

Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Ciência da Computação

GUILHERME SAULO ALVES

MONOGRAFIA EM SISTEMAS DE INFORMAÇÃO II

**COLETA, ANÁLISE E VISUALIZAÇÃO DE DADOS ESTATÍSTICOS APLICADO
AO AMBIENTE DE UM PONTO DE TROCA DE TRÁFEGO**

Belo Horizonte
2016 / 2º Semestre

Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Curso de Bacharelado em Sistemas de Informação

**COLETA, ANÁLISE E VISUALIZAÇÃO DE DADOS
ESTATÍSTICOS APLICADO AO AMBIENTE DE UM
PONTO DE TROCA DE TRÁFEGO**

por

GUILHERME SAULO ALVES

Monografia em Sistemas de Informação II

Apresentado como requisito da disciplina de Monografia em
Sistemas de Informação II do Curso de Bacharelado em Sistemas de
Informação da UFMG.

Prof. Dorgival Olavo Guedes Neto

Orientador

Luis Felipe Cunha Martins

Coorientador

Belo Horizonte
2016 / 2º Semestre

AGRADECIMENTOS

Primeiramente agradeço a Deus pela oportunidade e por ser meu amigo fiel não somente nestes anos de universidade, mas ao longo de toda minha vida. A minha família pelo amor e incentivo. Ao Prof. Dorgival Guedes e ao colega de trabalho Luis Felipe pela orientação na elaboração deste trabalho. E por fim, aos meus colegas de curso que fizeram parte da minha formação.

*“O temor do Senhor é o princípio do saber,
mas os loucos desprezam a sabedoria e o ensino.”*

Provérbios 1:7

RESUMO

O objetivo do presente trabalho foi realizar um estudo sobre os pontos de troca de tráfego (IX ou IXP) e implementar um serviço de coleta, análise e visualização de dados estatísticos para o ambiente. Para tanto, foram pesquisadas na literatura as principais ferramentas de apoio ao gerenciamento e monitoramento de redes que permitem implementar esse serviço no ecossistema de um IX. O estudo proposto foi desenvolvido com base na operação do IX de Minas Gerais (IX.br-MG), atualmente carente deste serviço de coleta. Espera-se que o sistema possa ser útil para o ambiente de um IX, tornando a operação do mesmo mais simples e eficaz, promovendo ganhos tanto para os administradores do IX quanto para os seus participantes.

Palavras-chave: Troca de tráfego, gerenciamento de redes, medição de fluxo de tráfego, protocolo sFlow.

ABSTRACT

In this work we study alternatives to implement a service of collection, analysis and visualization of statistical data from an Internet traffic Exchange Points (IX or IXP). We investigate the main tools to support the management and monitoring networks on IX ecosystem. The proposed study was developed based on operation of IX.br-MG, currently lacking this service. It is expected that the system can be useful for an IX environment, making operation even simpler and effective, providing both gains for IX administrators as to its participants.

Keywords: Peering, network management, traffic flow measurement, sFlow protocol.

LISTA DE FIGURAS

Figura 1. Troca de Tráfego entre ASes	7
Figura 2. Conexão dos ASes em um IX	8
Figura 3. Interação entre PIXes.....	9
Figura 4. Topologia de rede de um IX	10
Figura 5. Localidades atuais e em estudo do IX.br	13
Figura 6. Tráfego de entrada e saída entre dois ASes do IX.br-MG	16
Figura 7. Arquitetura básica de gerência de redes	19
Figura 8. Funcionamento do protocolo SNMP	21
Figura 9. Criação de fluxos no cache NetFlow	25
Figura 10. Formato de exportação do IPFIX.....	27
Figura 11. Arquitetura do IPFIX	28
Figura 12. Arquitetura sFlow	29
Figura 13. Diagrama do datagrama sFlow	30
Figura 14. Tecnologias que foram utilizadas no projeto.....	32
Figura 15. Protótipo da estrutura do IX	33
Figura 16. Geração de tráfego usando a ferramenta iperf	34
Figura 17. Exemplo de arquivo com datagrama sFlow.....	35
Figura 18. Exemplo de entradas no arquivo de métricas para o InfluxDB	35
Figura 19. Interface Web do InfluxDB	37
Figura 20. Dashboard construído no Grafana	38
Figura 21. Matriz de troca de tráfego entre os ASes	39
Figura 22. Tráfego total agregando todos os ASes	40
Figura 23. Tráfego total detalhado por AS.....	41
Figura 24. Tráfego total por vlan (ATM x ATB).....	41
Figura 25. Estatística por AS (destino AS3)	42
Figura 26. Estatística por AS (origem AS4)	42
Figura 27. Tráfego de entrada e saída para o S2	43
Figura 28. Tráfego total separado por acordos ATM e ATB e VLAN	43

LISTA DE SIGLAS

ANATEL	Agência Nacional de Telecomunicações
ARP	Address Resolution Protocol
AS	Autonomous System
ATB	Acordo de Troca de Tráfego Bilateral
ATM	Acordo de Troca de Tráfego Multilateral
BGP	Border Gateway Protocol
CGI	Comitê Gestor da Internet
CIX	Channel to IX
CMIP	Coupled Model Intercomparison Project
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPFIX	IP Flow Information Export
IP	Internet Protocol
IX	Internet Exchange
IXP	Internet Exchange Point
MAC	Media Access Control
MIB	Management Information Base
MSI	Monografia em Sistemas de Informação
NIC	Núcleo de Informação e Coordenação do Ponto
OSI	Open Systems Interconnection
POP	Ponto de Presença
PTT	Ponto de Troca de Tráfego
RFC	Request for Comments
RNP	Rede Nacional de Pesquisa
SGBD	Sistema de Gerenciamento de Banco de Dados
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UFMG	Universidade Federal de Minas Gerais

LISTA DE TABELAS

Tabela 1. Tags e campos utilizados na contabilização	36
---	----

SUMÁRIO

AGRADECIMENTOS	iii
RESUMO	v
ABSTRACT	vi
LISTA DE FIGURAS	vii
LISTA DE SIGLAS	viii
LISTA DE TABELAS	ix
1 INTRODUÇÃO	1
1.1 Motivação e Objetivos.....	2
1.2 Contribuição do Trabalho	2
1.3 Metodologia de Trabalho.....	3
1.4 Organização do Texto	4
2 TRABALHOS RELACIONADOS E ESTADO ATUAL DA ARTE	5
3 CONTEXTUALIZAÇÃO	6
3.1 Troca de tráfego - <i>Peering</i>	6
3.2 Pontos de Troca de Tráfego - Visão Geral.....	7
3.3 Pontos de Troca de Tráfego - Arquitetura.....	9
3.3.1 Servidor de Rotas	10
3.3.2 Looking Glass	10
3.3.3 PIXes.....	11
3.3.4 Sistemas Autônomos	11
3.4 Pontos de Troca de Tráfego - Tipos de acordos	11
3.5 Pontos de Troca de Tráfego - Benefícios	12
3.6 Projeto PTTMetro.....	12
3.6.1 Regras.....	14
3.6.2 Infraestrutura	15
3.6.3 Processos de Rotinas	15
3.6.4 Dificuldades e Problemas.....	16
3.7 Gerenciamento de Redes	17
3.7.1 Gerência de Redes	17
3.7.2 Protocolo SNMP	20
3.7.3 Monitoramento de tráfego.....	22
3.7.3.1 Monitoramento baseado em fluxos de tráfego.....	22
3.8 NetFlow	24
3.9 IPFIX.....	25
3.10 sFlow.....	28

4	PROJETO	31
4.1	Modelagem e prototipação do ambiente	31
4.1.1	Geração dos dados	32
4.1.2	Coleta, armazenamento e análise dos dados	34
4.1.3	Visualização dos dados	37
5	RESULTADOS E DISCUSSÃO	39
5.1	Matriz de troca de tráfego	39
5.2	Tráfego total agregado	40
5.3	Tráfego total detalhado	40
5.4	Tráfego total por VLAN (ATM x ATB)	41
5.5	Estatística por AS (destino AS3)	42
5.6	Estatística por AS (origem AS4)	42
5.7	Estatística por AS (entrada e saída do AS2)	43
5.8	Outras estatísticas	43
5.9	Benefícios gerais	44
5.10	Acesso à ferramenta “Wall-PTT”	44
6	CONCLUSÃO	45
	REFERÊNCIAS BIBLIOGRÁFICAS	46
	APÊNDICE A – CÓDIGO DOS SCRIPTS	50
A.1	influxData1.sh	50
A.2	influxData2.sh	51
	APÊNDICE B – QUERIES NA BASE DE DADOS DO INFLUXDB	52
B.1	Matriz de troca de tráfego	52
B.2	Tráfego total agregado	52
B.3	Tráfego total detalhado	52
B.4	Tráfego total por VLAN (ATM x ATB)	52
B.5	Estatística por AS (Destino AS3)	52
B.6	Estatística por AS (Origem AS4)	52
B.7	Estatística por AS (Entrada e Saída dos AS2)	53
B.8	Tráfego total para AS1 (ATM x ATB)	53
B.9	Tráfego total para AS2 (ATM x ATB)	53
B.10	Estatísticas por Endereço MAC	53

1 INTRODUÇÃO

A crescente evolução das tecnologias de redes, aliada à grande redução de custos dos recursos computacionais, motivou a proliferação da Internet pelos segmentos da sociedade. Uma das melhores funcionalidades que a Internet trouxe para as pessoas é a forma de realizar conectividade entre os meios de informação e entre os indivíduos. Porém, a evolução da Internet se deu sem a maturação de protocolos e algoritmos que compõem a infraestrutura de redes, permitindo que surgisse problemas na segurança, infraestrutura e topologia da rede.

Para diminuir esses problemas, surgiram os pontos de troca de tráfego (IXs ou IXP) que é uma solução que permite conexão direta entre as entidades que compõem a Internet, conhecidos como Sistemas Autônomos, ou ASes (*Autonomous Systems*). Um ponto de troca de tráfego busca incentivar a troca e tráfego entre os ASes e otimizar a conexão entre eles, possibilita melhor qualidade, menor custo e maior organização da estrutura de rede regional. Um dos interesses de uma conexão ao IX é o fato de ser possível conectar um AS a todos os outros participantes de um IX através de um único enlace para o mesmo. Hoje, os IXs constituem parte importante da Internet e existe um crescente interesse da comunidade em sua utilização e adesão.

Dada sua importância, os IXs se tornaram uma estrutura muito complexa e de difícil gerência. Um desafio na operação dos IX de menor porte, como o IX.br-MG, é a carência de soluções voltadas para a coleta e exibição de dados estatísticos de seus participantes (ASes). Alguns IX maiores, como o IX.br-PR, já possuem esse serviço de coleta de dados. A ferramenta utiliza o protocolo de amostragem sFlow (*sampled flow*) para coletar dados do IX e geram estatísticas dos membros a partir de uma matriz de tráfego. Essa abordagem possibilita entender melhor as políticas de roteamento adotadas pelos participantes e permite encontrar possíveis problemas de configuração e conexão dos participantes no IX.

1.1 Motivação e Objetivos

Um ponto de troca de tráfego permite um maior controle da rede em relação à entrega do tráfego, acarretando em uma melhor operação da Internet como um todo. Com isso, monitorar o fluxo de dados entre os participantes de um IX pode promover ganhos tanto para os administradores de rede do IX quanto para os seus participantes. De acordo com os fatos mencionados anteriormente, o projeto teve como objetivo geral estudar o IX.br-MG e implementar um protótipo de um serviço de gerência de dados estáticos de seus participantes, atualmente carente deste serviço, baseado nas especificações do protocolo sFlow. Como objetivos específicos, listamos:

- Estudar sobre os pontos de troca de tráfego, mais especificamente do IX.br-MG;
- Estudar as ferramentas de coleta, análise e exibição de dados estatísticos já existentes na literatura;
- Levantar os dados a serem coletados e pesquisar quais estatísticas são úteis para serem exibidas a partir destes dados;
- A partir dos estudos e levantamentos realizados, implementar a coleta de dados proposta, realizar a sua integração com a ferramenta escolhida e propor um modelo de exibição *dashboard* para os dados coletados e processados, melhorando a qualidade do monitoramento de dados atualmente realizado nesse ambiente.

1.2 Contribuição do Trabalho

A implementação do serviço de coleta, análise e visualização dos dados estáticos propôs melhorar a gerência de um IX, promovendo uma melhor visão do tráfego que envolve seus participantes e permitindo encontrar possíveis problemas de conexão entre os membros. Espera-se que o projeto contribua para o planejamento dos requisitos da infraestrutura para atender às demandas dos participantes, possibilite a contabilização detalhada da utilização dos recursos e permita a validação da qualidade de serviço de um IX. Considerando as inúmeras propriedades que compõem essa implementação, foram examinadas a operacionalização de um

IX, assim como a situação e desafios atuais. Além disso, foi feita uma pesquisa sobre gerenciamento de redes analisando tanto a origem dos dados (agentes e coletas) quanto no destino dos dados processados (servidor de análise dos dados).

1.3 Metodologia de Trabalho

O projeto iniciou-se a partir de uma pesquisa exploratória sobre ponto de troca de tráfegos, mais especificamente o IX.br-MG. Foi estudado o que é troca de tráfego, o funcionamento de um IX, sua finalidade, seus órgãos regulamentadores, rotinas dos administradores, infraestrutura, benefícios, dificuldades e problemas atuais. A partir dessa pesquisa, partiu-se para um estudo sobre as técnicas de gerenciamento de redes a fim de levantar as técnicas que podem ser aplicadas ao projeto. Com a definição da técnica de gerenciamento, foi realizado um estudo comparativo das tecnologias disponíveis no mercado para gerar dados (SNMP, NetFlow, IPFIX e sFlow), coleta (IndexDB e Grafite) e visualização dos dados estatísticos (Grafana) no ambiente de um IX. Com toda essa base teórica, implementou-se o protótipo do serviço utilizando as ferramentas escolhidas. Mais precisamente, a implementação do sistema foi constituída de três partes:

- Geração de dados: Informação obtida dos switches do IX;
- Coleta, armazenamento e análise dos dados: comunica com os switches por meio do protocolo sFlow e armazena as informações de fluxo em uma base de dados desenvolvida para esse fim;
- Visualização dos dados: geração e exibição das estatísticas de tráfego a partir das informações de fluxo na base de dados.

1.4 Organização do Texto

No restante do trabalho, discutiremos sobre a base teórica do projeto que foi implementado. O capítulo 2 apresenta os trabalhos relacionados e o estado da arte atual. A seguir, no capítulo 3 realizamos uma breve contextualização dos elementos básicos do trabalho, mostrando um estudo sobre pontos de troca de tráfego, técnicas de gerenciamento de redes e uma pesquisa sobre os principais protocolos de medição de tráfego existente no mercado. No capítulo 4, será discutido a modelagem e as ferramentas que foram aplicadas no projeto, sendo que no capítulo 5, serão apresentadas as estatísticas geradas e os benefícios gerais da sua aplicação. Por fim, no capítulo 6, serão realizadas as conclusões sobre o projeto.

2 TRABALHOS RELACIONADOS E ESTADO ATUAL DA ARTE

Como foi mencionado, alguns pontos de troca de tráfego no Brasil já implementaram o serviço de coleta, análise e visualização de dados estatísticos em seu ambiente. No ano de 2007, o IX.br-PR contava com 13 ASes e utilizou o protocolo de amostragem sFlow para efetuar medições membro a membro em sua infraestrutura. Na época, eram contabilizadas medições SNMP (*simple network management protocol*), que permitia visualizar somente mudanças das tabelas de roteamento BGP (*border gateway protocol*) e status da porta de conexão dos participantes. Com essa limitação, alguns dados eram difíceis de serem coletadas, como a quantidade de tráfego de uma participante X para um participante Y, quantidade de tráfego em determinada VLAN e outros tipos de tráfego. Para contornar essa dificuldade, o protocolo de amostragem sFlow foi adotado pela equipe do IX.br-PR para permitir uma visão geral da rede, antes limitado. O sFlow foi escolhido por ser uma tecnologia aplicável em interfaces de alta velocidade ($> 1\text{Gbps}$) e aplicável nos switches do IX (GRUPO DE TRABALHO DE ENGENHARIA E OPERAÇÃO DE REDES, 2007).

O mecanismo consistia em coletar pacotes *flow sampling* em uma taxa de amostragem 1/512 (coleta de 1 pacote a cada 512 observados) dos switches do IX. A maior vantagem dessa abordagem foi a extração de dados complementares dos switches. Pela técnica *flow sampling* do protocolo sFlow foi possível saber a VLAN de entrada e saída de um certo pacote, permitindo coletar estatísticas de tráfego em uma determinada VLAN. Esses dados foram exportados para uma máquina coletora que armazena temporariamente os pacotes gerados pelos switches. A partir destes dados, foi gerada uma matriz de tráfego (gráfico com medições de tráfego entre cada par de ASes do IX). As linhas e colunas da matriz continham os respectivos ASes do IX e para cada posição desta matriz, era possível visualizar o gráfico de tráfego de bits/pacotes entre os ASes envolvidos. Com esse serviço, foi possível perceber algumas anomalias no tráfego dos ASes, como assimetria de tráfego, diminuição do tráfego trocado, etc. Logo, a medição de tráfego via protocolo sFlow no IX.br-PR permitiu entender as políticas de roteamento adotadas pelos participantes e encontrar problemas que não eram percebidos.

Atualmente, o IX.br-MG compartilha dos mesmos problemas que existiu no IX.br-PR. Assim, objetivamos do mesmo ideal de utilizar o protocolo de amostragem sFlow para prover novas estatísticas de tráfego no ambiente de um IX e melhorar a tomada de decisões dentro do ambiente.

3 CONTEXTUALIZAÇÃO

De uma forma geral, o presente trabalho possui o objetivo explorar os benefícios da coleta de dados de tráfego usando o protocolo de amostragem sFlow no ambiente de um IX, facilitando e simplificando a operação do mesmo. Devido à complexidade e baixa familiaridade da maioria dos leitores com os elementos de um IX e demais particularidades envolvidas no ambiente, esse capítulo apresentará uma visão geral sobre os pontos de troca de tráfego, técnicas de gerenciamento de redes e as principais tecnologias de coleta, análise e visualização de dados de tráfego.

3.1 Troca de tráfego - *Peering*

A Internet consiste em uma rede de redes. A relação entre um usuário doméstico ou corporativo e um provedor de serviço de Internet é chamada de compra de trânsito. O provedor é responsável por transportar os dados do usuário para as demais redes, e vice-versa. Esses provedores que compõem a Internet são chamadas de Sistemas Autônomos (ASes). Os ASes são entidades composta por um conjunto de redes, que possuem controle das políticas de roteamento dentro do seu domínio administrativo. Para se comunicarem e trocarem informações de seus recursos de redes, os ASes utilizam o protocolo de roteamento interdomínio chamado BGP¹. Para a maioria das situações, a compra de trânsito com um provedor é o principal meio de conexão à Internet. Porém, para que um pacote trafegue para outras redes, os grandes provedores de serviços cobram taxas para interligar os ASes menores. Contudo, pode-se identificar ASes em que a comunicação através da rede seja realizada por um enlace físico direto, trocando através dele o tráfego que antes passava pelo provedor. Esse tipo de relação direta de troca de dados é chamada de troca de tráfego ou *peering*.

A figura 1 mostra essa substituição de uma relação de compra de trânsito pela troca de tráfego. As duas instituições participantes da Internet, fazem inicialmente uma conexão através de provedores maiores, pagando a eles pelo tráfego trocado com qualquer outro participante da rede. Caso elas percebam que trocam entre si muitos dados através da Internet, podem

¹ https://pt.wikipedia.org/wiki/Border_Gateway_Protocol

estabelecer uma conexão física direta e passar a trocar tráfego diretamente, como na situação ilustrada no lado direito da figura, o que permite a diminuição do tráfego trocado através dos provedores e a melhora na qualidade da conexão (menor latência).

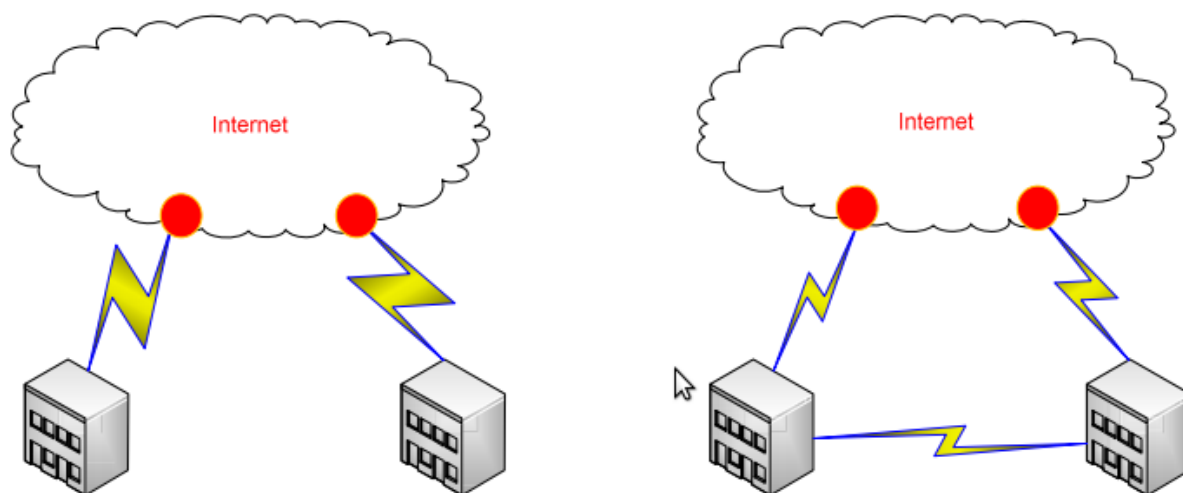


Figura 1. Troca de Tráfego entre ASES
[MOREIRAS, Antonio, GETSHKO, Demi]

Essa relação de troca de tráfego tem caráter colaborativo. Ou seja, consiste em um serviço recíproco, entre as redes envolvidas, e normalmente não envolve pagamentos de uma parte à outra. A troca de tráfego garante benefícios como economia, quando se deixa de pagar ao provedor pelo tráfego, e também melhoria de qualidade, porque conexões diretas são mais rápidas e confiáveis, não sofrendo de prejuízos quando ocorre algum evento, como um ataque de negação, no trânsito Internet.

3.2 Pontos de Troca de Tráfego - Visão Geral

Um ponto de troca de tráfego é um ponto público e central onde diversos ASes de uma determinada região podem se conectar e trocar tráfego entre si. Eles existem para ajudar os participantes da Internet a estabelecer relações de troca de tráfego, reduzindo os custos e potencializando os benefícios dessas relações. Dessa forma, não são necessários vários enlaces distintos para estabelecer relações de troca de tráfego com diferentes redes, mas apenas um enlace de capacidade adequada para o IX. Esse conceito está ilustrado na figura 2.

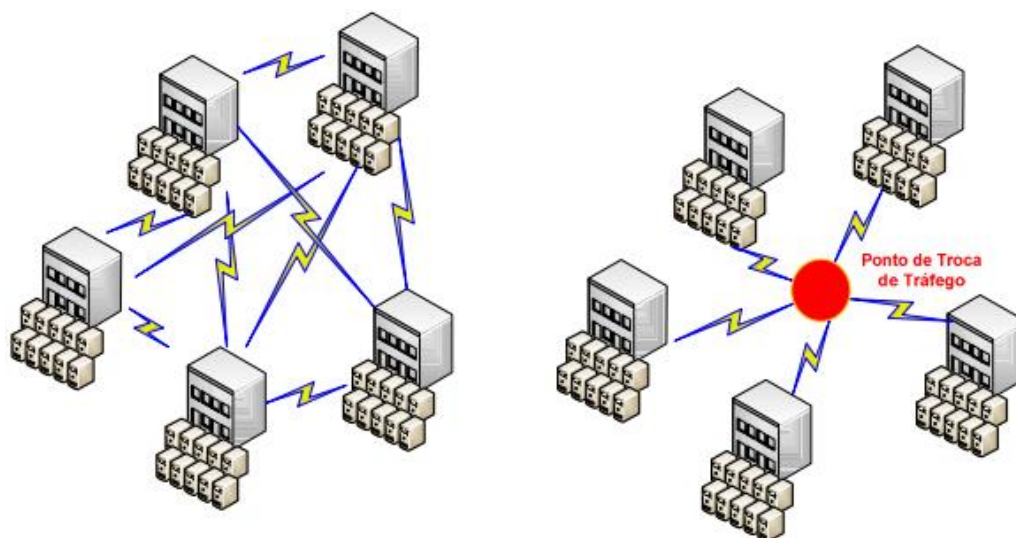


Figura 2. Conexão dos ASes em um IX
[CEPTRO.br, 2015]

Uma vez conectadas, os ASes podem fazer acordos de troca bilaterais (ATB), privados, que podem ter natureza comercial, ou participar do acordo de troca multilateral (ATM), onde todos os membros trocam tráfego entre si em um mesmo domínio de *broadcast*. Relações de compra de trânsito podem também ser estabelecidas através dos IXs, com um ou mais provedores, estabelecendo um ATB entre eles para a troca de tráfego e trânsito Internet, embora isso não seja o objetivo principal de sua existência.

No Brasil, o Comitê Gestor da Internet (CGI.br) lançou mão do projeto PTTMetro (IX.br), como forma de incentivar e apoiar a troca de tráfego regional. O projeto PTTMetro foi criado em meados de 2004, tendo o escopo inicial de construir cinco IXs, em importantes capitais brasileiras, tendo já ultrapassado em muito seus objetivos iniciais [CEPTRO.br, 2016]. Um IX do PTTMetro é composto por vários PIXes, pontos de interconexão de redes comerciais e acadêmicas, interligados entre si, para formar o IX, sendo o PIX responsável pela gerência centralizada, denominado PIX Central. O NIC.br é responsável por instalar os switches e demais equipamentos necessários e da sua administração, tanto no PIX central, como nos demais. Essa infraestrutura é de uso público e gratuito, e não se paga pelo volume de tráfego trocado. O PTTMetro tem hoje participantes importantes, como os principais provedores de banda larga, como Brasil Telecom, Oi, Telefônica, CTBC Telecom, GvT, Net e a Rede Nacional de Pesquisa (RNP). A interação entre os PIXes pode ser visualizada na figura 3.

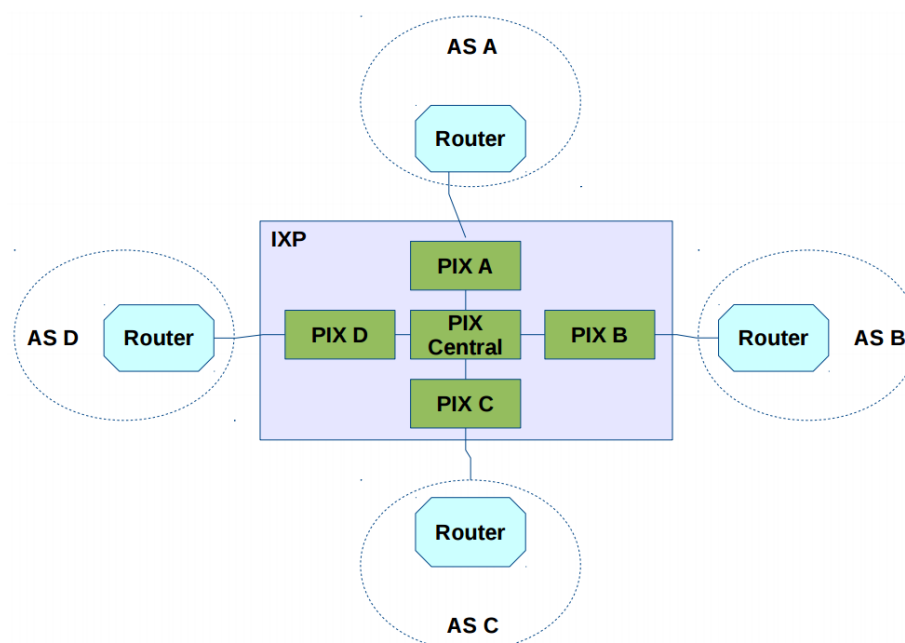


Figura 3. Interação entre PIXes
[GTER,2015]

3.3 Pontos de Troca de Tráfego - Arquitetura

Apesar de sua complexidade, a arquitetura de um IX é simples de se entender, consistindo em um ponto centralizado de conexão onde os ASes membros podem se conectar através de uma matriz de comutação em camada 2 conhecida como *switching-fabric*². Além disso, são configurados servidores de rotas (camada 3) onde os participantes podem estabelecer sessões BGP e alcançar todos os ASes do IX. A arquitetura de um IX, sua estrutura, seus acordos e os seus componentes principais, são mostrados na figura 4.

² https://en.wikipedia.org/wiki/Switched_fabric

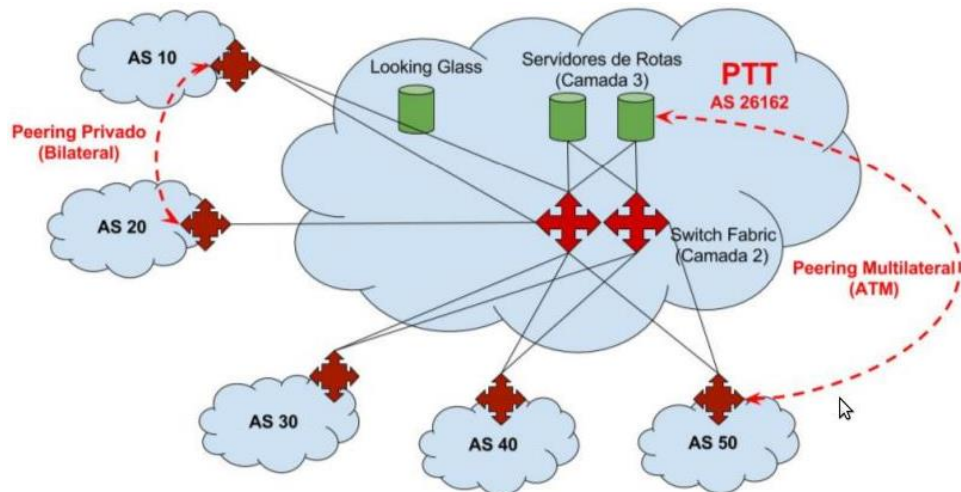


Figura 4. Topologia de rede de um IX
[MARTINS, 2016]

3.3.1 Servidor de Rotas

Um servidor de rotas ou RS (*Router Server*) é um servidor executando um software de roteamento BGP. A principal função de um RS é comunicar-se com todos os ASes e propagar as rotas aprendidas de cada um deles, provendo alcançabilidade entre os ASes.

3.3.2 Looking Glass

Looking Glass é um serviço que permite ao administrador de rede visualizar todas as rotas divulgadas dentro do IX, sem ter acesso físico à estrutura. Recomenda-se que todos os membros de um IX estabeleçam também sessões BGP com o servidor de *Looking Glass*, facilitando a solução de problemas com o roteamento [CEPTRO.br, 2016].

3.3.3 PIXes

Os PIXes são pontos de conexão geograficamente dispersos, espalhados por uma dada região, sendo cada um deles conectados em um PIX Central. Cada PIX possui um ou mais switches na estrutura do IX, cuja função é prover o meio físico de acesso para todos os ASes integrantes. Os PIXes provêm recursos de infraestrutura e, preferencialmente, 2 pares de fibras ópticas até o PIX central para fins de redundância.

3.3.4 Sistemas Autônomos

Um Sistema Autônomo (AS) é um grupo de redes IP, abaixo de uma única gerência técnica e que compartilham uma mesma política de roteamento [CTER, 2015]. No IX, todo participante necessita ser um AS e a troca de tráfego é realizada entre as redes que os diferentes ASes anunciam aos servidores de rotas.

3.4 Pontos de Troca de Tráfego - Tipos de acordos

Podem ocorrer os seguintes acordos de troca de tráfego entre os participantes de um IX:

- **Acordo de Troca de Tráfego Multilateral (ATM):** Para a participação no ATM basta que sejam estabelecidas sessões BGP com servidores de rotas disponíveis. Ao participar do ATM, um participante concorda em trocar tráfego com todos os demais que assim o desejarem em um VLAN compartilhada;
- **Acordo de Troca de Tráfego Bilateral (ATB):** Nesse caso, a administração do IX aloca uma VLAN diferente da usada no ATM e libera seu acesso apenas aos participantes envolvidos no acordo. Podem envolver a troca de tráfego ou a venda de trânsito, ou outros serviços. Esses tipos de acordos entre os ASes participantes podem ser visualizados na figura 4.

3.5 Pontos de Troca de Tráfego - Benefícios

Para entender os benefícios de um IX, suponha uma região onde exista alguns ASes, porém não há um IX, esses ASes estarão trocando o tráfego local, via Internet. Isso pode significar longas distâncias percorridas pelos pacotes. Com a criação de um IX regional, os ASes podem conectar-se diretamente. Isso significa redução da latência, maior tolerância a falhas e redução de custos. Os principais interesses econômicos das empresas de telecomunicações na conexão ao IX são [GTER, 2013]:

- Redução dos custos de interconexão;
- Provisionamento de *Last/First Mile* (cobrança) para conexão ao PTTMetro;
- Serviços IP de Interconexão;
- Utilização de VLANs dedicadas para prover isolamento lógico L2 para trânsito Internet (IPv4 e IPv6), Backup, Storage, VoIP, etc;
- Transporte entre Localidades do PTTmetro;
- Hospedagem de Pontos de Interconexão (PIX);

Assim, um IX permite que a entrega do tráfego ocorra o mais próximo possível do seu destino, melhorando o desempenho e qualidade para seus clientes e a operação da Internet como um todo.

3.6 Projeto PTTMetro

O PTTMetro é um projeto do Comitê Gestor da Internet no Brasil (CGI.br) sem fins lucrativos que promove e cria a infraestrutura necessária (Ponto de Troca de Tráfego – IX) para a interconexão direta entre os ASes que compõem a Internet Brasileira. O Núcleo de Informação e Coordenação do Ponto BR (NIC.br) é responsável pelo fornecimento dos equipamentos necessários (switches, servidores, etc), bem como pela sua operação, manutenção e suporte dos PIXes centrais, como nos demais. A atuação do PTTMetro volta-se às regiões metropolitanas

no País que apresentam grande interesse de troca de tráfego Internet. São características fundamentais para a implementação adequada de um PTTMetro [GTER, 2013]:

- Neutralidade - independência de provedores comerciais;
- Qualidade - troca de tráfego eficiente;
- Baixo custo das alternativas, com alta disponibilidade;
- Matriz de troca de tráfego regional única.

O projeto é tido como um grande sucesso e hoje o NIC.br opera 26 pontos de troca de tráfego no Brasil. Recentemente ultrapassou a meta de 1,6 Tbps de troca, o que o incluiu em um seleto grupo de IXs mundiais cujo troca ultrapassou esse valor. Não há custo para a porta do switch, ou seja, um participante não paga ao NIC.br para conectar-se ao IX, independentemente da capacidade da porta. O PTTMetro incentiva a maior utilização de banda possível dentro de sua estrutura, e o NIC.br encarrega-se dos upgrades de equipamentos quando necessários. O PIX Central é uma entidade neutra, sendo administrado pelo próprio NIC.br ou pelos Pontos de Presença da RNP (PoPs-RNP). No entanto, a maioria dos demais PIXes são comerciais e podem cobrar pelo acesso ao IX. A figura 5 traz uma síntese da distribuição dos IXs no território brasileiro (atuais e em estudo).



Figura 5. Localidades atuais e em estudo do IX.br

[IX.br, 2016]

O objetivo principal para a criação de localidades do PTTMetro é permitir que o tráfego local fique no próprio local de origem e assim evitar a interconexão remota. O CGI.br não tem planos de interconectar as localidades do PTTMetro e competir com as operadoras de Telecomunicações.

3.6.1 Regras

Algumas regras devem ser seguidas pelos ASes conectados ao IX [MARTINS, 2016]:

- Possuir e operar um sistema autônomo;
- Acordo multilateral de tráfego via RS, ou relações bilaterais diretas;
- Implementar protocolo de roteamento exterior BGP4;
- Dentro do ambiente do IX, são permitidos apenas quadros Ethernet do tipo IPv4 (0x0800), ARP (0x0806) e IPv6 (0x86dd);
- Estabelecer acordos de troca de tráfego com outros participantes;
- É proibido utilizá-las para passar tráfego interno entre as conexões do mesmo AS;
- É permitido utilizar a mesma porta para a conexão de múltiplos ASes, em uma modalidade chamada de CIX (*Channel to IX*) no IX.br, onde será utilizado tags de VLANs (IEEE 802.1Q) para realizar o isolamento lógico;
- É permitido apenas um endereço MAC por participante, cadastrado no momento da ativação;
- Caso anuncie prefixos de outros participantes é obrigatório marcar NEXT_HOP_SELF;
- Tráfego *broadcast* deve estar limitado exclusivamente a resolução ARP;
- Participantes não podem apontar rota default ou se utilizar de recursos de outros sem a devida autorização.
- O AS deve concordar com os termos de condições de uso gerais do IX.

3.6.2 Infraestrutura

Sobre a infraestrutura do IX [MARTINS, 2016], tem-se:

- Cada PIX consiste de um ou mais switches L2 interligados aos dos outros PIXes através de conexões de alta velocidade;
- Cada PIX precisa possuir conexão redundante com o resto do IX;
- Os sistemas autônomos que desejam trocar tráfego no IX devem conectar-se à um dos PIXes;
- Normalmente todo PIX está localizado em um datacenter ou estrutura semelhante, com diversos recursos de redundância e resistência à falhas;
- O participante ao conectar-se à um PIX particular, normalmente paga à este uma taxa de conexão (*golden connection*), que não depende da banda trafegada;
- Apesar de cada PIX ser potencialmente de uma empresa diferente, os equipamentos utilizados na infraestrutura de rede do IX são fornecidos e administrados exclusivamente pelo IX.br;
- Normalmente o custo das conexões entre PIXes, compostas por uma ou mais fibras apagadas, é rateado e/ou negociado entre as pontas.
- No nível de enlace a engenharia de tráfego do IX consiste apenas na gerência de rotas redundantes entre equipamentos e utiliza protocolos simples e agregação (802.3ad). Por ser uma rede em camada 2, a engenharia de tráfego em L3 pode ser considerada nula.

3.6.3 Processos de Rotinas

No dia a dia da equipe do IX.br, há várias tarefas a serem realizadas, incluindo desde a ativação de novos participantes até a gerência do ambiente. Entre as solicitações dos participantes, podemos citar a ativação de novas conexões, problemas de conectividade, alteração de endereço MAC, solicitação de filtros, VLANs bilaterais, aumento de prefixos, upgrade de porta e migração do AS para outro PIX da região. Uma das tarefas mais demoradas é a ativação de novos participantes, onde o AS a ser conectado passa por um processo de

validação conhecido como quarentena, período de tempo no qual o participante estará em uma área isolada do IX, sem comunicação com os demais ASes. [MARTINS, 2016].

Além das solicitações dos participantes, há também algumas tarefas administrativas a serem realizadas pela administração do IX. Entre elas, os filtros no ATM para proteger de abusos como utilizar o IX para trocar tráfego consigo mesmo, ou seja, impedir que o AS utilize o IX para prover conectividade entre seus pontos de presença locais.

3.6.4 Dificuldades e Problemas

Atualmente, um problema de infraestrutura que ocorre nos IXs de menor porte, como o IX.br-MG, é a carência de soluções voltadas para a coleta e exibição dos dados de seus participantes (ASes). Alguns IX maiores, como o de IX.br-PR, possuem esse serviço de coleta de dados. Esses serviços usam protocolos de monitoramento de pacotes, como os protocolos sFlow, IPFIX, SNMP, para saber o que acontece dentro da rede. Para visualizar os dados, o serviço utiliza ferramentas de visualização de séries temporais como Grafana, Graphite, sFlow-RT e Nfsen. A figura 6 mostra um exemplo de uma visualização de tráfego entre dois ASes no IX.br-MG, utilizando o tradicional protocolo SNMP.

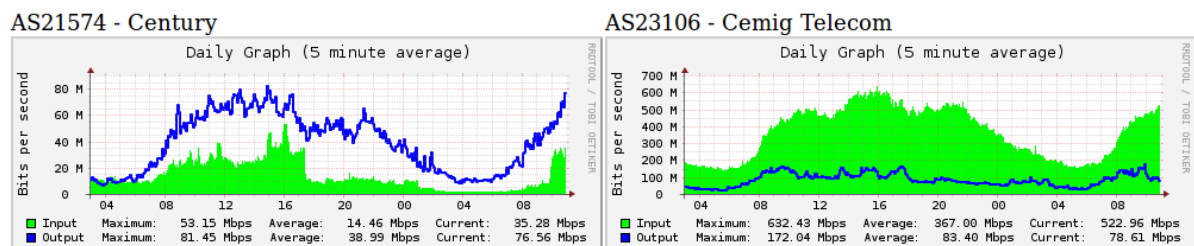


Figura 6. Tráfego de entrada e saída entre dois ASes do IX.br-MG

Hoje, é permitido utilizar a mesma porta para a conexão de múltiplos ASes, em uma modalidade chamada de CIX no IX. Porém, as estatísticas de tráfego no IX é coletada via SNMP, são realizadas por porta, de forma que quando vários ASes chegam juntos em uma mesma porta (CIX), não é possível coletar estatísticas individuais na porta de conexão do CIX no PIX. A solução existente hoje consiste em separar cada VLAN de entrada em portas distintas para contabilizar as estatísticas individualmente em cada porta. Essa solução não é boa, levando

a uma subutilização dos recursos de hardware e da capacidade das portas. Além disso, o mesmo problema acontece nos acordos bilaterais (ATB), porque o participante (AS) chega em uma porta e troca tráfego através das ATBs e do ATM. Como a estatística é por porta, não é possível separar o tráfego de cada ATB e do ATM para contabilizar e gerar as estatísticas com um maior detalhamento.

Levando em consideração os fatos mencionados no capítulo 2, é possível realizar a coleta do tráfego de dados de cada participante individualmente na mesma porta, com o uso do protocolo sFlow, evitando a subutilização e permitindo uma coleta com um maior nível de granularidade e detalhes dos dados dos participantes (AS).

3.7 Gerenciamento de Redes

Esta seção apresenta as alternativas para o gerenciamento de redes e as principais metodologias e protocolos. Será destacado o protocolo tradicional SNMP e o monitoramento baseado em fluxos de tráfego, abordando os conceitos que permeiam sua arquitetura e seus principais protocolos: NetFlow, IPFIX e sFlow.

3.7.1 Gerência de Redes

As redes de computadores atuais são compostas por uma grande variedade de dispositivos que devem se comunicar e compartilhar recursos. Na maioria dos casos, a eficiência dos serviços prestados está associada ao bom desempenho dos sistemas da rede. Para gerenciar esses sistemas e as próprias redes, um conjunto eficiente de ferramentas de gerenciamento automatizadas é necessário, sendo fundamental a utilização de técnicas padronizadas para a correta representação e o intercâmbio das informações obtidas.

As principais metas do gerenciamento de redes são redução dos custos operacionais da rede, redução do congestionamento da rede, aumento da flexibilidade de operação e integração, maior eficiência e facilidade de uso da rede [MENEZES, 1998]. O gerenciamento de redes está associado ao controle e ao monitoramento do uso dos recursos no ambiente da rede. O

monitoramento é a função que faz o acompanhamento de todas as atividades da rede no sentido de contabilizá-los, e o controle é a função que permite que os ajustes sejam feitos visando melhorar o desempenho da rede. As tarefas básicas desta gerência são [PINHEIRO, 2006]:

- Obter as informações da rede;
- Tratar as informações para diagnosticar possíveis problemas;
- Propor soluções para os problemas.

O gerenciamento de redes de computadores envolve monitoração e controle de diferentes elementos de hardware e software, dentre os quais podem ser citados [MENEZES, 1998]:

- Componentes dos computadores, tais como dispositivos de armazenamentos, impressoras, etc;
- Componentes de interconexão e conectividade, tais como roteadores, hubs, switches, etc;
- Sistemas operacionais, softwares de aplicação, ferramentas de desenvolvimento, etc.

Um sistema de gerenciamento é composto de uma coleção de ferramentas para monitorar e controlar a rede, como os elementos gerenciados, agentes, gerentes, bancos de dados, protocolos para troca de informações de gerenciamento, interfaces para programas aplicativos e interfaces com o usuário. A arquitetura geral dos sistemas de gerência de redes apresenta quatro componentes básicos [FILHO, 2012]:

- Agentes: são os elementos gerenciados e são implementados por um software que permite que o monitoramento e controle do equipamento.
- Gerentes: são estações de gerência que interage diretamente com os agentes para monitorá-los e gerenciá-los.
- Protocolo de Gerência: é a interface entre a estação de gerência e o agente por meio de uma normatização das operações de monitoramento (leitura) e controle (escrita).
- Informações de Gerência: são os dados que podem ser referenciados em operações do protocolo de gerência, que podem ser estáticos, dinâmicos e estatísticos.

A monitoração consiste na observação de informações relevantes ao gerenciamento, que podem classificadas em três categorias:

- Estática: caracteriza os elementos na atual configuração, como o número e identificação das portas em um roteador;
- Dinâmica: relacionada aos eventos na rede, como a transmissão de um pacote;
- Estatística: pode ser derivada de informações dinâmicas como a média de pacotes transmitidos por unidade de tempo em um determinado sistema.

A informação de gerenciamento é coletada e armazenada por agentes e repassada para um ou mais gerentes. Duas técnicas podem ser utilizadas na comunicação entre agentes e gerentes: *polling* e *event-reporting*. A técnica de *polling* consiste em uma interação do tipo solicitação/respostas entre um gerente e um agente. O gerente pode solicitar a um agente (para o qual ele tenha autorização), o envio de valores de diversos elementos de informação. O agente responde com os valores constantes em sua base de dados de informações MIB (*Management Information Base*). Na técnica de *event-reporting*, a iniciativa é do agente. O gerente fica na escuta, esperando pela chegada de informações. Um agente pode gerar um relatório periodicamente para fornecer ao gerente o seu estado atual [FILHO, 2012]. A periodicidade do relatório pode ser configurada previamente pelo gerente. Um agente também pode enviar um relatório quando ocorre um evento significativo ou não usual. A base de informação gerencial (MIB) é o nome conceitual para a informação de gerenciamento, incluindo os objetos gerenciados e seus atributos, operações e notificações. A figura 7 abaixo mostra uma arquitetura genérica de gerenciamento de redes.

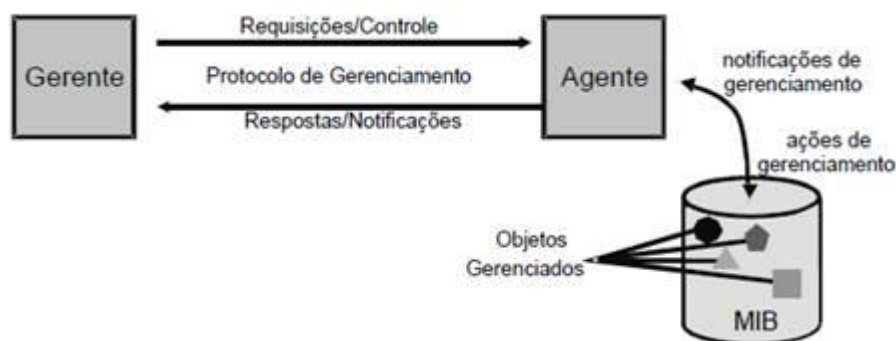


Figura 7. Arquitetura básica de gerência de redes

[FILHO, 2012]

A ampla gama de soluções desenvolvidas para o gerenciamento de redes trouxe a necessidade de criar protocolos para o desenvolvimento de monitoramento de redes. Os protocolos de monitoramento de redes descrevem um formato para o envio de informações entre os equipamentos de redes monitorados e as máquinas responsáveis pelo armazenamento de tais informações. As tecnologias mais conhecidas no monitoramento de redes são baseadas no modelo TCP/IP, modelo SNMP e redes baseadas no modelo (OSI), utilizam o protocolo CMIP. Entre os dois protocolos, o SNMP é o que obteve o maior sucesso, pois baseia-se no fato de ter sido o primeiro protocolo de monitoramento não proprietário. Será especificado na próxima seção a família de especificações do *Simple Network Management Protocol* (SNMP), uma vez que ele é o mais utilizado atualmente nos IXs, porém limitado para o ambiente.

3.7.2 Protocolo SNMP

SNMP é o protocolo padrão para monitoramento e gerenciamento de redes. O seu desenvolvimento teve continuidade e a versão 1.0 do SNMP foi publicada em maio 1991, tornando o SNMP um padrão de fato, especificado inicialmente na RFC 1067 (agosto/1988), evoluindo depois para as versões SNMPv1 (RFC 1157), SNMPv2 (RFC 1901) até chegar ao SNMPv3 (RFC 2571). Desenvolvido para facilitar a troca de informações de monitoramento entre ativos de redes, o protocolo SNMP pertence à camada de aplicação e está especificado na *Request for Comments* (RFC 1157) [FILHO, 2012].

O SNMP é o protocolo mais utilizado em gerenciamento de redes e permite que uma ou mais máquinas na rede sejam designadas como gerentes de rede. Esta máquina recebe informações de todas as outras da rede, chamadas de agentes, e através do processamento destas informações, pode gerenciar toda a rede e detectar facilmente os problemas ocorridos. As informações coletadas pela máquina gerente estão armazenadas nas próprias máquinas da rede (MIB). Nesta base estão gravadas todas as informações necessárias para o gerenciamento deste dispositivo, através de variáveis que são requeridas pela estação gerente [DIAS, 2008].

Como exibido na figura 8 abaixo, o gerente é um programa que é executado em um servidor e, mediante a comunicação com um ou mais agentes, obtêm e armazena informações de monitoramento referentes a cada um dos ativos que hospedam o agente. Para obter essas

informações é utilizada uma técnica chamada *pooling*, que é uma interação do tipo pergunta-resposta entre gerente e agente.

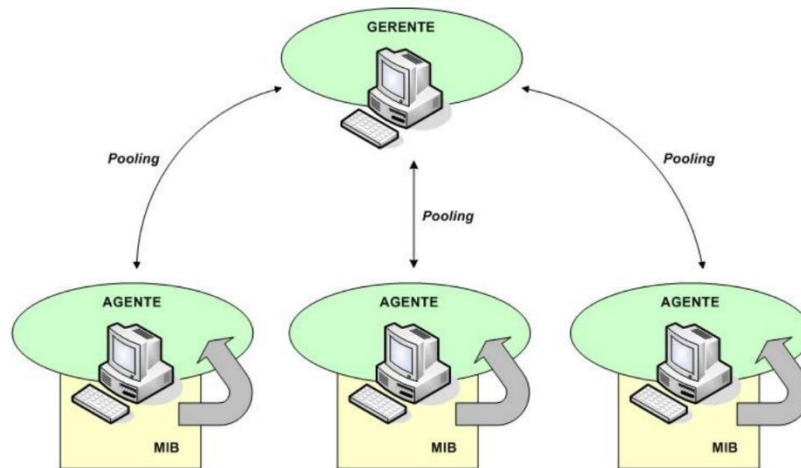


Figura 8. Funcionamento do protocolo SNMP
[DIAS, 2008]

Implementações básicas do SNMP possibilitam monitorar e isolar falhas. As aplicações mais avançadas permitem gerenciar o desempenho e a configuração da rede. Essas aplicações, geralmente, incorporam alarmes e menus para facilitar a interação com o profissional que está monitorando os ativos de redes. Apesar de ser o protocolo mais usado para saber o que acontece dentro de ativos de redes e serviço, o protocolo SNMP possui limitações, como as que seguem abaixo [SANTOS, 2016]:

- Falta de segurança;
 - Esquema de autenticação trivial;
 - Limitações no uso do método SET;
- Ineficiência
 - Esquema de eventos limitado e fixo;
 - Operação baseada em *pooling*;
 - Comandos transportam poucos dados;
- Falta de funções específicas
 - MIB com estrutura fixa;
 - Falta de comandos de controle;
 - Falta de comunicação entre gerenciadores;
- Não confiável;

- Baseado em UDP/IP;
- *Traps* sem reconhecimento.

Em redes extremamente grandes, como um IX, a utilização do SNMP não é recomendada para coleta de dados de tráfego devido à limitação de performance do *pooling*, uma vez que a probabilidade de erros e ruídos acontecerem aumenta.

3.7.3 Monitoramento de tráfego

Tráfego é a troca de dados entre duas entidades da rede. A função de monitoramento do gerenciamento de rede pode ser classificada como ativo e passivo. O monitoramento ativo é executado pela inserção e análise de pacotes de teste na rede. Nesta técnica a quantidade de dados armazenados não é considerável, em contrapartida, o desafio é adequar o volume de pacotes inseridos para sucessão dos testes e atingimento das métricas desejadas sem que se interfira no desempenho e alocação excessiva de recursos. Por outro lado, o monitoramento passivo analisa os pacotes que estão trafegando na rede sem interferir no fluxo de pacotes e consequentemente no desempenho da rede, produzindo um substancial volume de dados coletados que será a base pelo qual a análise se procederá. O grande desafio dessa abordagem é conseguir restringir a quantidade de dados coletados, armazenando somente as informações necessárias [COUTO, 2016].

3.7.3.1 Monitoramento baseado em fluxos de tráfego

Existem diversas tecnologias disponíveis para medir o tráfego com medição passiva. Uma forma é o monitoramento do tráfego através do armazenamento dos fluxos da rede. Um fluxo pode ser definido como um conjunto de pacotes IP passando por um ponto de observação da rede durante um certo intervalo de tempo, em que todos os pacotes ditos pertencentes a esse fluxo possuem um grupo de propriedades em comum, como um mesmo endereço de origem e destino, mesma porta de origem e destino. Um pacote é definido como pertencente a um fluxo,

se ele satisfaz completamente todas as propriedades definidas para esse fluxo. Essas propriedades, como mesmo protocolo, porta de origem, porta de destino, endereço de origem e endereço de destino, definirão cada fluxo para um ponto de observação. O monitoramento baseado em fluxos de tráfego facilita a quantificação e a qualificação do tráfego, sem que haja a necessidade de analisar cada interface de rede do segmento e cada pacote que passa por esse segmento individualmente [SANTOS, 2007].

Sistemas de monitoramento de fluxo geralmente envolve três entidades: medidores, um coletor e um sistema de análise. Os medidores são dispositivos que têm a funcionalidade de capturar os pacotes dos tráfegos do segmento da rede, identificar os seus fluxos através do rastreamento das conexões e exportar um agrupamento de fluxos a outro dispositivo denominado coletor. O medidor normalmente é um equipamento da infraestrutura da rede (switch, roteador e ou firewall) capaz de operar as funcionalidades descritas por meio dos protocolos de gerência de fluxos. O medidor deve montar um registro de informações sobre as propriedades aferidas durante a medição (número de pacotes que compõem o fluxo, tamanho desse fluxo em bytes) e propriedades características ao fluxo (IP de origem, IP de destino, porta de origem, porta de destino). Adicionalmente, os registros de fluxo podem incluir a criação de novos registros, o cálculo de dados estatísticos para cada um dos fluxos, a derivação de propriedades desses fluxos e remoção desses registros. O coletor possui a funcionalidade de receber os encaminhamentos dos medidores e armazenar de forma persistente esses dados, comumente em discos físicos. O sistema de análise deve ser capaz de entender o formato dos arquivos gerados pelo coletor e acessá-los como base, para a produção de estatísticas que auxiliem a gestão dos recursos da rede [COUTO, 2016].

O monitoramento do tráfego de rede baseado no conceito de fluxos foi originalmente desenvolvido pela empresa CISCO Systems, através do protocolo proprietário NetFlow. Na versão 9, o NetFlow trouxe o conceito de definição de campos flexíveis baseado em modelos definidos diretamente pelos usuários. Este conceito, bem como todas as definições do protocolo NetFlow, foi seguido e aprimorado pelo protocolo aberto IPFIX, definido pelo grupo de trabalho IETF. Paralelo ao NetFlow e ao IPFIX, o protocolo sFlow surgiu como alternativa para o monitoramento baseado em ambientes de volume de tráfego extremamente altos pois a medição por amostragem difere do método de agregação de fluxo de tráfego utilizado pelo NetFlow e conseqüentemente pelo IPFIX. Nas próximas seções, será abordada as questões relacionadas aos protocolos de monitoramento de fluxos, em seus aspectos de: projeto e

arquitetura de um sistema de coleta de fluxos, formas de comunicação entre coletores e agentes, características do protocolo e capacidades de amostragens.

3.8 NetFlow

O NetFlow é um protocolo aberto, desenvolvido pela Cisco para coletar a informação de tráfego IP que passa pelos equipamentos desenvolvidos por esta empresa. Roteadores e switches que suportam o protocolo podem coletar estatísticas de tráfego IP em todas as interfaces onde o NetFlow está habilitado e depois exportar essas estatísticas como registros através de pacotes UDP para um coletor [OPSERVICES, 2016]. O protocolo define um fluxo IP como uma sequência de pacotes com um grupo de atributos em comum. Esses atributos são definidos pela combinação dos seguintes campos, denominados campos-chave:

- Endereço IP da origem;
- Endereço IP de destino;
- Porta de origem;
- Porta de destino;
- Tipo de protocolo na camada 3;
- Tipo de serviço;
- Entrada na interface lógica.

O protocolo é composto por três componentes: o Cache NetFlow, o coletor de fluxo e o analisador de dados, conforme a figura 9. Todos os pacotes com mesmos campos-chave são agrupados em um único fluxo, contabilizando para este fluxo o número de pacotes e o total de bytes. Todas essas informações são então agregadas e armazenadas em uma base de dados chamada NetFlow Cache [CISCO, 2012], conforme ilustrado pela figura 9.

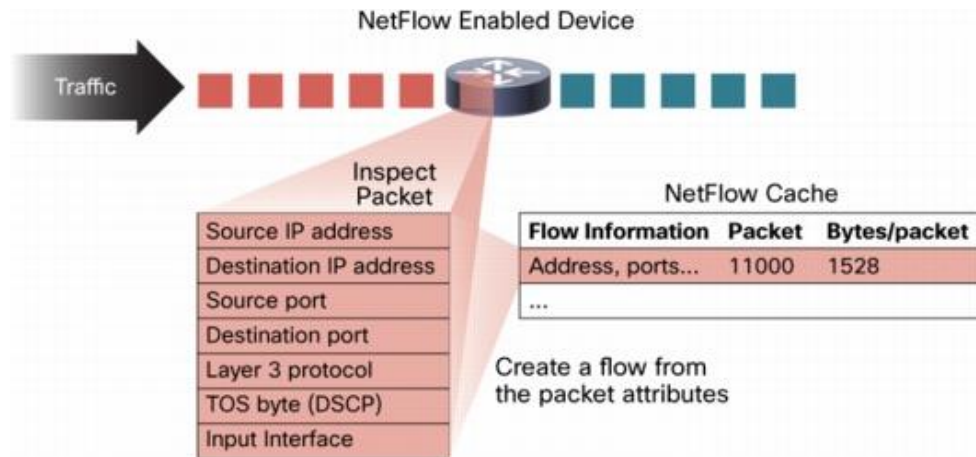


Figura 9. Criação de fluxos no cache NetFlow.

[CISCO, 2012]

A partir da aquisição dessas informações, o dispositivo de rede usa um mecanismo, chamado *NetFlow Exporter*, para enviar todas as informações ao coletor NetFlow. O coletor normalmente é um servidor responsável pelo armazenamento e análise dos pacotes de informações de fluxo. Para isso, o *NetFlow Exporter* faz uso de *templates*, elementos que especificam a estrutura e semântica do grupo de informações que precisam ser enviadas ao coletor. O uso de *templates* permite que novos campos possam ser adicionados ao registro de fluxo sem que se modifique a estrutura dos registros, fazendo com que novos atributos possam ser incorporados ao protocolo mais rapidamente.

A partir do uso de *templates* do protocolo NetFlow, torna-se possível o desenvolvimento de protocolos com os mais diversos fins, onde a fácil expansibilidade e adaptabilidade sejam desejáveis e por ter sido desenvolvido pela Cisco possui boa aceitação no mercado. Porém, o fato de ser exclusivamente adotada por equipamentos Cisco dificulta o seu uso para o gerenciamento total de uma rede.

3.9 IPFIX

Com o crescimento da popularidade da gerência de redes através de fluxos, o grupo IETF decidiu conduzir um estudo sobre os protocolos baseados em fluxos existentes para definir um padrão universal. O protocolo IPFIX foi baseado no NetFlow da Cisco, também conhecido como NetFlow versão 9. O desenvolvimento do IPFIX iniciou-se em 2002, e através

do padrão RFC 3917, foram definidos os requisitos que norteou o grupo de trabalho na confecção do novo protocolo. Dentre as diversas definições da norma RFC 3917, os requisitos de geração dos fluxos devem ser analisados sob os seguintes aspectos:

- Os fluxos devem ser estabelecidos em pacotes que não são criptografados, aonde os dados de todos os campos do cabeçalho estão disponíveis para análise;
- A identificação do sentido dos fluxos deve ser baseada quanto à entrada de pacotes nos sensores pelas interfaces de entrada e saída;
- A geração dos fluxos é definida com base em alguns campos do cabeçalho (Versão do endereço IP; IP origem/destino; Tipo de protocolo; Portas);
- O modelo de informação para exportação dos fluxos deve ser extensível e expansível;
- A transferência dos fluxos deve incluir mecanismos de confiabilidade, controle de congestionamento e segurança;
- O processo de exportação dos fluxos deve suportar os modos de solicitação e encaminhamento (*pull/push*), dentre outros.

Entre as principais diferenças entre o IPFIX e o NetFlow, destaca-se [COUTO, 2012]:

- O NetFlow foi projetado para utilizar o protocolo UDP na camada de transporte, enquanto que o IPFIX necessita garantir a entrega de seus dados, especificando o *Stream Control Transmission Protocol* (SCTP) como seu protocolo padrão;
- Os elementos que transportam as informações sobre os fluxos padronizados pelo IETF precisam ser enviados com um identificador que defina qual protocolo o fluxo é originado, diferente dos elementos não definidos pelo IETF, como os do NetFlow;
- Existem campos diferentes entre os cabeçalhos do NetFlow e do IPFIX e em alguns casos, campos que são usados em ambos os protocolos, mas que podem assumir valores distintos;
- *Templates* de opções de controle possuem especificações distintas entre os protocolos;
- O campo tamanho do pacote é tratado de forma distinta entre os dois protocolos;
- O protocolo NetFlow possui um indicador de *timestamp* extra em seu cabeçalho, inexistente no IPFIX, que indica qual foi a última reinicialização que o processo de exportação dos dados sofreu.

O IPFIX assume a estrutura geral do formato de exportação do protocolo NetFlow v9, ou seja, traz consigo a estrutura flexível e escalável de definições abarcadas pelos conceitos de: Modelo do conjunto de fluxos (*Template FlowSet*); Opções do modelo do conjunto de fluxos (*Options Template FlowSet*) e o conjunto de dados de fluxos (*Data FlowSet*), conforme ilustrado pela figura 10.

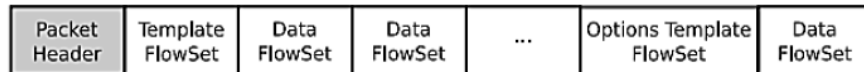


Figura 10. Formato de exportação do IPFIX.

[KREJCÍ, 2009]

A arquitetura IPFIX é formada por dois elementos básicos: o dispositivo IPFIX e o coletor. É considerado um dispositivo IPFIX todo aquele elemento que realiza pelo menos um processo de exportação de dados através do protocolo IPFIX. Esse processo se baseia no envio, em direção a um ou mais coletores, de um registro de fluxo, gerado a partir de um ou mais processos de medição. O processo de medição consiste na captura do cabeçalho de cada pacote que passam pelo seu domínio de observação, a marcação do seu tempo (*timestamping*), a amostragem e a classificação desse elemento, visando a manutenção dos registros de fluxo [SANTOS, 2007].

O domínio de observação é um conjunto de pontos de observação para os quais as informações de fluxo podem ser agregadas por um processo de medição. Cada domínio de observação possui um identificador exclusivo ao processo de coleta, usado para identificar as mensagens IPFIX geradas. Por sua vez, coletor é todo dispositivo que recebe registros de fluxo de um ou mais dispositivos IPFIX. Esse elemento pode processar os registros de fluxo ou armazená-los, entretanto essas ações não fazem parte do escopo do IPFIX. A figura 11 mostra cada um desses elementos.

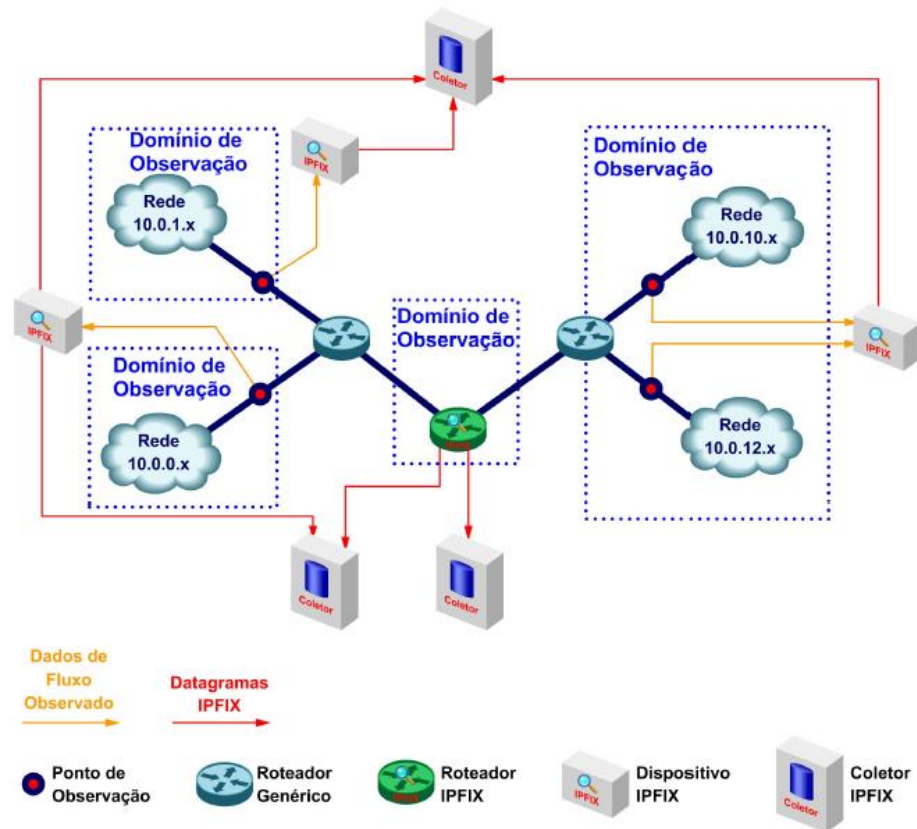


Figura 11. Arquitetura do IPFIX

[SANTOS,2007]

O princípio básico do protocolo IPFIX, comum ao NetFlow, é o uso de *templates* na definição dos registros de fluxo. Conforme visto anteriormente, o dispositivo IPFIX envia ao coletor não apenas as informações sobre os fluxos (registros de fluxo), mas também informação sobre o processo de medição como um todo, referenciadas como informações de controle. Todas essas informações irão compor os pacotes do protocolo IPFIX.

3.10 sFlow

O protocolo sFlow, ou *sampled flow*, é um mecanismo para captura de dados de tráfego em redes roteadas ou comutadas capaz de usar a tecnologia de amostragem para capturar estatísticas do fluxo de tráfego, especificado no RFC 3176. Por esse motivo, o protocolo é indicado às redes de alta velocidade (redes Gigabit ou superior) e redes com grande número de

agentes de medição necessitando da medição de amostragem para a sumarização dos dados a serem tratados.

O monitoramento passivo baseado em amostragem possui as seguintes características: precisão no monitoramento de redes de alta performance, através do ajuste dinâmico nos parâmetros das técnicas de amostragem; escalabilidade, capacidade do sistema gerenciar inúmeros agentes de um ponto centralizado e baixo custo de implementação [SFLOW, 2003].

A arquitetura do protocolo sFlow consiste em agentes e coletores. Os agentes são embarcados em switches ou roteadores e possuem a função de monitorar o tráfego de rede, usando a amostragem na captura dos pacotes, e enviar os dados estatísticos para o coletor. O coletor consiste em uma aplicação de software que armazena os dados dos agentes sFlow em discos físicos e analisa esse tráfego, gerando as métricas necessárias para o gerenciamento. A arquitetura do protocolo pode ser visualizada na figura 12.

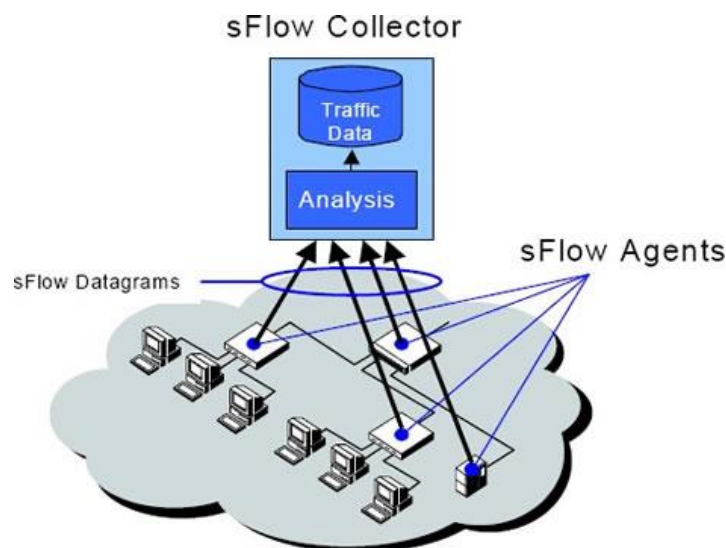


Figura 12. Arquitetura sFlow
[REESE, 2007]

O agente sFlow utiliza duas técnicas de amostragem:

- *Flow Sampling*: baseado na amostra de pacotes, usado para obter informações do conteúdo do pacote como protocolos e etc.
- *Counter Sampling*: baseado na amostra de tempo, usado para obter estatísticas de interfaces.

Diferente dos protocolos NetFlow e IPFIX, os agentes sFlow não coletam todo o tráfego. O protocolo sFlow coleta amostras, tipicamente um em cada 100 pacotes (o administrador especifica essa taxa de amostragem) e envia esse pacote inteiro para o coletor [OPSERVICES, 2016]. Este tipo de amostragem não fornece um resultado preciso, mas fornece um resultado com exatidão quantificáveis. Um fluxo é definido pelo protocolo sFlow como todos pacotes que são recebidos em uma interface do switch ou roteador e são enviados para outra interface.

Os datagramas sFlow são enviados pelos agentes para o coletor por uma porta específica (padrão é 6343) como um pacote UDP, conforme figura 13. A falta de confiabilidade no mecanismo de transporte UDP não afeta significativamente a precisão das medidas obtidas a partir de um agente sFlow. Se as amostras são perdidas, novos valores serão enviados no próximo intervalo de consulta. A perda de amostras de fluxo de pacotes é uma ligeira redução na taxa de amostragem efetiva. Cada datagrama fornece informações sobre cabeçalhos do pacote, endereço de origem e destino de pacotes, portas de origem e destino, VLAN, destino de AS Path, estatísticas de interface, etc.

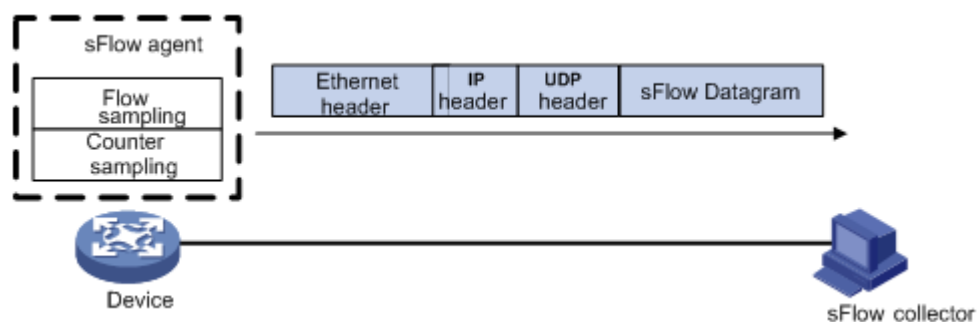


Figura 13. Diagrama do datagrama sFlow
[H3C,2016]

O protocolo sFlow tem sido implementado em uma ampla gama de fabricantes de switches e roteadores de rede. Estas aplicações oferecem uma variedade de soluções como controle de congestionamento, criação de perfil de rotas, análise de segurança de auditoria e contabilidade para o faturamento.

4 PROJETO

Este capítulo mostra como ocorreu o desenvolvimento do protótipo do sistema de coleta, análise e visualização de dados estatísticos aplicado ao ambiente de um ponto de troca de tráfego baseado nas especificações do protocolo sFlow. O protocolo foi escolhido pois é uma solução de baixo custo e escalável, que utiliza técnica de medição de fluxo de tráfego por amostragem, ideal para ambientes de alto volume de tráfego como um IX. Por fim, será destacado cada um dos elementos que formam o sistema nas seções subsequentes.

4.1 Modelagem e prototipação do ambiente

O seguinte projeto de monografia teve como objetivo geral estudar os pontos de troca de tráfego e implementar um serviço de gerência de dados estatísticos de seus participantes baseado nas especificações sFlow. Essa solução foi baseada no ambiente do IX.br-MG que atualmente é carente deste serviço. O desenvolvimento do protótipo foi realizado em uma máquina virtual instalada em uma máquina física com processador Intel Core i3, 8Gb de RAM e Ubuntu Desktop 14.04 LTS. O servidor consiste em uma Máquina Virtual chamada “wall-ptt” (ip 150.164.8.26) com 2 CPUs lógicas, 4Gb de RAM, 32Gb de armazenamento e sistema operacional Ubuntu Server 16.04.1 LTS. Neste servidor virtualizado, analisou-se os dados de tráfego e exibiu-se as estatísticas em uma visualização *dashboard*. A figura 14 detalha cada um dos elementos que constituem o serviço e na próxima seção descreve cada uma das ferramentas indicados.

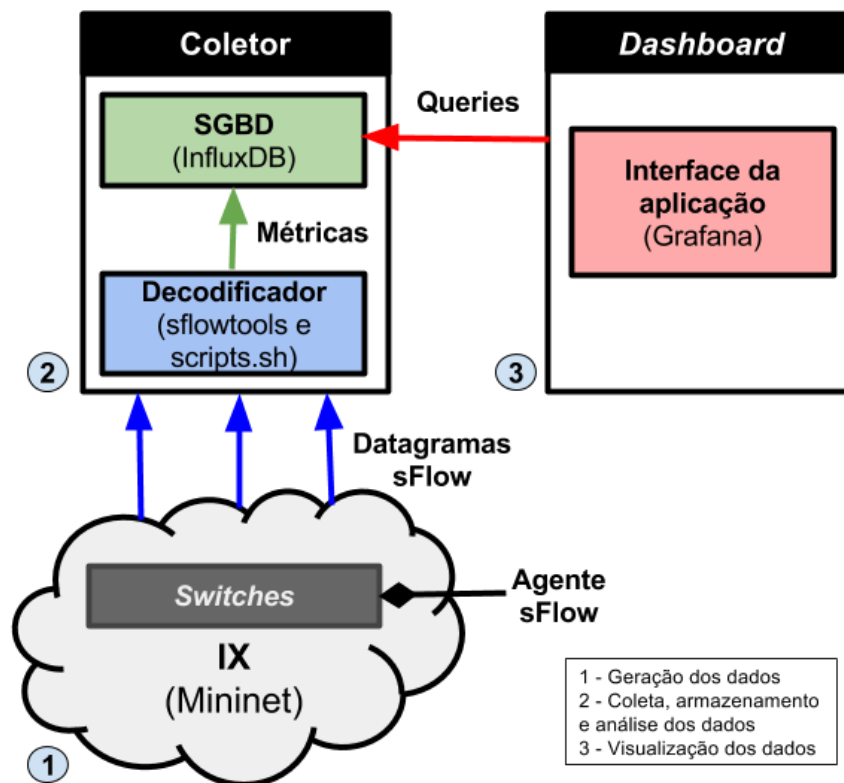


Figura 14. Tecnologias que foram utilizadas no projeto

4.1.1 Geração dos dados

A princípio, esperava-se que projeto fosse implementado utilizando a estrutura o IX.br-MG. Porém, explorar a estrutura de um IX real necessitava de permissão do NIC.br e demandaria muito tempo para autorização. Assim, foi necessário encontrar outra forma para simular a estrutura de um IX que permitisse implementar o serviço. Logo, foi utilizada uma estrutura virtualizada do mesmo. O protótipo da estrutura do IX foi simulada utilizando a ferramenta de criação de redes virtuais Mininet³, sob autoria do PoP-MG, que possibilita instanciar hosts, enlaces e switches virtuais. Com essa estrutura, foi possível definir uma topologia de rede similar à do IX.br-MG, detalhada na figura 15.

³ <http://mininet.org>

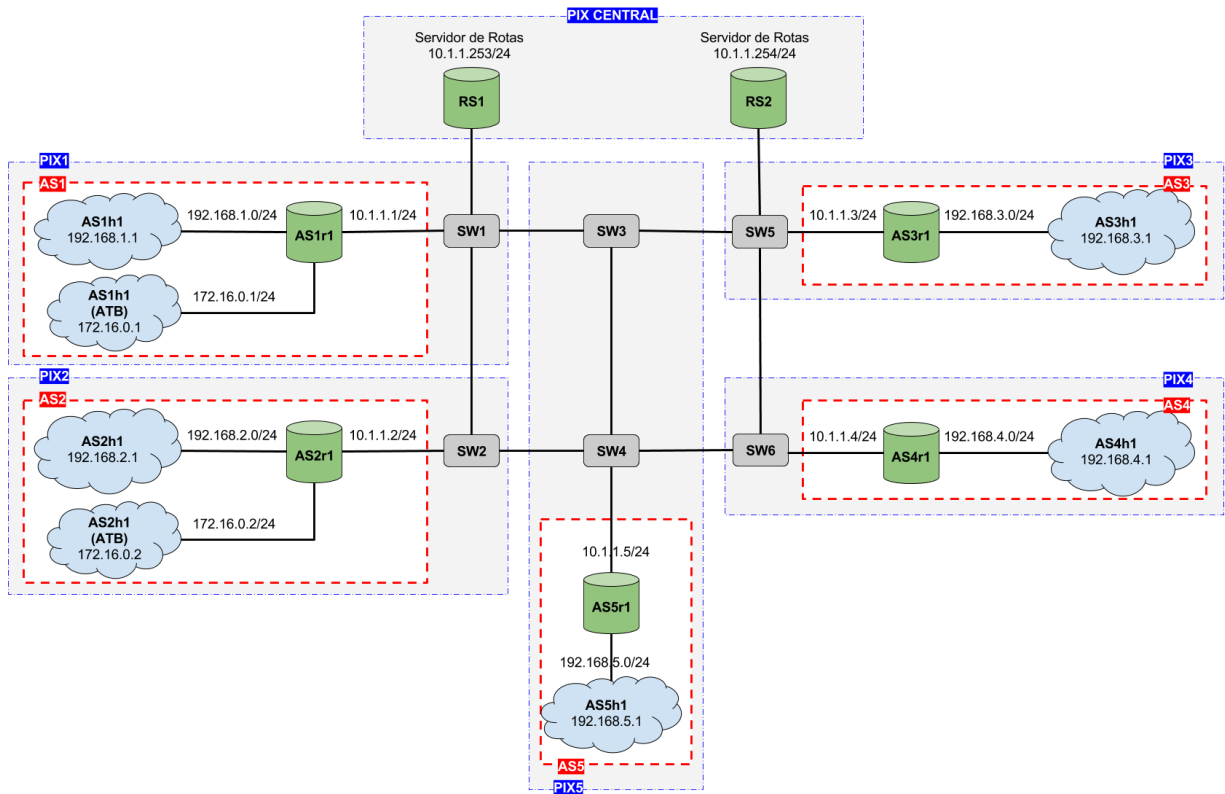


Figura 15. Protótipo da estrutura do IX

Para a geração dos datagramas, o protocolo sFlow foi habilitado e configurado nos agentes, no caso os switches indicados na figura 15. Os datagramas foram gerados por meio de uma ferramenta chamada *iperf*⁴ dentro da aplicação mininet, que permite simular tráfego no link entre dois pontos via linha de comando. Em um AS foi executado o *iperf* como servidor, utilizando o comando *iperf -s* para esperar conexões. No segundo AS foi executado o *iperf* como cliente, utilizando o comando *iperf -c domínio/ip_servidor*. A figura 16 detalha este procedimento, onde o AS2 envia 1 MBytes para o AS1 durante 10 segundos. Para gerar as estatísticas, foi gerado seis fluxos de tráfego entre os ASes em períodos de tempo diferentes utilizando a ferramenta *iperf*.

⁴ <https://pt.wikipedia.org/wiki/Iperf>

```

[Node: AS1h1"@wall-ptt AS1 SERVIDOR
root@wall-ptt:/ix/mininet# iperf -s -u -i -1
WARNING: interval too small, increasing from -1.00 to 0.5 seconds.
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 208 KByte (default)

[ 45] local 192.168.1.1 port 5001 connected with 192.168.2.1 port 34478
[ ID] Interval      Transfer      Bandwidth      Jitter    Lost/Total Datagrams
[ 45] 0.0- 0.5 sec  60.3 KBytes  988 Kbits/sec  0.002 ms  0/ 42 (0%)
[ 45] 0.5- 1.0 sec  61.7 KBytes  1.01 Mbits/sec 0.010 ms  0/ 43 (0%)
[ 45] 1.0- 1.5 sec  60.3 KBytes  988 Kbits/sec  0.003 ms  0/ 42 (0%)
[ 45] 1.5- 2.0 sec  61.7 KBytes  1.01 Mbits/sec 0.019 ms  0/ 43 (0%)
[ 45] 2.0- 2.5 sec  60.3 KBytes  988 Kbits/sec  0.007 ms  0/ 42 (0%)
[ 45] 2.5- 3.0 sec  61.7 KBytes  1.01 Mbits/sec 0.009 ms  0/ 43 (0%)
[ 45] 3.0- 3.5 sec  60.3 KBytes  988 Kbits/sec  0.005 ms  0/ 42 (0%)
[ 45] 3.5- 4.0 sec  61.7 KBytes  1.01 Mbits/sec 0.008 ms  0/ 43 (0%)
[ 45] 4.0- 4.5 sec  60.3 KBytes  988 Kbits/sec  0.005 ms  0/ 42 (0%)
[ 45] 4.5- 5.0 sec  61.7 KBytes  1.01 Mbits/sec 0.009 ms  0/ 43 (0%)
[ 45] 5.0- 5.5 sec  60.3 KBytes  988 Kbits/sec  0.003 ms  0/ 42 (0%)
[ 45] 5.5- 6.0 sec  61.7 KBytes  1.01 Mbits/sec 0.007 ms  0/ 43 (0%)
[ 45] 6.0- 6.5 sec  60.3 KBytes  988 Kbits/sec  0.004 ms  0/ 42 (0%)
[ 45] 6.5- 7.0 sec  61.7 KBytes  1.01 Mbits/sec 0.011 ms  0/ 43 (0%)
[ 45] 7.0- 7.5 sec  60.3 KBytes  988 Kbits/sec  0.005 ms  0/ 42 (0%)
[ 45] 7.5- 8.0 sec  61.7 KBytes  1.01 Mbits/sec 0.006 ms  0/ 43 (0%)
[ 45] 8.0- 8.5 sec  60.3 KBytes  988 Kbits/sec  0.002 ms  0/ 42 (0%)
[ 45] 8.5- 9.0 sec  61.7 KBytes  1.01 Mbits/sec 0.007 ms  0/ 43 (0%)
[ 45] 9.0- 9.5 sec  60.3 KBytes  988 Kbits/sec  0.006 ms  0/ 42 (0%)
[ 45] 9.5-10.0 sec 61.7 KBytes  1.01 Mbits/sec 0.003 ms  0/ 43 (0%)
[ 45] 0.0-10.0 sec 1.19 MBytes  1.00 Mbits/sec 0.003 ms  0/ 852 (0%)

[Node: AS2h1"@wall-ptt AS2 CLIENTE
root@wall-ptt:/ix/mininet# iperf -c 192.168.1.1 -u -b 1m -t 10
Client connecting to 192.168.1.1, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 208 KByte (default)

[ 45] local 192.168.2.1 port 34478 connected with 192.168.1.1 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 45] 0.0-10.0 sec  1.19 MBytes  1000 Kbits/sec
[ 45] Sent 852 datagrams
[ 45] Server Report:
[ 45] 0.0-10.0 sec  1.19 MBytes  1.00 Mbits/sec  0.002 ms  0/ 852 (0%)
root@wall-ptt:/ix/mininet#

```

Figura 16. Geração de tráfego usando a ferramenta iperf

4.1.2 Coleta, armazenamento e análise dos dados

Após a configuração das regras de fluxo, os datagramas sFlow foram enviados e armazenados no disco do servidor dedicado. A ferramenta utilizada para salvar e analisar os datagramas é chamada *sflowtools*⁵. A figura 17 mostra as principais tags de um datagrama sFlow. Para popular a base de dados, as regras do datagrama sFlow precisaram ser decodificados em métricas, com auxílio de *shell scripts* descritos na seção de apêndice (influxData1.sh e influxData2.sh). Após a filtragem das regras de fluxo para apenas àquelas de interesse para a contabilização (destacadas em vermelho na figura 17), iniciou-se o processo de contabilização propriamente dito.

⁵ <http://www.inmon.com/technology/sflowTools.php>

```

startDatagram =====
datagramSourceIP 127.0.0.1
datagramSize 1324
unixSecondsUTC 1479490263
datagramVersion 5
agent 127.0.0.1
packetSequenceNo 948
samplesInPacket 1
startSample -----
sampleType FLOWSAMPLE
sampleSequenceNo 4755
inputPort 14
outputPort 4
extendedType SWITCH
in_vlan 250
out_vlan 250
flowSampleType HEADER
headerProtocol 1
sampledPacketSize 1520
dstMAC 000000010201
srcMAC 000000010101
decodedVLAN 250
IPSize 1498
srcIP 172.16.0.1
dstIP 172.16.0.2
IPProtocol 17
UDPSrcPort 59248
UDPDstPort 5001
UDPBytes 1478
endSample -----
startSample -----
endDatagram =====

```

Figura 17. Exemplo de arquivo com datagrama sFlow

Assim, os arquivos de datagramas sFlow são decodificados em arquivos de métricas e enviados para o banco de dados do InfluxDB. A figura 18 mostra algumas métricas de exemplo decodificadas por scripts.

```

octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.253,dstIP=10.1.1.3,srcMAC=000000000001,dstMAC=000000010301 value=74 1479490260
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.1,dstIP=10.1.1.254,srcMAC=000000010101,dstMAC=000000000002 value=93 1479490261
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.3,dstIP=10.1.1.253,srcMAC=000000010301,dstMAC=000000000001 value=93 1479490263
octets,ipprotocol=udp,in_vlan=250,out_vlan=250,srcIP=172.16.0.1,dstIP=172.16.0.2,srcMAC=000000010101,dstMAC=000000010201 value=1103520 1479490263
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.253,dstIP=10.1.1.5,srcMAC=000000000001,dstMAC=000000010501 value=93 1479490264
octets,ipprotocol=udp,in_vlan=250,out_vlan=250,srcIP=172.16.0.1,dstIP=172.16.0.2,srcMAC=000000010101,dstMAC=000000010201 value=1269200 1479490264
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.254,dstIP=10.1.1.2,srcMAC=000000000002,dstMAC=000000010201 value=93 1479490265
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.254,dstIP=10.1.1.5,srcMAC=000000000002,dstMAC=000000010501 value=82 1479490265

```

Figura 18. Exemplo de entradas no arquivo de métricas para o InfluxDB

As métricas foram armazenadas no InfluxDB. Este é um SGBD de código aberto escrito em *Go* que lida com dados de séries temporais que possui um alto desempenho de leitura e escrita, não sofrendo de problemas de I/O como o Grafite (Carbon + Whisper). O InfluxDB opera no modelo de métricas, que contém um conjunto de Tags (campos), associadas a um valor e uma marcação de tempo (*timestamp*). Segue abaixo as seguintes características que motivaram o InfluxDB como ferramenta de armazenamento de dados:

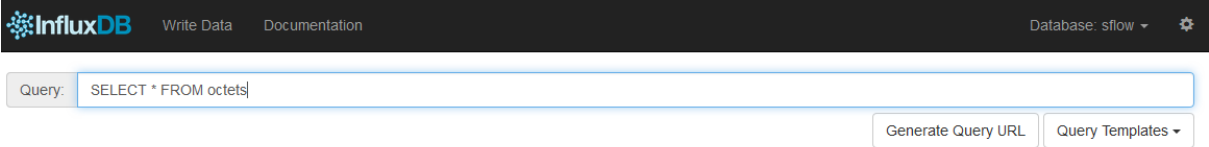
- Instalação rápida, sem dependências externas;
- Suporte à servidores Linux e OS X;
- Possui interface HTTP para ler e escrever os dados;
- Utiliza SQL como linguagem de consulta;
- Escalável para implementações complexas (dados do IX);
- Flexível (trabalha com o *dashboard* Grafana);

Para a contabilização do tráfego, foi definida a métrica octets, que engloba a quantidade de bytes trafegados entre dois ASes respectivamente. Uma descrição mais detalhada das TAGS utilizadas na métrica octets, é descrita na tabela 1.

Contabilização do Tráfego		
TAG	Valores	Descrição
ipprotocol	[numérico]	Identificação do protocolo IP (6=tcp, 17=udp)
in_vlan	[numérico]	Identificação da VLAN de entrada usada
out_vlan	[numérico]	Identificação da VLAN de saída usada
srcIP	[prefixo IP]	Identificação do IP de origem (AS de origem)
dstIP	[prefixo IP]	Identificação do IP de destino (AS de destino)
srcMAC	[numérico]	Identificação do endereço MAC de origem
dstMAC	[numérico]	Identificação do endereço MAC de destino
Campos	Valores	Descrição
value	[numérico]	Valor do contador de bytes
timestamp	[numérico]	Valor do <i>timestamp</i> da coleta (em segundos)

Tabela 1. Tags e campos utilizados na contabilização

O InfluxDB também possui uma interface HTTP, que permite escrever e consultar métricas no banco de dados, conforme a figura 19.



octets

time	dstIP	dstMAC	in_vlan	ipprotocol	out_vlan	srcIP	srcMAC	value
2016-12-28T17:40:22Z	"10.1.1.2"	"000000010201"	"10"	"tcp"	"10"	"10.1.1.253"	"000000000001"	930
2016-12-28T17:40:25Z	"10.1.1.254"	"000000000002"	"10"	"tcp"	"10"	"10.1.1.4"	"000000010401"	740
2016-12-28T17:40:25Z	"10.1.1.4"	"000000010401"	"10"	"tcp"	"10"	"10.1.1.254"	"000000000002"	740
2016-12-28T17:40:28Z	"10.1.1.254"	"000000000002"	"10"	"tcp"	"10"	"10.1.1.4"	"000000010401"	930
2016-12-28T17:40:28Z	"10.1.1.253"	"000000000001"	"10"	"tcp"	"10"	"10.1.1.1"	"000000010101"	930
2016-12-28T17:40:29Z	"10.1.1.253"	"000000000001"	"10"	"tcp"	"10"	"10.1.1.4"	"000000010401"	740
2016-12-28T17:40:30Z	"10.1.1.5"	"000000010501"	"10"	"tcp"	"10"	"10.1.1.253"	"000000000001"	740
2016-12-28T17:40:31Z	"10.1.1.1"	"000000010101"	"10"	"tcp"	"10"	"10.1.1.253"	"000000000001"	930
2016-12-28T17:40:31Z	"10.1.1.2"	"000000010201"	"10"	"tcp"	"10"	"10.1.1.253"	"000000000001"	740
2016-12-28T17:40:31Z	"10.1.1.254"	"000000000002"	"10"	"tcp"	"10"	"10.1.1.2"	"000000010201"	930
2016-12-28T17:40:33Z	"10.1.1.253"	"000000000001"	"10"	"tcp"	"10"	"10.1.1.5"	"000000010501"	930
2016-12-28T17:40:34Z	"10.1.1.4"	"000000010401"	"10"	"tcp"	"10"	"10.1.1.254"	"000000000002"	930
2016-12-28T17:40:34Z	"10.1.1.254"	"000000000002"	"10"	"tcp"	"10"	"10.1.1.4"	"000000010401"	930
2016-12-28T17:40:34Z	"10.1.1.1"	"000000010101"	"10"	"tcp"	"10"	"10.1.1.253"	"000000000001"	930

Figura 19. Interface Web do InfluxDB

4.1.3 Visualização dos dados

A partir dos dados armazenados no servidor do InfluxDB, foram gerados diversos gráficos no *dashboard* do Grafana. O Grafana é uma Ferramenta de *dashboard* open-source utilizado para visualização de dados de séries temporais de infraestrutura de redes e permite que você tenha vários painéis, sendo que cada um deles pode conter um ou mais gráficos. A figura 20 mostra o *dashboard* do serviço construído no Grafana.

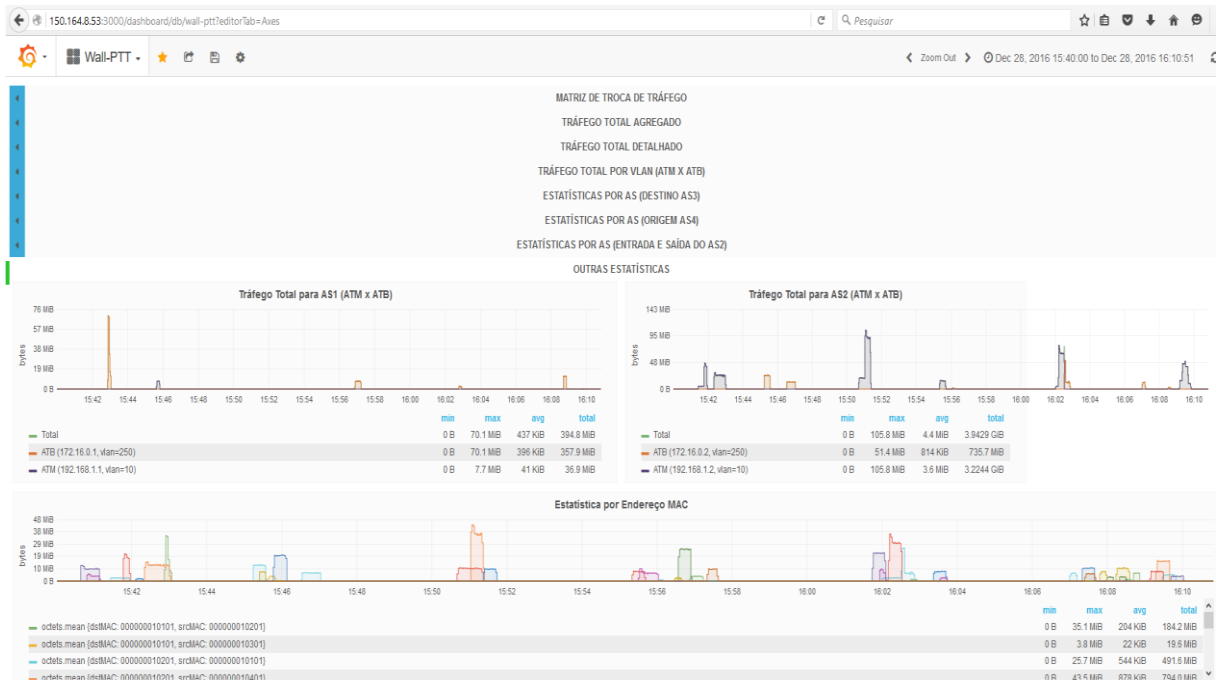


Figura 20. Dashboard construído no Grafana

Segue abaixo as seguintes características que motivaram o Grafana como ferramenta dashboard:

- Suporta InfluxDB como backend;
- Feito em JavaScript;
- Código Aberto;
- Suporte Debian/Ubuntu;
- Fácil Instalação (Versão atual v3.0.4).

5 RESULTADOS E DISCUSSÃO

Com a implementação do protótipo de serviço de coleta, análise e visualização de dados de tráfego, foi possível gerar diversos gráficos estatísticos no *dashboard* do Grafana. Devido à alta granularidade da aplicação, diferentes tipos de gráficos podem ser gerados, mas será exibido somente alguns para demonstrar o potencial da solução proposta.

5.1 Matriz de troca de tráfego

A demonstração do tráfego entre um par de AS de origem e destino é denominada matriz de troca de tráfego. Um exemplo de matriz de tráfego foi mostrado no IX.br-PR, detalhado na seção 2, para representar as medições de fluxo de tráfego entre cada par de membros do IX. Em nosso projeto, é possível visualizar a matriz de troca de tráfego entre todos os pares de ASes que trocaram dados em um certo período de tempo, na figura 21. Esta estatística foi construída agrupando as métricas do InfluxDB pelas tags *srcIP* e *dstIP*.

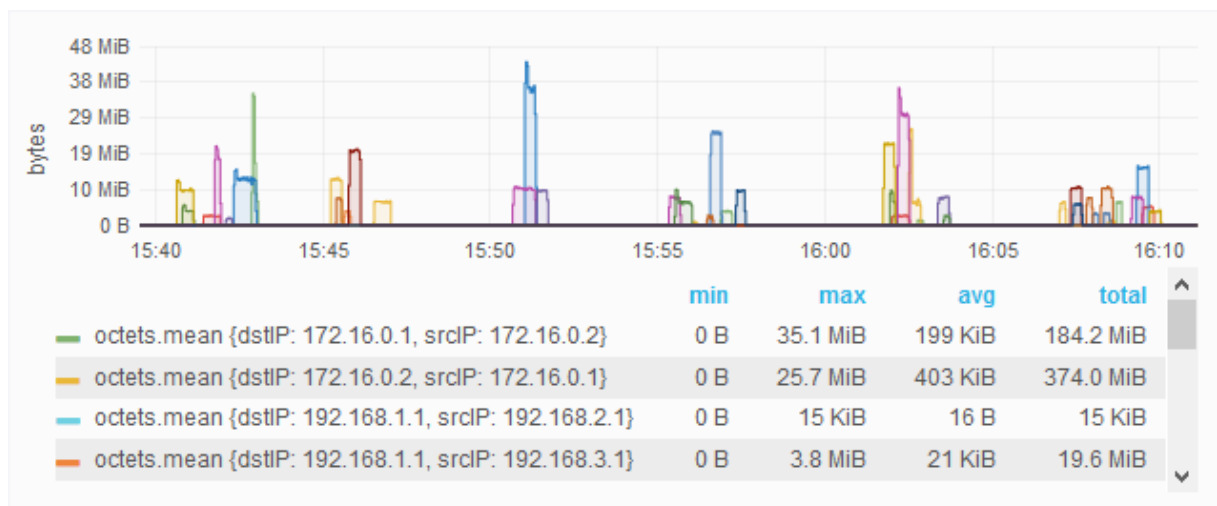


Figura 21. Matriz de troca de tráfego entre os ASes

5.2 Tráfego total agregado

A estatísticas da figura 22 disponibiliza a troca total de tráfego no IX. Esta estatística foi construída somando todas o tráfego de AS no mesmo instante de tempo.

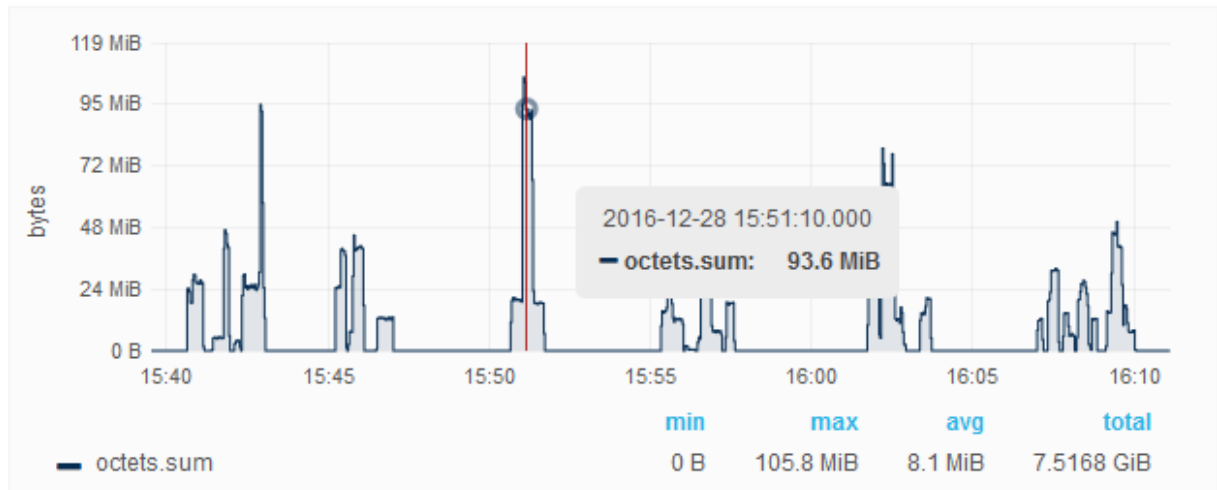


Figura 22. Tráfego total agregando todos os ASes

5.3 Tráfego total detalhado

A estatísticas é parecida com a anterior e disponibiliza a troca total de tráfego no IX. Porém, essa estatística permite descobrir a quantidade de dados trafegados entre um par de ASes em um certo instante de tempo. Na figura 23, é possível visualizar a troca de tráfego entre dois ASes e a soma total deste tráfego em um período de tempo.

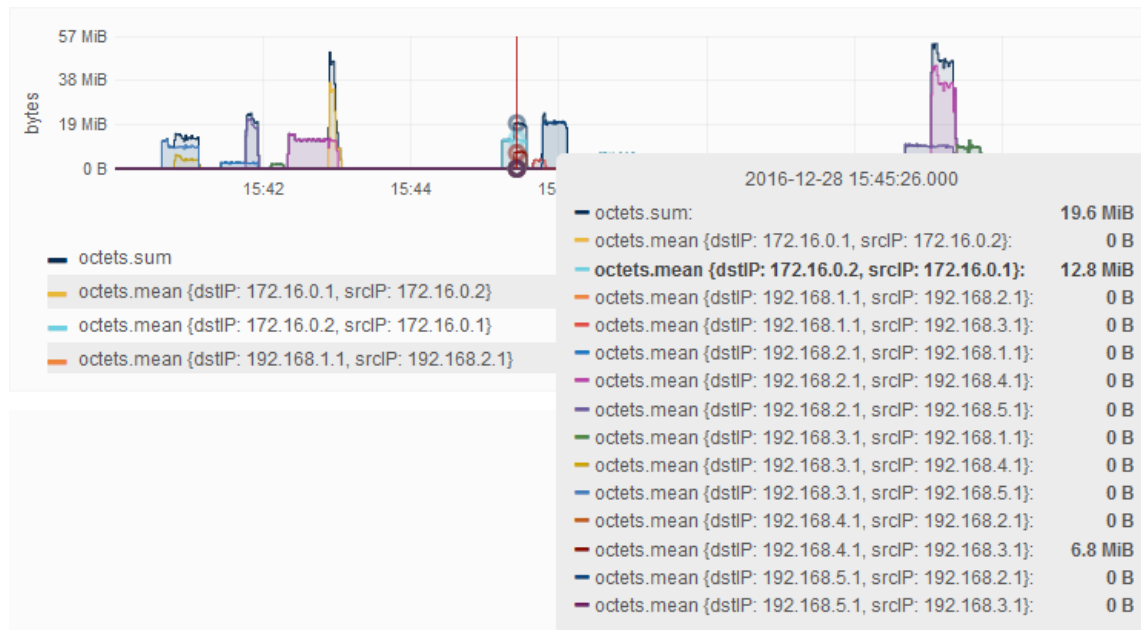


Figura 23. Tráfego total detalhado por AS

5.4 Tráfego total por VLAN (ATM x ATB)

No IX.br-MG, a contabilização atual é realizada por porta, não sendo possível a amostragem do tráfego por critérios mais detalhados, como a troca em uma ATB específica, conforme já discutido anteriormente. Nesta estatística, é possível visualizar o total de tráfego em um IX separado por VLANs e acordos, conforme a figura 24, provendo uma granularidade muito maior nas análises do IX.

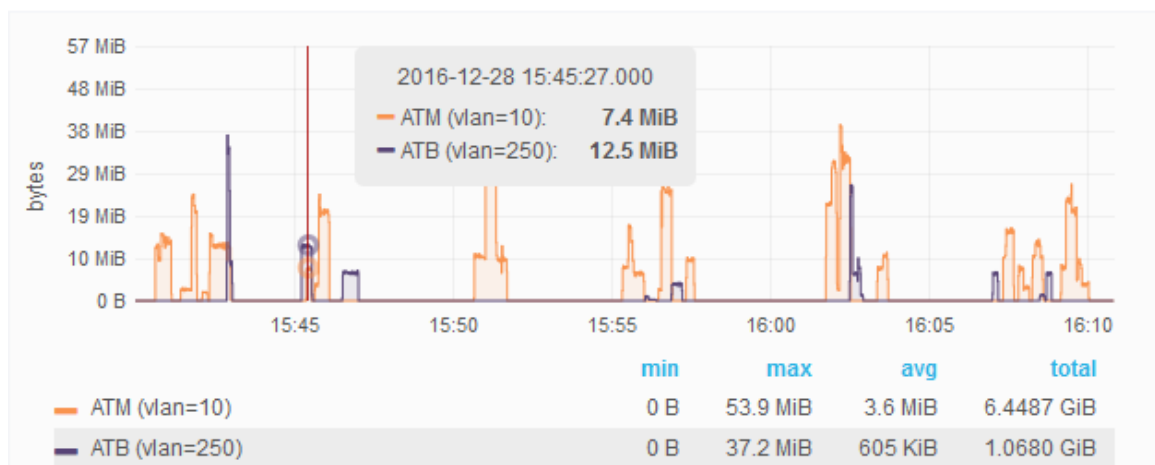


Figura 24. Tráfego total por vlan (ATM x ATB)

5.5 Estatística por AS (destino AS3)

Uma estatística útil é a amostragem do tráfego para um AS específico. A figura 25 mostra a quantidade de tráfego e quais ASes estão trocando tráfego com o AS3 (destino) em um determinado tempo.

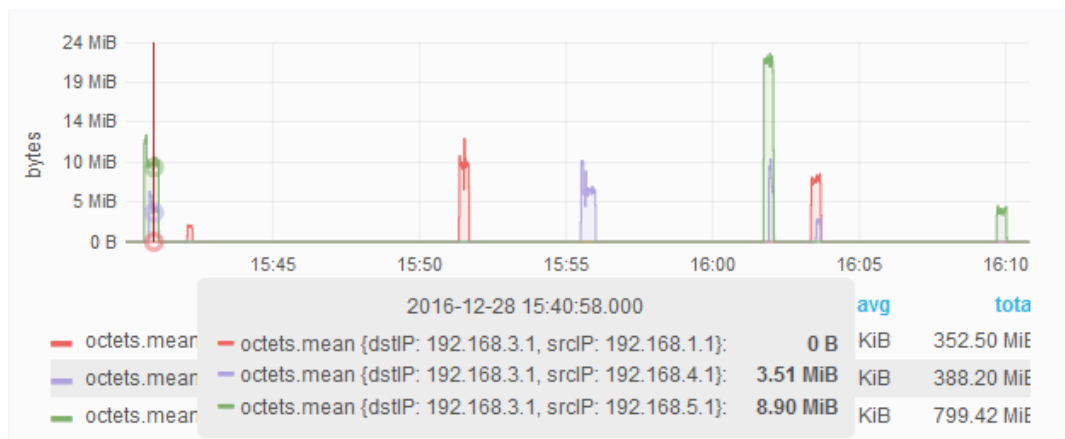


Figura 25. Estatística por AS (destino AS3)

5.6 Estatística por AS (origem AS4)

Na figura 26 podemos ver o total de tráfego e quais Ases estão trocando tráfego com o AS4 (tomando ele como ponto de origem).

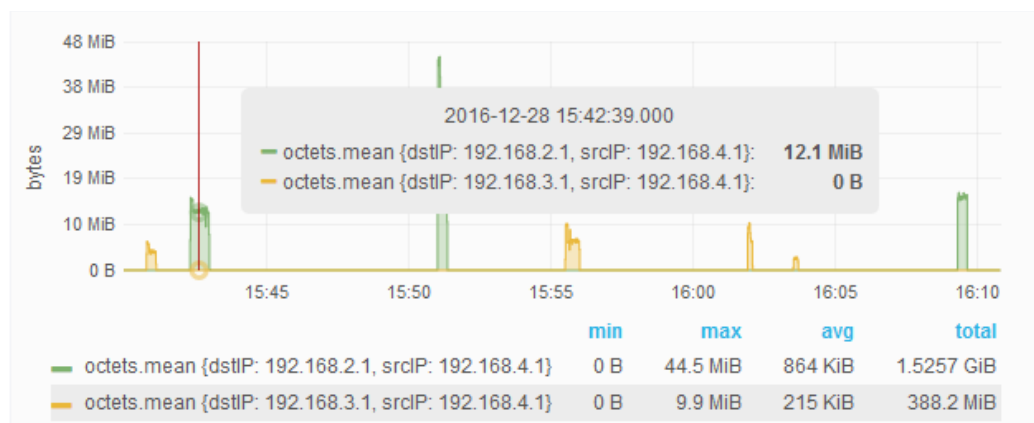


Figura 26. Estatística por AS (origem AS4)

5.7 Estatística por AS (entrada e saída do AS2)

Uma contabilização interessante é a amostragem por AS, onde é mostrado o tráfego de entrada e saída para um AS específico. Na figura 27 podemos visualizar esta estatística do AS2.

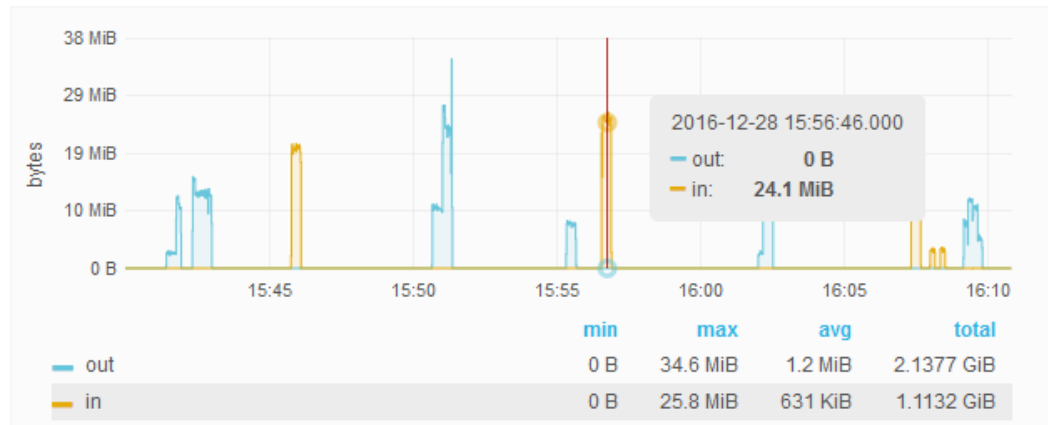


Figura 27. Tráfego de entrada e saída para o S2

5.8 Outras estatísticas

Diversas outras estatísticas são possíveis de serem construídas na plataforma, além das já exibidas. A figura 28 mostra um gráfico com o tráfego total para o AS2 separado por acordos (ATM e ATBs) e VLAN.

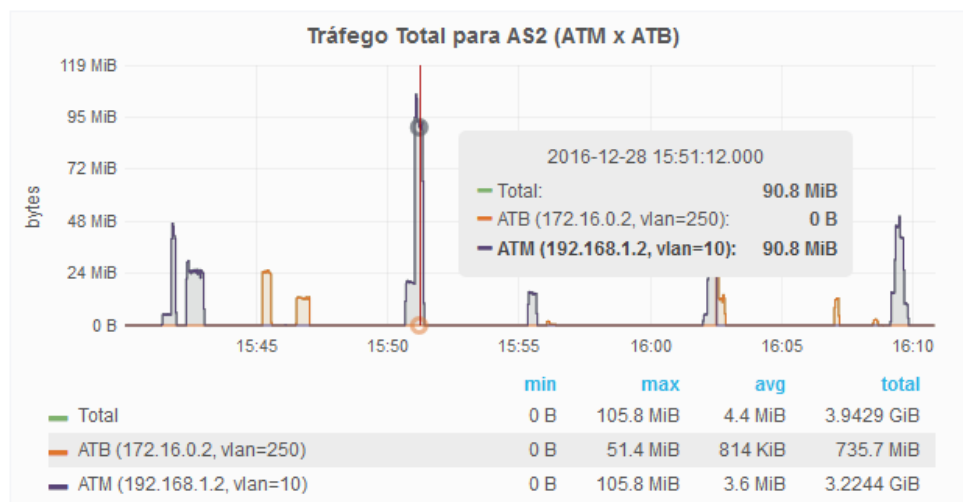


Figura 28. Tráfego total separado por acordos ATM e ATB e VLAN

5.9 Benefícios gerais

Com a implementação do protótipo, espera-se que o serviço seja executado em uma estrutura real do IX, tornando sua administração mais fácil e eficaz, além dos seguintes benefícios:

- Maior flexibilidade no monitoramento do tráfego no IX;
- Visualização de padrões de tráfego associados aos ASes;
- Melhor planejamento dos requisitos da infraestrutura para atender às demandas dos participantes;
- Melhor planejamento da rede, permitindo antecipar possíveis problemas minimizando os custos de operação;
- Permitir detecção de tráfego indesejado e mudanças no tráfego de rede indicando anomalias em potencial;
- Permitir a contabilização detalhada da utilização dos recursos (granularidade);
- Validar a qualidade do serviço do IX.

5.10 Acesso à ferramenta “Wall-PTT”

A ferramenta está acessível até 16/02/2017 no seguinte endereço <http://150.164.8.26:3000/dashboard/db/wall-ptt>. Para acessar o sistema, entre com o usuário visualizador (User: *viewer* Password: *viewersflow*). Para entrar no link é necessário estar conectado na rede do DCC/UFMG ou na VPN, conforme guia em <http://crc.dcc.ufmg.br/tutoriais/vpn/start>. Qualquer dúvida, entre em contato com guisaulo@hotmail.com.

Link do vídeo:

- Youtube: <https://youtu.be/XErL5VwjxfA>
- Google Drive: <https://goo.gl/KXPgxs>

6 CONCLUSÃO

O presente trabalho da disciplina de Monografia em Sistemas de Informação II apresentou um estudo e uma implementação de um serviço de coleta, análise e visualização de dados estatísticos aplicado ao ambiente de um ponto de troca de tráfego. O foco do estudo foi nos benefícios providos por esse serviço quanto a simplificação das tarefas de administração do IX, tornando sua operação mais simples e eficaz.

Com o estudo realizado, foi possível conhecer a infraestrutura, os desafios e a importância de um IX para melhorar a troca de tráfego em uma região. Além disso, foi pesquisado as principais técnicas de gerenciamento e monitoramento de redes assim como os seus principais protocolos, como o SNMP, NetFlow, IPFIX e sFlow. A segunda parte do projeto foi a parte mais difícil, pois a implementação do protótipo exigiu bastante tempo, mas foi possível aprender muitas coisas novas como virtualização de servidores, construção de redes emuladas, testes de rede, linguagens de scripts, administração de banco de dados, etc.

Levando em consideração os fatos mencionados na seção 3.6.4, foi possível solucionar o problema de realizar a coleta do tráfego de dados de cada participante individualmente em cada VLAN, com o uso do protocolo sFlow, evitando a subutilização e permitindo uma coleta com um maior nível de granularidade e detalhes dos dados dos participantes.

Dessa forma, acredito que o trabalho cumpriu a sua finalidade, permitindo a aplicação de conceitos adquiridos durante o curso de Sistemas de Informação, como os conceitos de modelagem de um projeto, conceitos de redes de computadores, aplicação de sistemas de gerenciamento de banco de dados e técnicas de visualização de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ÂNGULO, Franklin. *Getting Started with Monitoring using Graphite*, 2015. Disponível em: <www.infoq.com/articles/graphite-intro>. Acessado em 16 jun. 2016.

BENTLEY, Wilson. *Snowflakes, IPFIX, NetFlow and sFlow*, 2012. Disponível em: <blog.sflow.com/2012/09/snowflakes-ipfix-netflow-and-sflow.html>. Acessado em: 15 jun. 2016.

BRITO, Samuel Henrique Bucke. *Cisco NetFlow na Classificação do Tráfego em Fluxo*, 2013. Disponível em: <labcisco.blogspot.com.br/2013/08/cisco-netflow-na-classificacao-do.html>. Acessado em: 01 jun. 2016.

CLAISE, B., CISCO, Inc. *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*, 2013. Disponível em: <tools.ietf.org/html/rfc7011>. Acessado em: 10 jun. 2016.

CISCO. *Introduction to Cisco IOS NetFlow - A Technical Overview*. Disponível em: <www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html>, 2012. Acessado em: 01 jun. 2016.

CISCO. *Cisco IOS NetFlow Overview*, 2004. Disponível em: <www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_presentation0900aecd80311f57.pdf>. Acessado em: 01 jun. 2016.

CEPTRO.br. *PTTMetro - Pontos de Troca de Tráfego Metropolitanos*. Disponível em <www.ceptro.br/CEPTRO/MenuCEPTROSPPTTMetro>, 2016. Acessado em: 13 mar. 2016.

COUTO, André Valente do. *Uma abordagem de gerenciamento de redes baseado no monitoramento de fluxos de tráfego NetFlow com o suporte de técnicas de business intelligence*, 2012. 131 f. Dissertação (mestrado) – Departamento de Engenharia Elétrica, Universidade de Brasília. Brasília, 2012. Disponível em: <repositorio.unb.br/bitstream/10482/11519/1/2012_AndreValentedoCouto.pdf>. Acessado em: 06 jun. 2016.

DIAS, Henrique de Lima. *A importância do monitoramento de ativos de redes: Um estudo de caso com o sistema CACIC*, 2008. 67 f. Monografia (Graduação) - Escola Politécnica de Pernambuco – Universidade de Pernambuco, Pernambuco, 2008. Disponível em: <tcc.ecomp.poli.br/20082/TCC_Henrique_Dias_2008-2.pdf>. Acesso em: 29 jun. 2005.

FILHO, Olavo Poleta Filho. *Gerenciamento e Monitoramento de Rede I: Teoria de Gerência de Redes*, 2012. Disponível em: <www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_3.asp>. Acessado em: 30 mai. 2016.

GRAFANA. *Documentation* – *InfluxDB*. Disponível em: <docs.grafana.org/datasources/influxdb/>. Acessado em: 18 jun. 2016.

GRUPO DE TRABALHO DE ENGENHARIA E OPERAÇÃO DE REDES, 2007, Belo Horizonte. *PTTrix, Uso do sFlow para efetuar medições membro a membro no PTT*. Belo Horizonte: RNP, 2007. Disponível em: <ftp.registro.br/pub/gter/gter23/02-PTTrix.pdf>. Acesso em: 13 abr. 2016.

GRUPO DE TRABALHO DE ENGENHARIA E OPERAÇÃO DE REDES, 2013, São Paulo. *PTTMetro/PTT.br Evolução, Atualizações e Planejamento*. São Paulo: NIC.br, 2013. Disponível em: <ftp.registro.br/pub/gter/gter35/01-PttMetroEvolucaoUpdates.pdf>. Acesso em: 28 abr. 2016.

GRUPO DE TRABALHO DE ENGENHARIA E OPERAÇÃO DE REDES, 2015, São Paulo. *PTT.br Desafios de infraestrutura e Soluções para o crescimento*. São Paulo: NIC.br, 2015. Disponível em: <ftp.registro.br/pub/gter/gter39/03-PttDesafiosCrescimento.pdf>. Acesso em: 28 abr. 2016.

H3C. *Network Management and Monitoring Configuration Guide*, 2016. Disponível em: www.h3c.com.hk/technical_support_documents/technical_documents/switches/h3c_s12500_series_switches/configuration/operation_manual/h3c_s12500_cg-release7128-6w710/12/201301/772702_1285_0.htm. Acessado em: 03 jun. 2016.

IX.br. *Mapa com as localidades atuais*. Disponível em: <ix.br/localidades/novasmmap>, 2016. Acessado em: 03 mai. 2016.

JASINSKA, Elisa. *sFlow I can feel your traffic*, 2006. Disponível em: <events.ccc.de/congress/2006/Fahrplan/attachments/1137-sFlowPaper.pdf>. Acessado em: 10 jun. 2016.

JENSEN, Lee. *Beautidul Monitoring with Grafana and InfluxDB*. Disponível em: <pt.slideshare.net/leesjensen/beautiful-monitoring-with-grafana-and-influxdb>. Acessado em 17 jun. 2016.

KREJČÍ, R. *Network Traffic Collection with IPFIX Protocol*. 2009. Dissertação (mestrado) - Masarykova Univerzita. Disponível em: <is.muni.cz/th/98863/fi_m/xkrejc14_dp.pdf>. Acessado em: 02 jun. 2016.

Lindsay Hill. *Using InfluxDB + Grafana to Display Network Statistics*, 2015. Disponível em: <lkhill.com/using-influxdb-grafana-to-display-network-statistics/>. Acessado em: 15 jun. 2016.

MARTINS, Luis Felipe Cunha. *Redes definidas por software aplicada ao ecossistema de pontos de troca de tráfego: uma abordagem sistêmica e prática*. 2016. Dissertação (mestrado) – Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, Belo Horizonte, 2004.

MENEZES, Elionildo da Silva. *Gerenciamento de Redes: Estudos de Protocolos*, 1998. Disponível em: <www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html>. Acessado em: 04 jun. 2016.

MOREIRAS, Antonio, GETSHKO, Demi. *Os Pontos de Troca de Tráfego, o PTTMetro e a Internet Brasileira*. Disponível em: <www.ceptro.br/pub/CEPTRO/PalestrasPublicacoes/Os_Pontos_de_Troca_de_Trfego_o_PTTMetro_e_a_Internet_Brasileira.pdf>. Acessado em: 13 mar. 2016.

OPSERVICES. *O que é NetFlow e como funciona essa tecnologia*, 2016. Disponível em: <www.opservices.com.br/o-que-e-netflow-e-como-funciona-essa-tecnologia/>. Acessado em: 01 jun. 2016.

OPSERVICES. *O que é sFlow e quais suas vantagens*, 2016. Disponível em: <www.opservices.com.br/o-que-e-o-protocolo-sflow-e-quais-suas-vantagens/>. Acessado em: 07 jun. 2016.

O'TOOLE, Philip. *InfluxDB e Grafana Howto*, 2014. Disponível em: <www.philipotoole.com/influxdb-and-grafana-howto/>. Acessado em: 17 jun. 2016.

PETER. *Rapidly detecting large flows, sFlow vs. NetFlow/IPFIX*, 2013. Disponível em: <blog.sflow.com/2013/01/rapidly-detecting-large-flows-sflow-vs.html>. Acessado em: 15 jun. 2016.

PETER. *InfluxDB and Grafana*, 2014. Disponível em: <blog.sflow.com/2014/12/influxdb-and-grafana.html>. Acessado em: 15 jun. 2016.

PHAAL, P., INMON CORP. *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*, 2001. Disponível em: <www.rfc-editor.org/rfc/pdf/rfc3176.txt.pdf>. Acessado em: 08 jun. 2016.

PATTERSON, Michael. *What is IPFIX vs. NetFlow v9?*, 2009. Disponível em: <www.plixer.com/blog/netflow/what-is-ipfix-vs-netflow-v9/>. Acessado em: 10 jun. 2016.

PINHEIRO, José Mauricio Santos. *Gerenciamento de Redes de Computadores: Uma Breve Introdução*, 2006. Disponível em: <www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acessado em: 02 jun. 2016.

REESE, Brad. *Cisco's NetFlow vs. Inmon's sFlow: Which will prevail*, 2007. Disponível em: <www.networkworld.com/article/2349966/cisco-subnet/cisco-s-netflow-vs--inmon-s-sflow--which-will-prevail-.html>. Acessado em: 05 jun. 2016.

SANTOS, Gléderson Lessa dos. *Sistema baseado nas recomendações IPFIX para exportação e análise de informações de fluxos em redes convergente*, 2007. 122 f. Dissertação (mestrado) -Faculdade de Engenharia Elétrica da Pontifícia Universidade Católica do Rio Grande do Sul. Rio Grande do Sul, 2007. Disponível em: <repositorio.pucrs.br/dspace/bitstream/10923/3139/1/000390448-Texto%2bCompleto-0.pdf>. Acessado em: 02 jun. 2016.

SANTOS, Aldri Luiz dos. *Protocolos de gerência*, 2016. Disponível em: <www.inf.ufpr.br/aldri/disc/aula5_snmp.pdf>. Acessado em: 04 jun. 2016.

SFLOW. *Traffic Monitoring using sFlow*, 2003. Disponível em: <www.sflow.org/sFlowOverview.pdf>. Acessado em: 07 jun. 2016

TELCO MANAGER. *Gerenciamento de rede com NetFlow - Quebrando paradigmas*, 2016. Disponível em: <www.telcomanager.com/pt-br/o-que-e-netflow>. Acessado em: 01 jun. 2016.

APÊNDICE A – CÓDIGO DOS SCRIPTS

A.1 influxData1.sh

```
#!/bin/bash

while read var1 var2; do

    case $var1 in
        "unixSecondsUTC")
            unixSecondsUTC=$var2
            ;;
        "sampleType")
            sampleType=$var2
            ;;
        "in_vlan")
            in_vlan=$var2
            ;;
        "out_vlan")
            out_vlan=$var2
            ;;
        "sampledPacketSize")
            sampledPacketSize=$var2
            ;;
        "dstMAC")
            dstMAC=$var2
            ;;
        "srcMAC")
            srcMAC=$var2
            ;;
        "srcIP")
            srcIP=$var2
            ;;
        "dstIP")
            dstIP=$var2
            ;;
        "IPProtocol")
            IPProtocol=$var2
            if [ $IPProtocol = "6" ]; then
                IPProtocol="tcp"
            elif [ $IPProtocol = "17" ]; then
                IPProtocol="udp"
            fi
            ;;
        esac

        if [ "$var1" == "endSample" ] && [ "$sampleType" == "FLOWSAMPLE" ]
    ]; then
        echo
        'octets','ipprotocol='$IPProtocol,'in_vlan='$in_vlan,'out_vlan='$out_vlan
        , 'srcIP='$srcIP,'dstIP='$dstIP,'srcMAC='$srcMAC,'dstMAC='$dstMAC
        'value='$sampledPacketSize $unixSecondsUTC
            in_vlan="NULL"
            out_vlan="NULL"
            sampledPacketSize="NULL"
    
```

```
dstMAC="NULL"  
srcMAC="NULL"  
srcIP="NULL"  
dstIP="NULL"  
IPProtocol="NULL"  
  
fi  
  
done
```

A.2 influxData2.sh

```
#!/bin/bash  
  
sort -k 3 | awk NF | uniq -c | sed -e "s/value=/value\ /" | awk '{  
printf("%s value=%s %s\n", $2, $1*$4, $5 ) }' | sort -k 3
```

APÊNDICE B – QUERIES NA BASE DE DADOS DO INFLUXDB

B.1 Matriz de troca de tráfego

```
SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND  
$timeFilter GROUP BY time($interval), "srcIP", "dstIP" fill(0)
```

B.2 Tráfego total agregado

```
SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND  
$timeFilter GROUP BY time($interval) fill(0)
```

B.3 Tráfego total detalhado

```
SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND  
$timeFilter GROUP BY time($interval) fill(0)  
  
SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND  
$timeFilter GROUP BY time($interval), "dstIP", "srcIP" fill(0)
```

B.4 Tráfego total por VLAN (ATM x ATB)

```
SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND  
"in_vlan" = '10' AND $timeFilter GROUP BY time($interval) fill(0)  
  
SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND  
"in_vlan" = '250' AND $timeFilter GROUP BY time($interval) fill(0)
```

B.5 Estatística por AS (Destino AS3)

```
SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"  
= '192.168.3.1' AND $timeFilter GROUP BY time($interval), "srcIP",  
"dstIP" fill(0)
```

B.6 Estatística por AS (Origem AS4)

```
SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "srcIP"  
= '192.168.4.1' AND $timeFilter GROUP BY time($interval), "srcIP",  
"dstIP" fill(0)
```

B.7 Estatística por AS (Entrada e Saída dos AS2)

```
SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '192.168.2.1' AND $timeFilter GROUP BY time($interval) fill(0)

SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "srcIP"
= '192.168.2.1' AND $timeFilter GROUP BY time($interval) fill(0)
```

B.8 Tráfego total para AS1 (ATM x ATB)

```
SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '192.168.1.1' OR "dstIP" = '172.16.0.1' AND $timeFilter GROUP BY
time($interval) fill(0)

SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '172.16.0.1' AND "in_vlan" = '250' AND $timeFilter GROUP BY
time($interval) fill(0)

SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '192.168.1.1' AND "in_vlan" = '10' AND $timeFilter GROUP BY
time($interval) fill(0)
```

B.9 Tráfego total para AS2 (ATM x ATB)

```
SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '172.16.0.2' OR "dstIP" = '192.168.2.1' AND $timeFilter GROUP BY
time($interval) fill(0)

SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '172.16.0.2' AND "in_vlan" = '250' AND $timeFilter GROUP BY
time($interval) fill(0)

SELECT sum("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND "dstIP"
= '192.168.2.1' AND "in_vlan" = '10' AND $timeFilter GROUP BY
time($interval) fill(0)
```

B.10 Estatísticas por Endereço MAC

```
SELECT mean("value") FROM "octets" WHERE "ipprotocol" = 'udp' AND
$timeFilter GROUP BY time($interval), "srcMAC", "dstMAC" fill(0)
```