas as tarefas. Foram feitos alguns testes com o processamento distribuído, porém para abranger todas as vantagens do uso do Borealis de forma distribuída, são necessárias algumas adaptações dos componentes da ferramenta desenvolvida. Além disso, pelo fato do Borealis se tratar de um SGSD ainda em desenvolvimento, alguns detalhes precisam ser verificados diretamente no código. A documentação do Borealis ainda é falha em relação a todo seu potencial, assim como algumas partes do código ainda precisam de aperfeiçoamento.

## **7.3. Estudos de desempenho**

As duas dissertações de mestrado defendidas na UFPR demonstraram um potencial para o processamento de fluxos da ordem de 40 mil registros de fluxo por segundo de forma sustentada, por nodo de processamento, e utilizando máquinas relativamente modestas (mono-processadas). Tal capacidade se mostrou o suficiente para o processamento em tempo real de registro de fluxo (Netflow) do PoP-PR. Além da melhoria do hardware é possível que otimizações no código elevem bastante esse patamar e é uma das contribuições esperadas do GT.

Os testes realizados em ambos os trabalhos foram suficientes para validar a viabilidade da proposta e mostrar como pode ser útil no monitoramento de um backbone. No entanto, as melhorias a serem realizadas na ferramenta devem aumentar ainda mais a capacidade da ferramenta, o que poderá ser demonstrado em novos estudos de desempenho.

## **7.4. Interfaces de controle**

Criação de ferramentas gráficas que permitam o controle dos nodos de processamento, criação de consultas e visualização de resultados.

## **7.5 Integração com MonIPÊ**

A ferramenta proposta deverá ter possibilidade de uso integrado com Serviço Experimental MonIPÊ [9]. Está previsto o uso desta ferramenta como alternativa para a monitoração passiva, hoje realizada no contexto do ambiente perfSONAR [10]. Para a integração, os dados medidos, ou até mesmo o controle da coleta devem ser realizados via Web Services.

Destaca-se que o projeto Géant3 [11] em definição deverá contemplar um esquema de medições passivas que será baseado no trabalho realizado anteriormente no contexto do serviço de medição passiva Lobster [12] que, assim como o perfSONAR pode ser considerado completar à ferramenta proposta no presente GT-BackStreamDB.

Os **cronograma** para obtenção de resultados esperado pelo GT-BackStreamDB são os seguintes:

- *Rede de nodos de processamento de fluxos*: Implantação de uma rede piloto de nodos de processamento de fluxos, na qual os nodos se localizam próximos às fontes geradoras de informação de fluxo, ou seja, nos Pontos de Presença da RNP. (Mês 1-6)
- *Servidor de controle de nodos*: Implementação de um servidor que promove a coordenação das ações dos nodos, como o registro de consultas para a obtenção das métricas desejadas, e o controle de acesso aos nodos de processamento. (Mês 1-6)
- *Avaliação de desempenho*: Realização de experimentos para determinar o desempenho do sistema na obtenção de métricas em tempo real. Destaca-se que este tipo de informação só podem ser obtida *a posteriori* pelas ferramentas de monitoramento de tráfego mais usadas atualmente. (Mês 4-12)
- *Interfaces de controle*: Criação de ferramentas gráficas que permitam o controle dos nodos de processamento, criação de consultas e visualização de resultados. (Mês 5-9)
- Por fim será realizada uma integração com o arcabouço de monitoração de tráfego MonIPÊ. (Mês 4-12)

## 8. Ambiente para testes do protótipo

O ambiente para os testes do protótipo incluirá os mesmos equipamentos para desenvolvimento orçados nesta proposta, além de máquinas de serviço da RNP nos PoP-PR e nos laboratórios das equipes envolvidas. Os testes serão realizados no backbone da RNP, destacando-se que não impõem sobrecarga representativa visto que se constituem de experimentos de monitoração passiva.

## 9. Referências

[1] Daniel. J. Abadi, Yanif Ahmad, Magdalena Balazinska, Ugur Centintemel, Mitch Cherniack, Jeong-Hyon Hwang, Wolfgang Lindner, Anurag S. Maskey, Alexander Rasin, Esther Ryvkina, Nesime Tatbul, Ying Xing, Stan Zdonik: *The Design of the Borealis Stream Processing Engine*. Proceedings of the 2nd Conference on Classless Inter-Domain Routing (CIDR'05), 2005, pp. 277-289

- [2] Stanford Linear Accelerator Center: *Network Monitoring Tools*, [www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html](http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html), 2008
- [3] Chuck Cranor, Theodore Johnson, Oliver Spatscheck, Vladislav Shkapenyuk: *The Gigascope Stream Database*, IEEE Data Engineering Bulletin, volume 26, número 1, 2003, pp. 27-32
- [4] Natascha P. Ligocki: *Uma Ferramenta de Monitoramento de Redes usando Sistemas Gerenciadores de Streams de Dados*, Dissertação de Mestrado, Departamento de Informática, Universidade Federal do Paraná, 2008
- [5] Natascha Petry Ligocki, Christian Lyra, Carmem Hara: *A Flexible Network Monitoring Tool based on a Data Stream Management System*, Proceedings of the 2008 IEEE Symposium on Computers and Communications (ISCC), Marrakech, Morocco, 2008
- [6] Christian L. Gomes: *Análise de Tráfego de Backbones Baseada em Sistemas Gerenciadores de Streams de Dados*, Dissertação de Mestrado, Departamento de Informática, Universidade Federal do Paraná, 2008
- [7] Cisco Systems Inc, *NetFlow Services and Applications - White Paper*, [www.cisco.com/warp/public/cc/pd/iosq/ioft/neflc](http://www.cisco.com/warp/public/cc/pd/iosq/ioft/neflc), 2008
- [8] Donald Chamberlin, Raymond F. Boyce: *SEQUEL: A Structured English Query Language*, *Proceedings of the 1974 ACM SIGFIDET Workshop on Data Description, Access and Control*, pp. 249–264.
- [9] Serviço de Monitoração Experimental MonIPÊ, <http://wiki.nuperc.unifacs.br/monipe/>, 2008
- [10] PerfSONAR, [www.perfsonar.net](http://www.perfsonar.net), 2008
- [11] Géant2 Website, <http://www.geant2.net/>, 2008
- [12] Lobster: *Large Scale Monitoring of Broadband Internet Infrastructures*, <http://www.ist-lobster.org/>, 2008