

---

---

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

**Monografia em Sistemas de Informação II**

Guilherme Saulo Alves

Orientador: *Prof. Dorgival Olavo Guedes Neto*

---

---

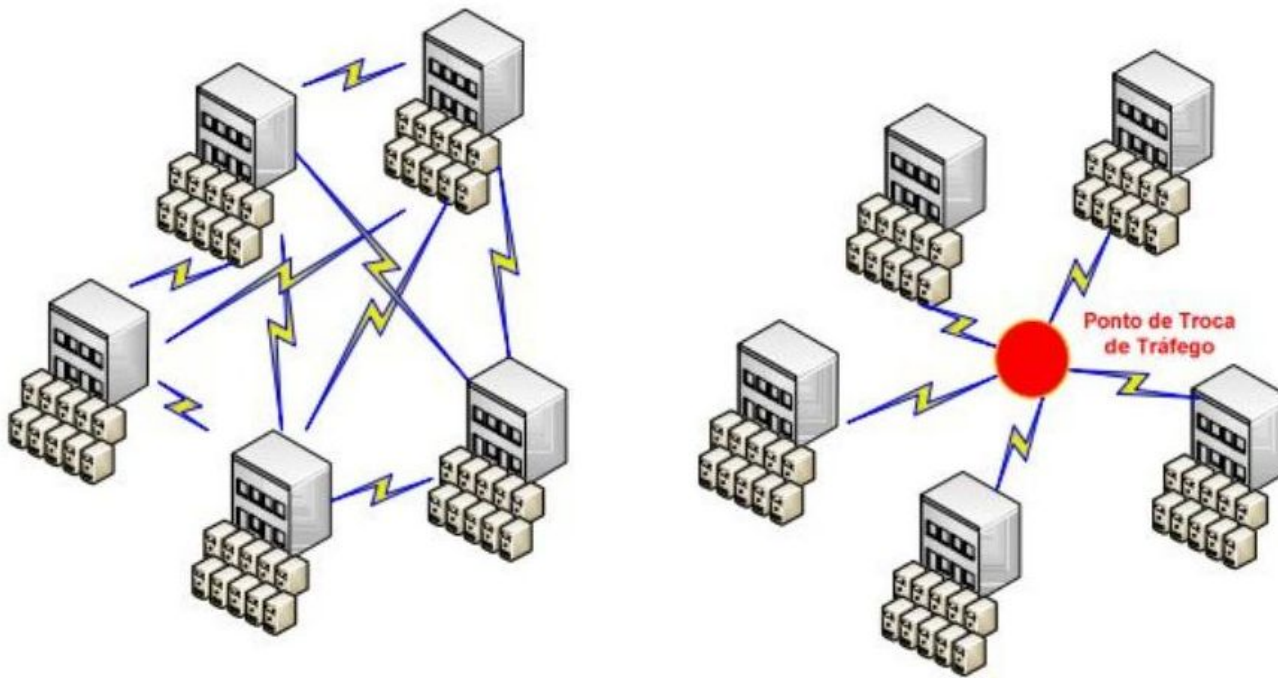
# Ponto de Troca de Tráfego de Minas Gerais (IX.br-MG)

- Um **ponto de troca de tráfego** é um ponto público e central onde diversos ASes, conhecido como **Sistemas Autônomos**, 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;

# Ponto de Troca de Tráfego de Minas Gerais (IX.br-MG)

- 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 1 da apresentação.
- No dia a dia da equipe de um IX, há várias tarefas a serem realizadas, incluindo desde a ativação de novos participantes até a gerência do ambiente;
  - O IX.br-MG se localiza no PoP-MG, sala 3050 do ICEX.

# Ponto de Troca de Tráfego de Minas Gerais (IX.br-MG)



- Troca de Tráfego;
- Participantes;
- Benefícios;
- Custos;
- Processos de rotinas;
- Localização.

**Figura 1.** Conexão dos ASes em um IX

# Objetivo Geral

- ✓ 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.

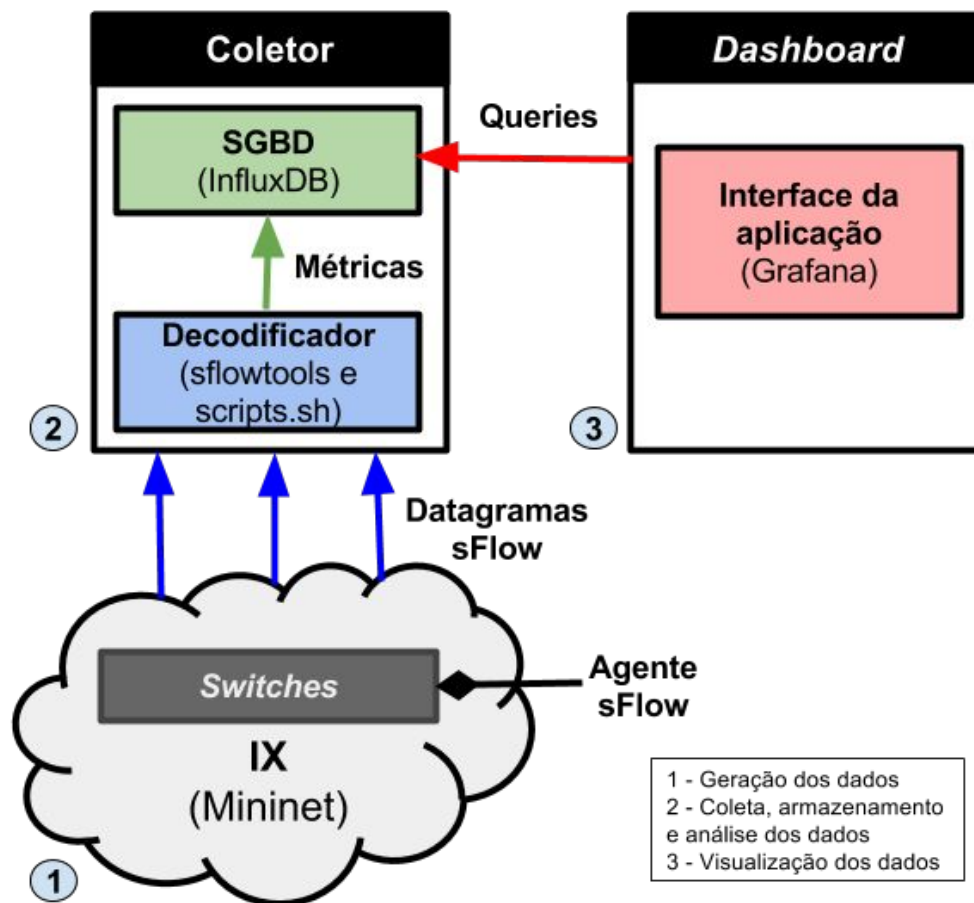
# Objetivos Específicos

- ✓ Estudar sobre os pontos de troca de tráfego (IX.br-MG) **(MSI I)**;
- ✓ Estudar as ferramentas de coleta, análise e visualização de dados estatísticos já existentes na literatura **(MSI I)**;
- ✓ Levantar os dados a serem coletados e quais estatísticas são úteis para serem exibidas a partir destes dados **(MSI I)**;
- ✓ 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. **(MSI II)**.
- **Motivação:** IX.br-MG é carente de um serviço de exibição de dados estatísticos;

# Modelagem e prototipação do ambiente

- O protótipo da estrutura do IX foi simulada utilizando a ferramenta de criação de redes virtuais *Mininet*;
- Para a geração dos datagramas, o protocolo sFlow foi habilitado e configurado nos agentes, no caso os *switches*;
- 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*;
- Para popular a base de dados, as regras do datagrama sFlow precisaram ser decodificados em métricas, com auxílio de *shell scripts*;
- Assim, os arquivos de datagramas sFlow foram decodificados em arquivos de métricas e enviados para o banco de dados do *InfluxDB*;
- A partir dos dados armazenados no servidor do *InfluxDB*, foram gerados diversos gráficos no *dashboard* do *Grafana*.

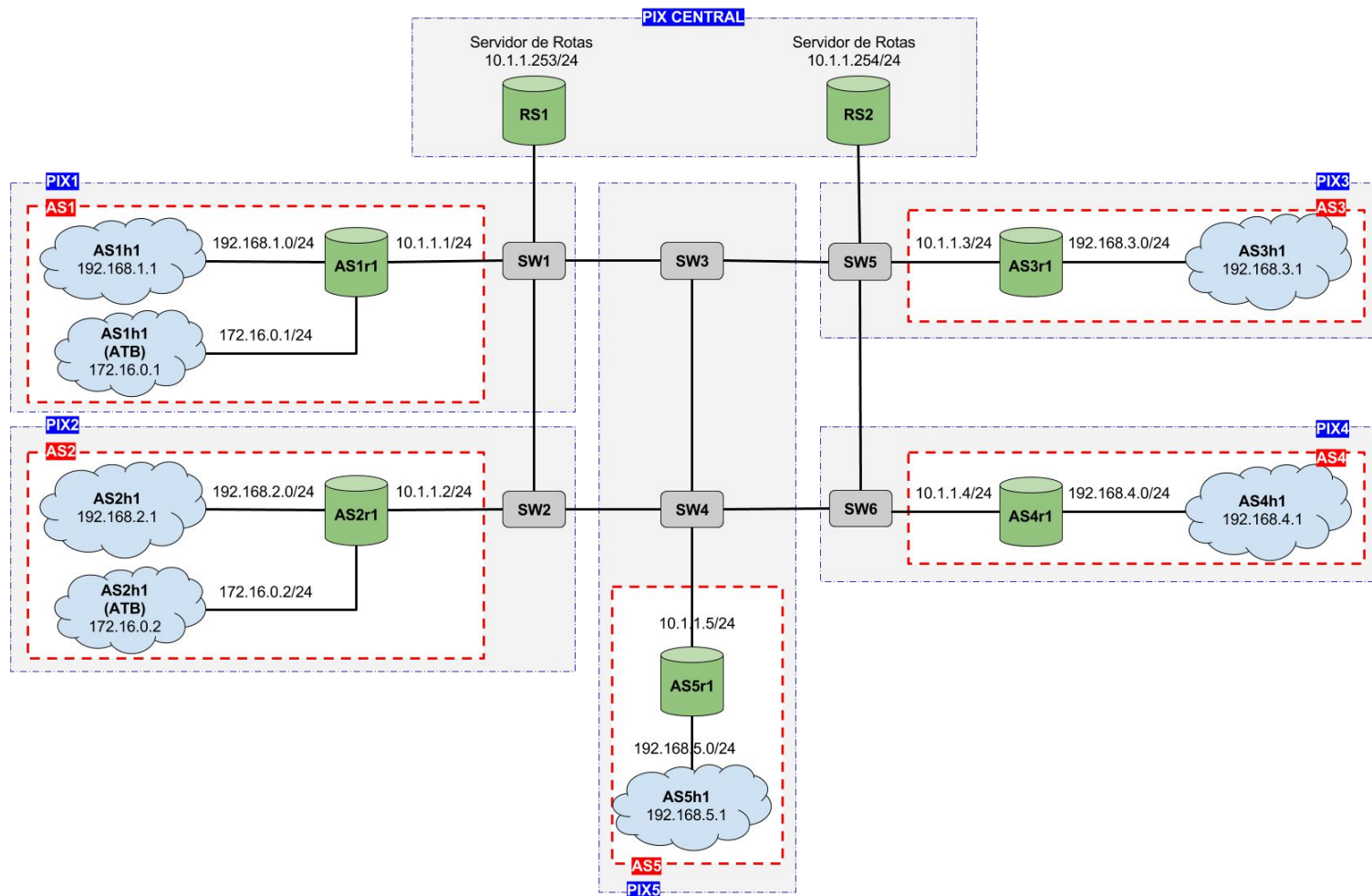
# Modelagem e prototipação do ambiente



**Figura 2.** Tecnologias que foram utilizadas no projeto



# 1 - Geração dos dados



**Figura 3.** Protótipo da estrutura do IX

## 2 - Coleta, armazenamento e análise dos dados

```
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 4.** Exemplo de arquivo com datagrama sFlow

## 2 - Coleta, armazenamento e análise dos dados

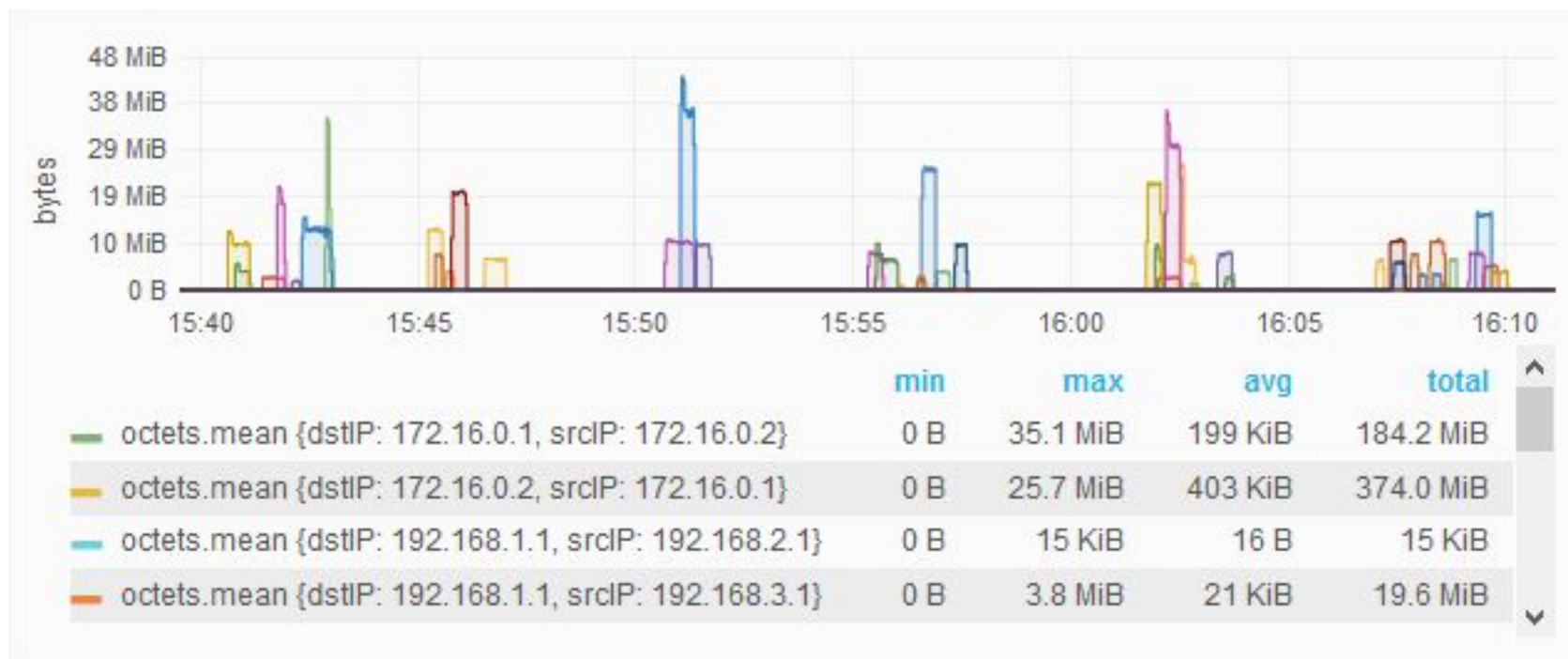
```
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.253,dstIP=10.1.1.3,srcMAC=000000000001,dstMAC=0000000010301 value=74 1479490260
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.1,dstIP=10.1.1.254,srcMAC=000000010101,dstMAC=0000000000002 value=93 1479490261
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.3,dstIP=10.1.1.253,srcMAC=0000000010301,dstMAC=0000000000001 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=0000000000001,dstMAC=0000000010501 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=0000000000002,dstMAC=0000000010201 value=93 1479490265
octets,ipprotocol=tcp,in_vlan=10,out_vlan=10,srcIP=10.1.1.254,dstIP=10.1.1.5,srcMAC=0000000000002,dstMAC=0000000010501 value=82 1479490265
```

**Figura 5.** Exemplo de entradas no arquivo de métricas para o *InfluxDB*

## 3 - Visualização dos dados

- 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.

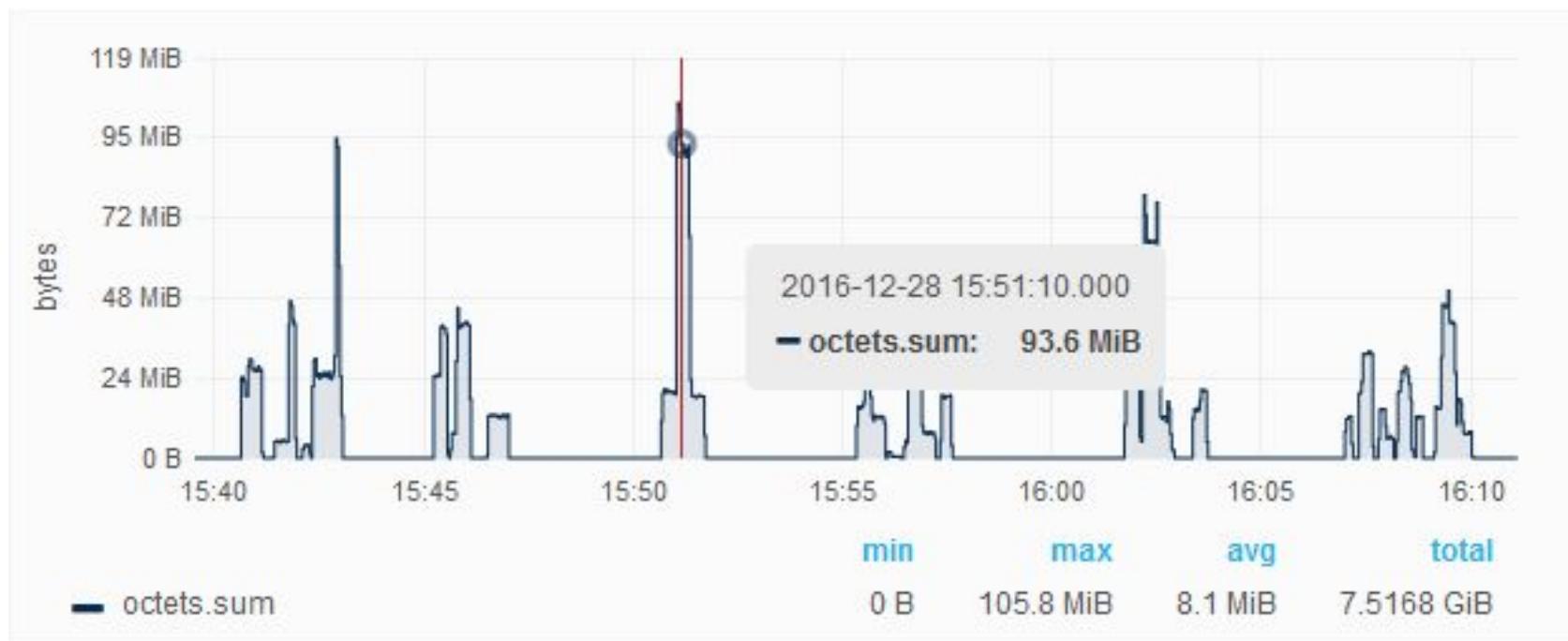
### 3 - Visualização dos dados



**Figura 6.** 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. Na figura 6, é possível visualizar a matriz de troca de tráfego entre todos os pares de ASes que trocaram dados em um certo período de tempo. Esta estatística foi construída agrupando as métricas do *InfluxDB* pelas tags *srcIP* e *dstIP*.

### 3 - Visualização dos dados

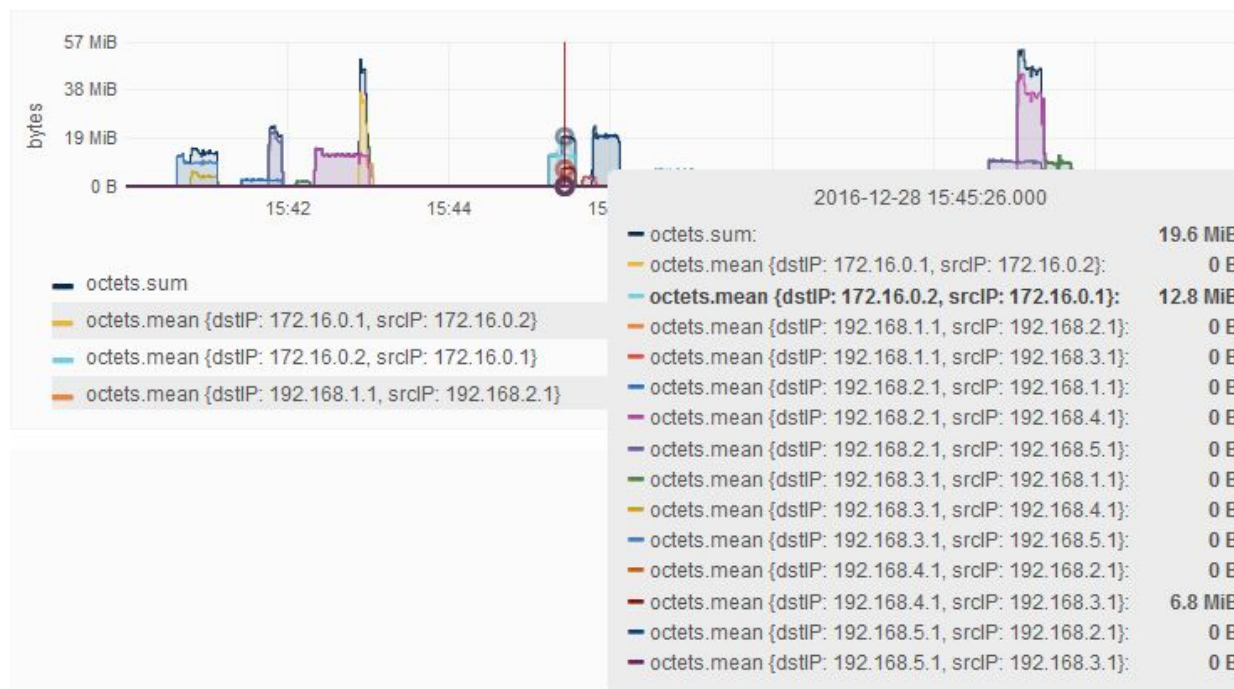


**Figura 7.** Tráfego total agregado

A estatísticas da figura 7 disponibiliza a troca total de tráfego no IX. Esta estatística foi construída somando todas o tráfego de AS no mesmo instante de tempo.



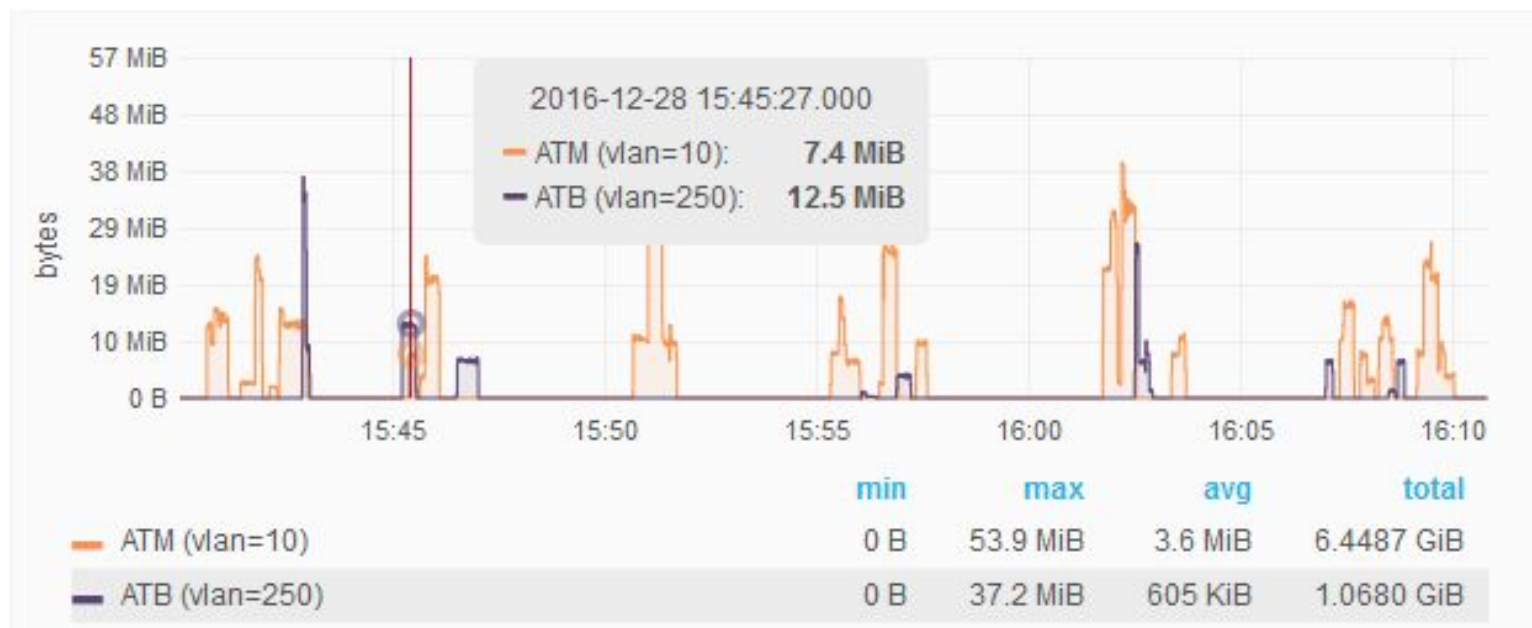
### 3 - Visualização dos dados



**Figura 8.** Tráfego total detalhado por AS

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 8, é possível visualizar a troca de tráfego entre dois ASes e a soma total deste tráfego em um período de tempo.

### 3 - Visualização dos dados

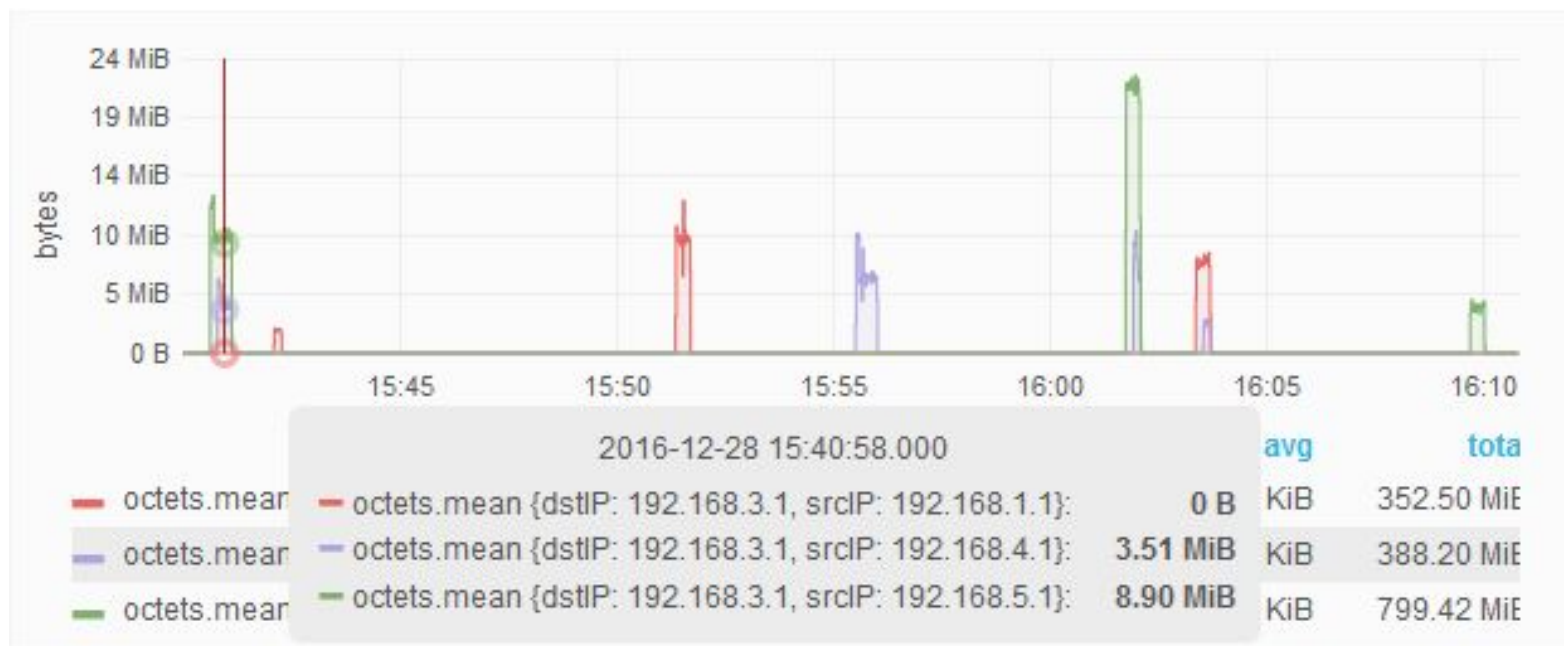


**Figura 9.** Tráfego total por vlan (ATM x ATB)

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. Nesta estatística, é possível visualizar o total de tráfego em um IX separado por VLANs e acordos, conforme a figura 9, provendo uma granularidade muito maior nas análises do IX.



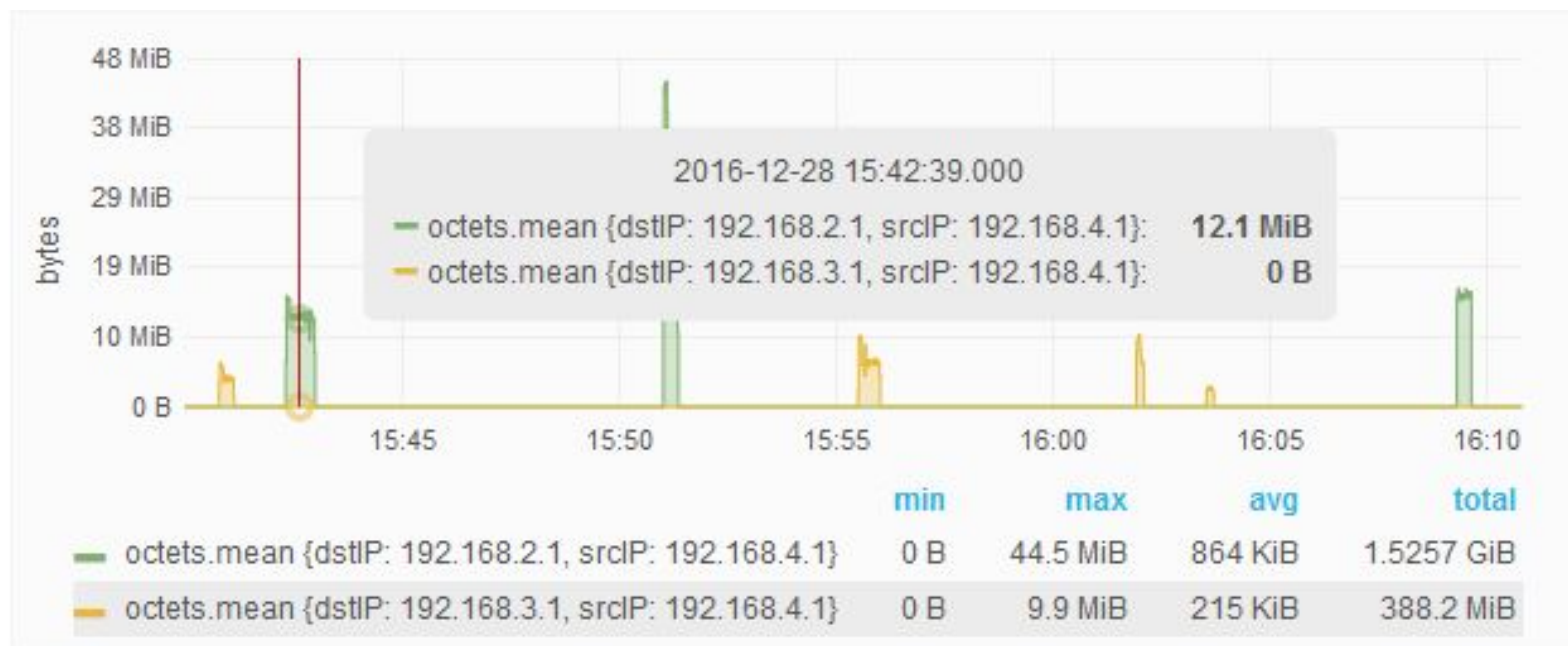
### 3 - Visualização dos dados



**Figura 10.** Estatística por AS (destino AS3)

Uma estatística útil é a amostragem do tráfego para um AS específico. A figura 10 mostra a quantidade de tráfego e quais ASes estão trocando tráfego com o AS3 (destino) em um determinado tempo.

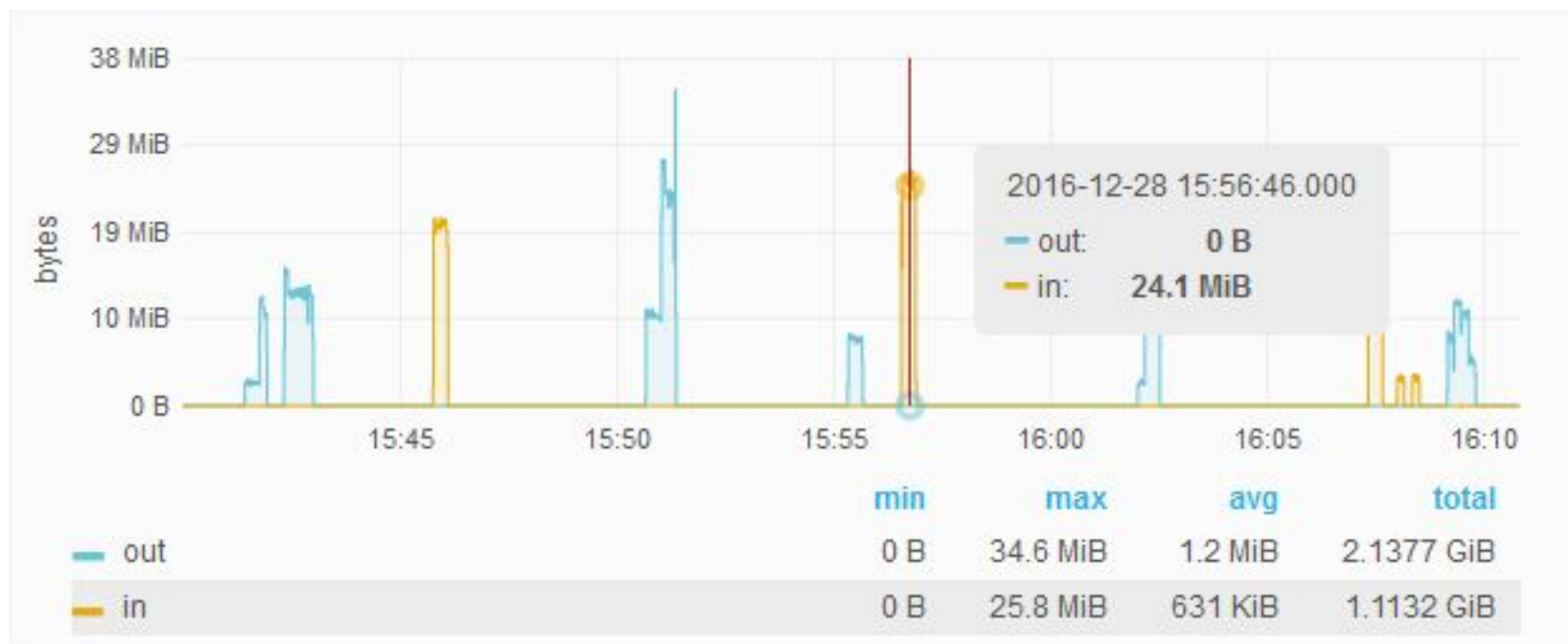
### 3 - Visualização dos dados



**Figura 11.** Estatística por AS (origem AS4)

Na figura 11 podemos ver o total de tráfego e quais Ases estão trocando tráfego com o AS4 (tomando ele como ponto de origem).

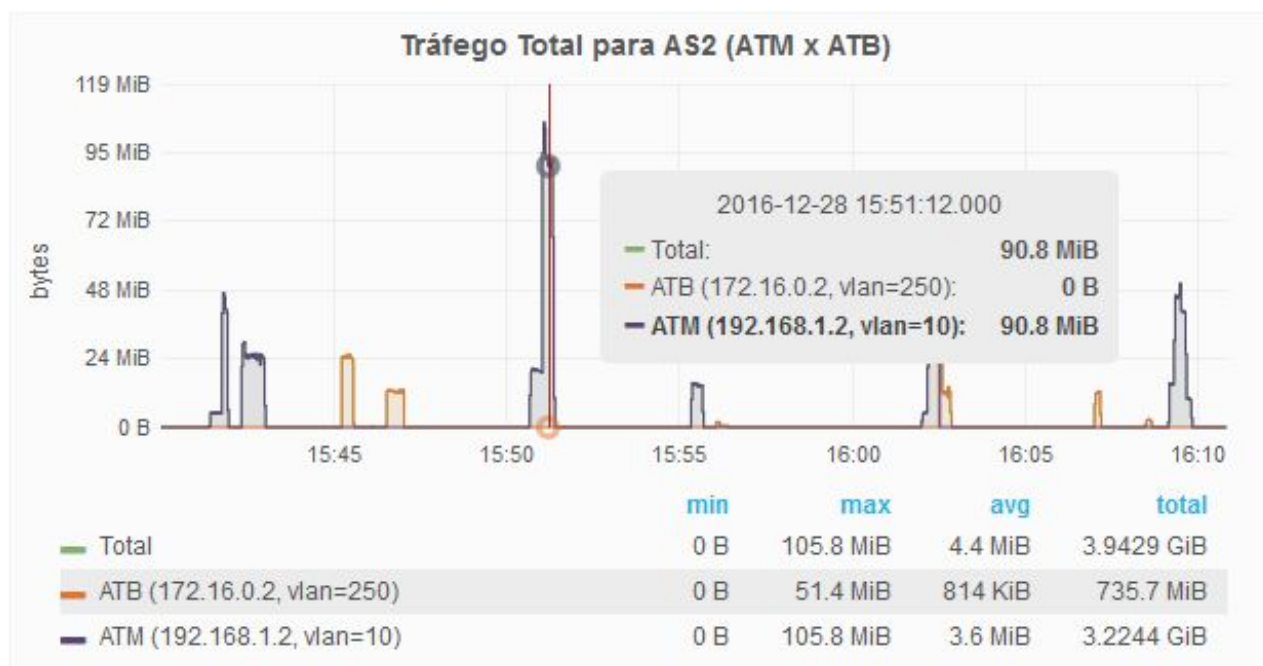
### 3 - Visualização dos dados



**Figura 12.** 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 12 podemos visualizar esta estatística do AS2.

### 3 - Visualização dos dados



**Figura 13.** Tráfego total separado por acordos ATM e ATB e VLAN

Diversas outras estatísticas são possíveis de serem construídas na plataforma, além das já exibidas. A figura 13 mostra um gráfico com o tráfego total para o AS2 separado por acordos (ATM e ATBs) e VLAN.

# 3 - Visualização dos dados

- 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](mailto:guisaulo@hotmail.com)
- Link do vídeo:
  - Youtube: <https://youtu.be/XErL5VwjxfA>
  - Google Drive: <https://goo.gl/KXPgxs>