Departamento de Sistemas e Computação - FURB
Curso de Ciência da Computação
Trabalho de Conclusão de Curso 2 - 2018/1

Comportamento e Desempenho de Redes: Uma Análise Baseada em Fluxos

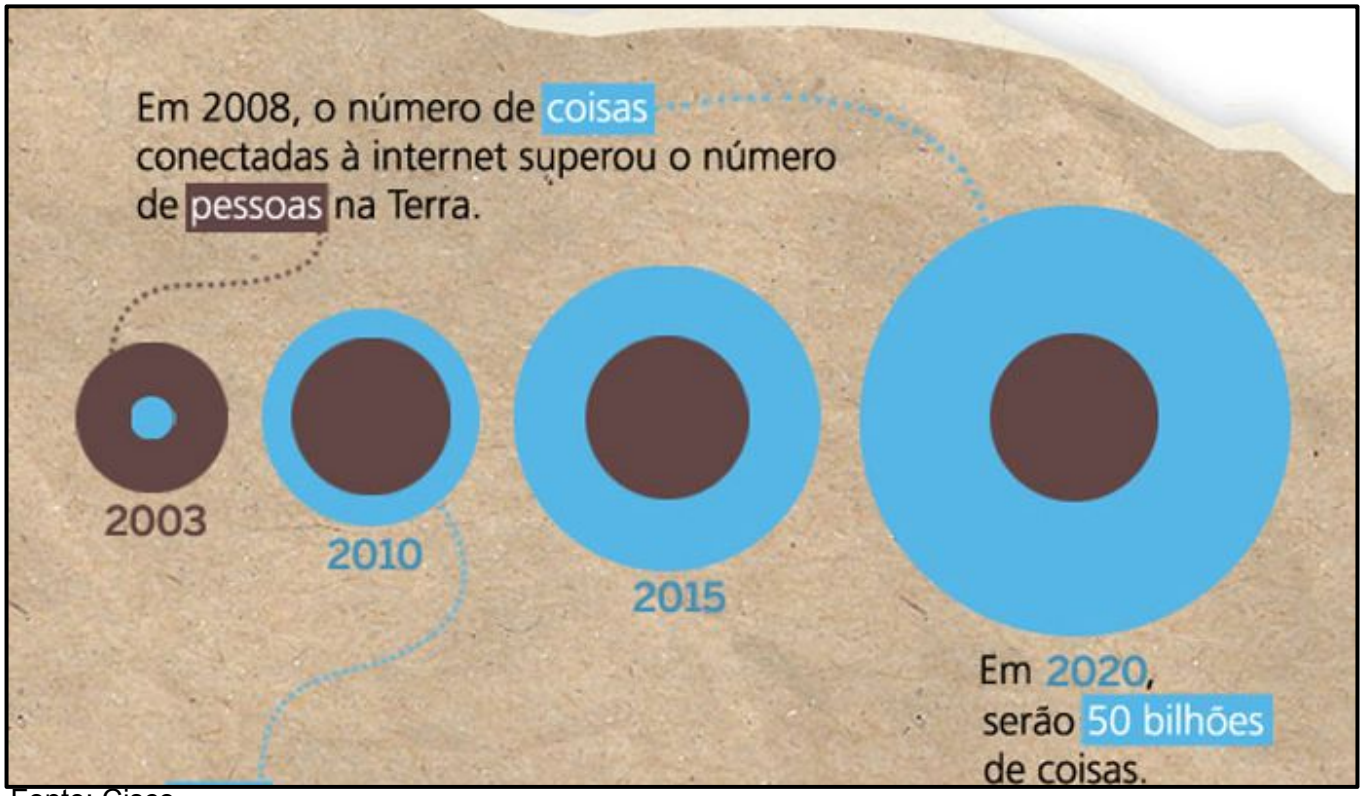
Acadêmico: Guilherme Henrique Ramos
ghrramos@gmail.com

Orientador: Prof. Francisco Adell Péricas
pericas@furb.br

Roteiro

- Motivação
- Trabalhos correlatos
- Objetivos
- Requisitos
- Ferramentas utilizadas
- Especificação
- Implementação
- Resultados
- Conclusões
- Extensões

Motivação



Fonte: Cisco.

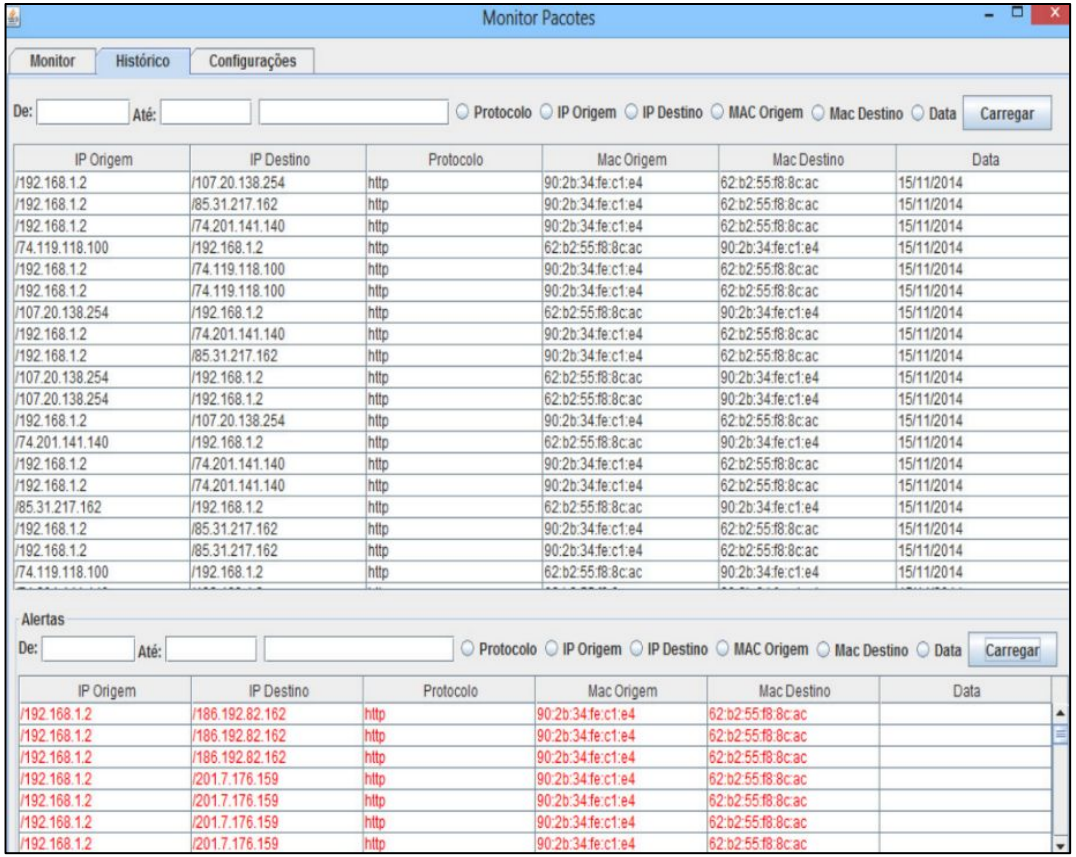
Motivação

- A utilidade/importância da rede aumenta a cada novo dispositivo que se conecta.
- O administrador de rede precisa de estatísticas de desempenho para ajudá-lo a planejar, administrar e manter grandes redes em operação.

Atualmente a Internet é provavelmente o maior sistema de engenharia já criado pela humanidade, com centenas de milhões de computadores conectados (KUROSE, 2013).

Trabalhos Correlatos

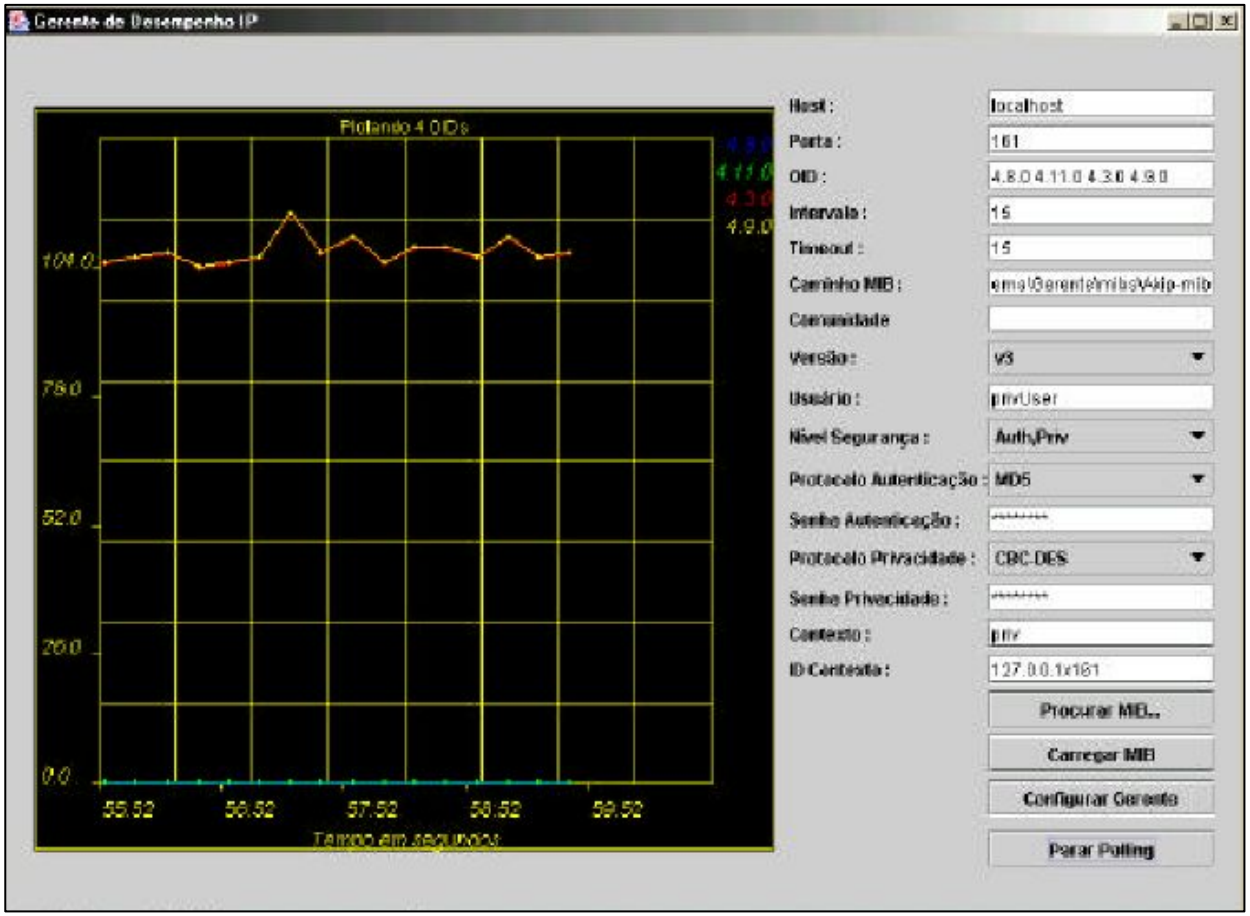
Título: Ferramenta para monitoração e gerenciamento de tráfego em uma rede local



Fonte: Bennertz (2014).

Características/ Correlatos	Bennertz (2014)
Possui agente	✖
Intercepta os pacotes TCP/IP	✔
SNMP V2	✖
SNMP V3	✖
Envia alerta	✔
Cria representações gráficas	✖
Armazena os dados	✔

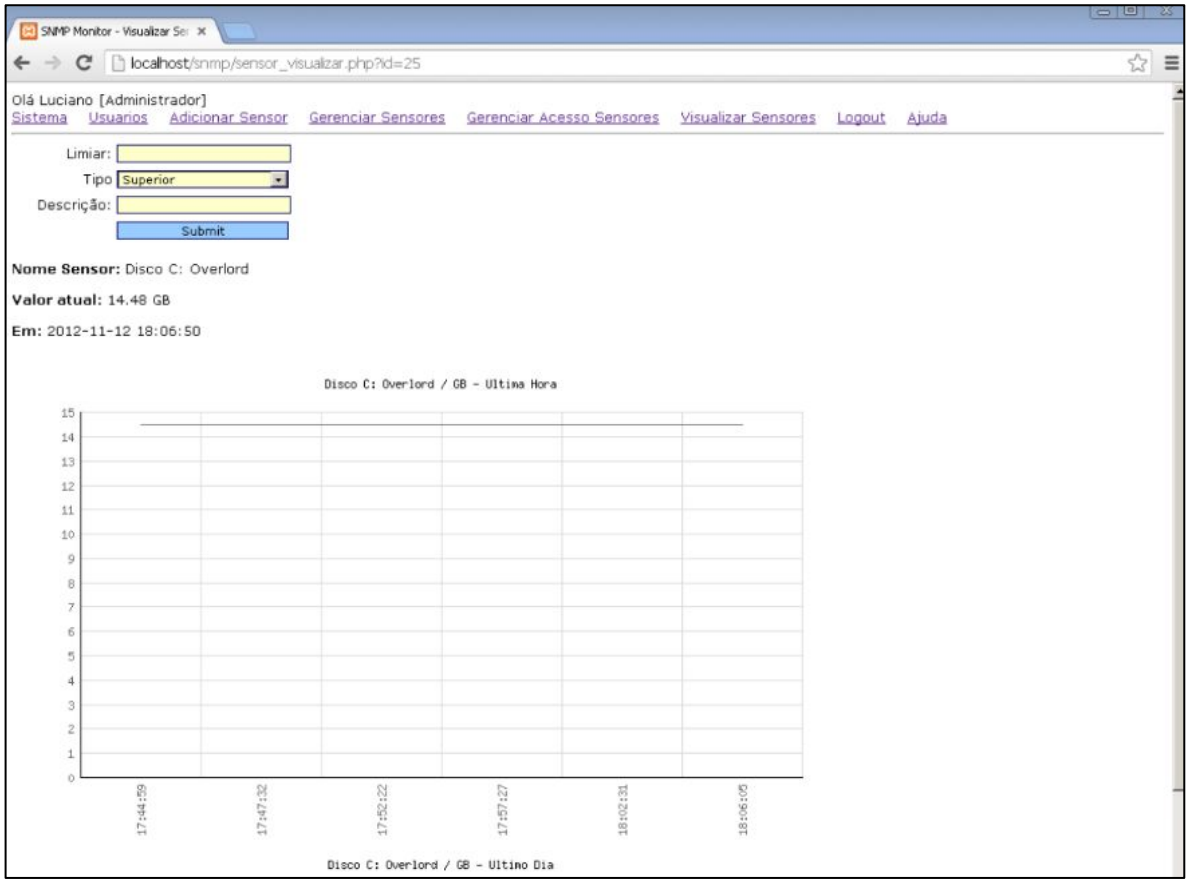
Título: Protótipo de um sistema de monitoramento de desempenho de redes de computadores baseado no protocolo SNMP V3



Fonte: Karing (2002).

Características/ Correlatos	Karing (2002)
Possui agente	✔
Intercepta os pacotes TCP/IP	✖
SNMP V2	✔
SNMP V3	✔
Envia alerta	✖
Cria representações gráficas	✔
Armazena os dados	✖

Título: Monitoramento de servidores e dispositivos de rede utilizando SNMP



Fonte: Lingau (2012).

Características/ Correlatos	Lingnau (2012)
Possui agente	✖
Intercepta os pacotes TCP/IP	✖
SNMP V2	✔
SNMP V3	✖
Envia alerta	✔
Cria representações gráficas	✔
Armazena os dados	✔

Trabalho proposto

Objetivo geral:

O objetivo deste trabalho é desenvolver uma ferramenta para prover informações do comportamento e desempenho da rede, analisando seu fluxo de dados.

Objetivo específicos:

- exportar o fluxo de dados de um equipamento central
- coletar e armazenar o fluxo de dados
- analisar o fluxo de dados
- exibir o resultado da análise na forma de gráficos e tabelas

Fundamentação Teórica

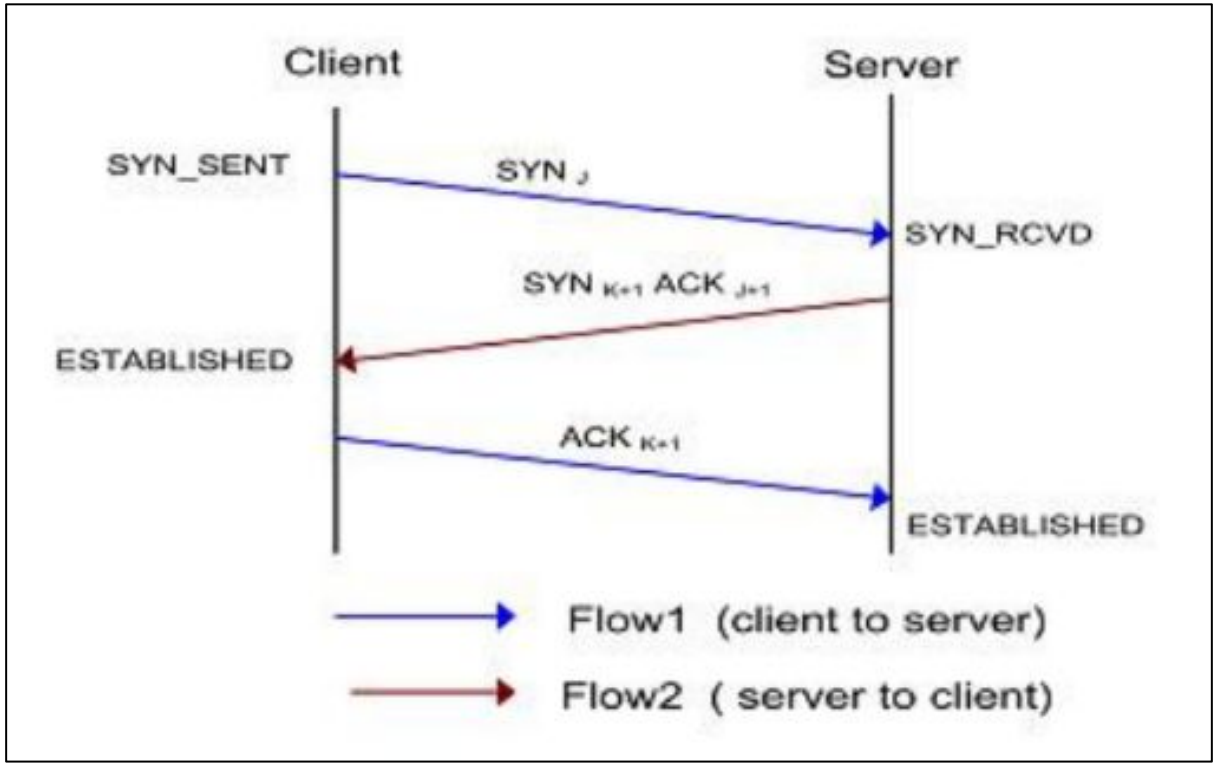
Método de captura

- Método ativo
  - Injeta pacote na rede

- Método passivo
  - Monitora o tráfego por observação

O método escolhido é o **passivo**.

O que é um fluxo?



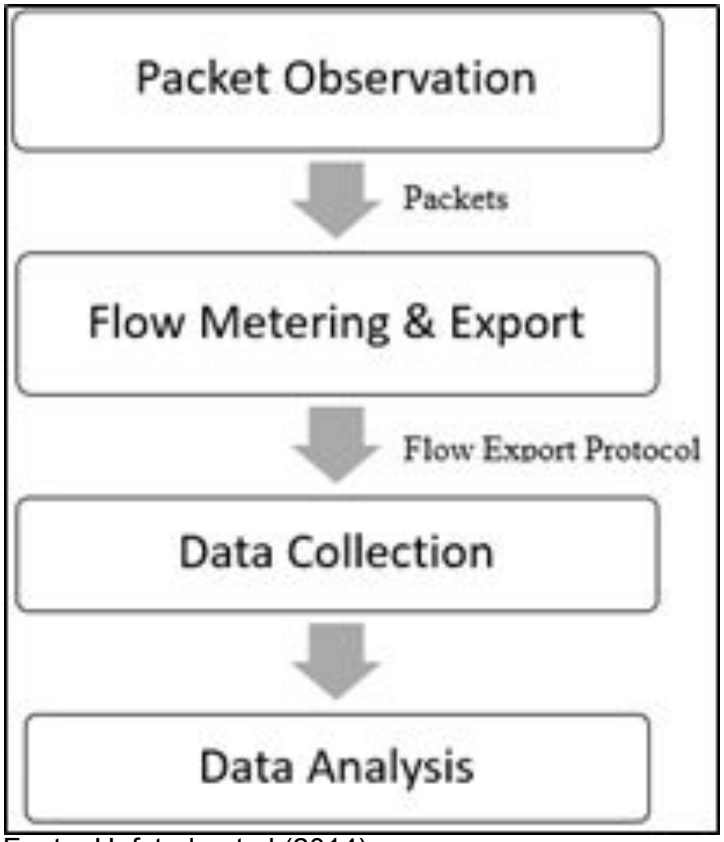
Fonte: Hofstede et al (2014).

Fluxo de Dados

ID	Name	Description
152	flowStartMilliseconds	Timestamp of the flow's first packet.
153	flowEndMilliseconds	Timestamp of the flow's last packet.
8	sourceIPv4Address	IPv4 source address in the packet header.
12	destinationIPv4Address	IPv4 destination address in the packet header.
7	sourceTransportPort	Source port in the transport header.
11	destinationTransportPort	Destination port in the transport header.
4	protocolIdentifier	IP protocol number in the packet header.
2	packetDeltaCount	Number of packets for the flow.
1	octetDeltaCount	Number of octets for the flow.

Fonte: Hofstede et al (2014).

Quais são as etapas?



Fonte: Hofstede et al (2014).

Requisitos funcionais

Requisito	Descrição
RF01	Exibir um gráfico em linha e barra com o total de fluxos
RF02	Exibir um gráfico em linha e barra do consumo diário em GB
RF03	Exibir um gráfico em linha e barra do consumo dos últimos 5 minutos em MB
RF04	Exibir um gráfico em linha dos protocolos TCP, UDP e ICMP
RF05	Exibir um gráfico em pizza dos protocolos utilizados nos últimos 5 min
RF06	Exibir um gráfico em pizza dos top 10 IPs que mais transferiram dados
RF07	Exibir um gráfico em pizza das top 10 origens que mais transferiram dados
RF08	Exibir um gráfico em pizza dos top 10 destinos que mais transferiram dados
RF09	Possibilitar que o usuário escolha visualizar os dados das últimas 24 horas ou 7 dias

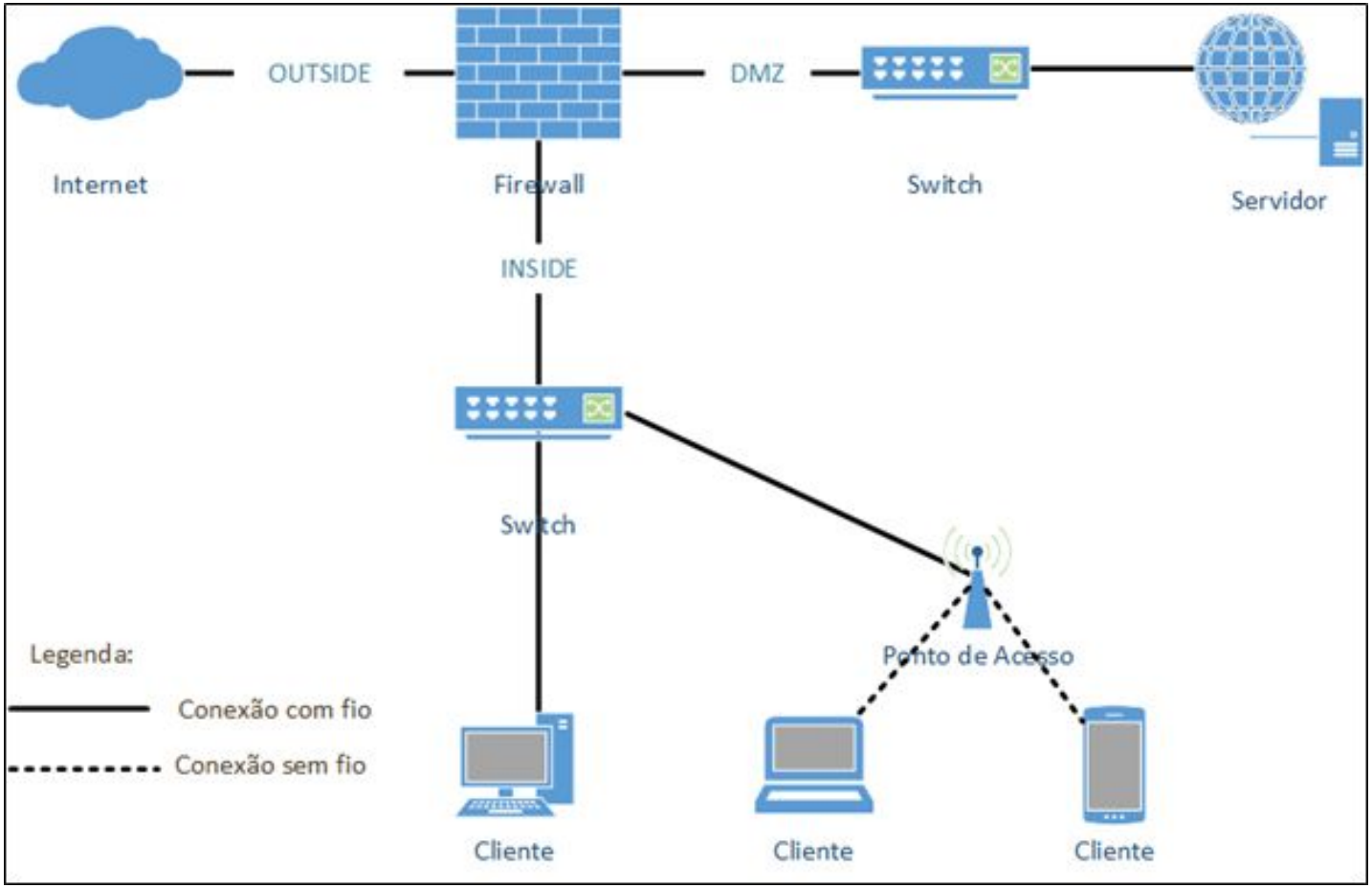
Requisitos não funcionais

Requisito	Descrição
RNF01	Rodar na plataforma Linux
RNF02	Ser desenvolvido para plataforma WEB
RNF03	Utilizar HTML 5, CSS, Bootstrap, JQuery e Java Script no front end
RNF04	Utilizar a biblioteca Chart.js para criar gráficos
RNF05	Ser acessível pelo navegador Google Chrome
RNF06	Coletar o fluxo de dados exportado com a ferramenta Nfcap
RNF07	Utilizar a ferramenta nfdump para leitura e análise dos registros
RNF08	Armazenar os resultados obtidos da leitura e análise em arquivos JSON

Ferramentas utilizadas

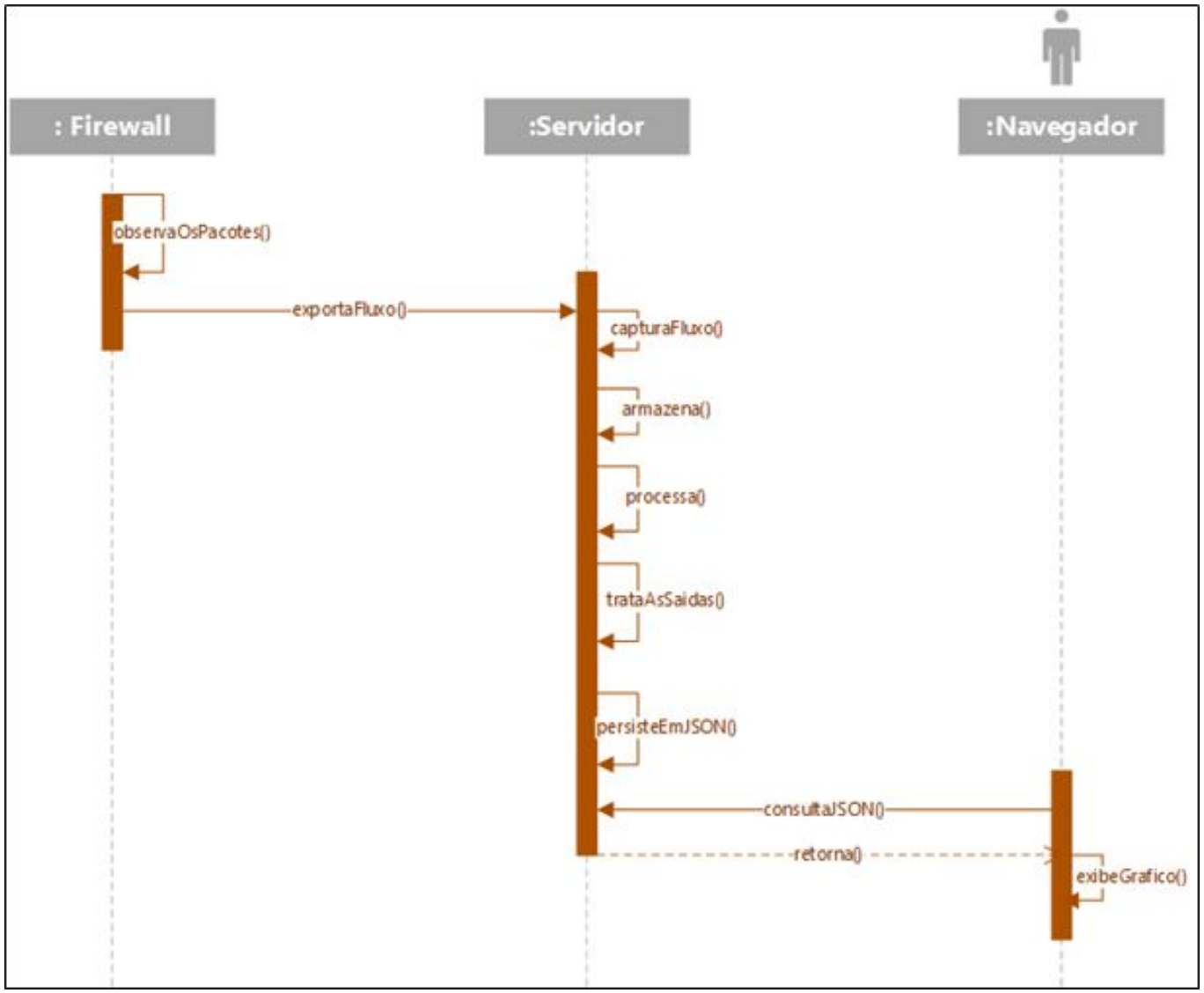
- Visual Studio Code
- Tcpdump
- Nfdump
- CSVtoJSON
- Java Script
  - Chart.js
- Shell script

Especificação



Fonte: elaborado pelo autor.

Especificação



Fonte: elaborado pelo autor.

Implementação

```
#!/bin/sh

scriptName='ipByBytes'
data_path='/var/www/html/data/'
tmp_path='/home/netflow/git/flow-script/tmp/'
log='/var/www/html/log/flow.log'

output="${tmp_path}${scriptName}.csv"
data="${data_path}${scriptName}.json"

echo $(date +"%b %d %H:%M:%S") $scriptName'['$$']:' Start >> $log

nfdump -r $1 -s ip/bytes -o csv > $output

top_10=$(sed -n '1,11p' $output | csv2json)
summary=$(sed -n '14,15p' $output | csv2json | sed -n '2p')

echo '{ "top_10": '  $top_10  ', "summary":'  $summary  ' }' > $data

echo $(date +"%b %d %H:%M:%S") $scriptName'['$$']:' End >> $log
```

Fonte: elaborado pelo autor.

Implementação

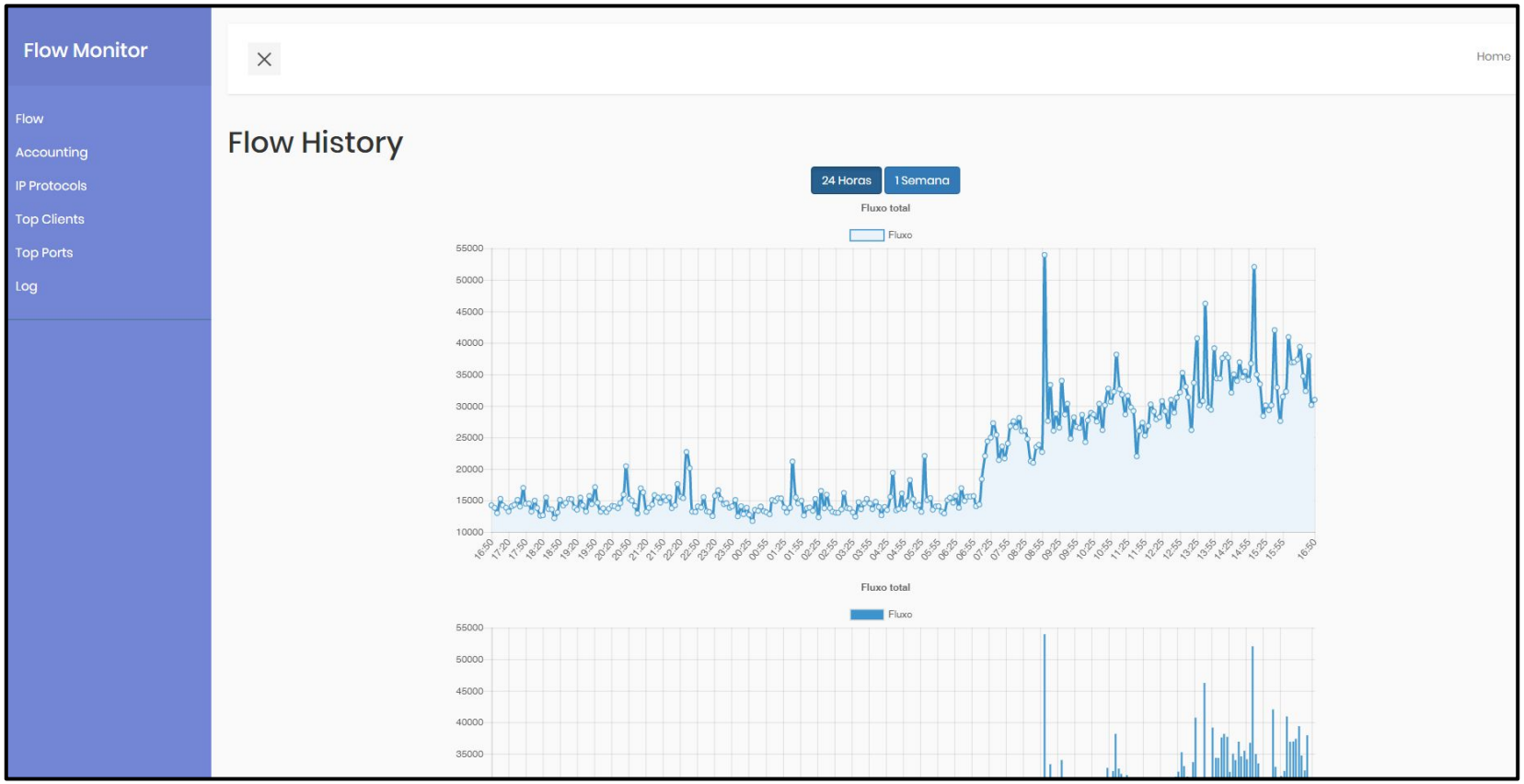
```
fetch(url)
  .then(resp => resp.json())
  .then(arquivo => {
    const total = arquivo.top_10.length;
    const inicio = total - dias * 288;
    const horas = arquivo.top_10.map(funcao[0]).slice(inicio, total);
    let dados;

    if (funcao.length > 2) {
      dados = arquivo.top_10
        .map(funcao[1])
        .map(funcao[2])
        .slice(inicio, total);
    } else {
      dados = arquivo.top_10.map(funcao[1]).slice(inicio, total);
    }

    //Line chart
    new Chart(doc, {
      type: tipo,
      data: {
        labels: horas,
        datasets: [
          {
            data: dados,
            label: label,
            borderColor: "#3e95cd",
            backgroundColor: "#ebf4fa",
            fill: true
          }
        ]
      },
      options: {
        title: {
          display: true,
          text: titulo
        }
```

Fonte: elaborado pelo autor.

Resultados



Fonte: elaborado pelo autor.

Resultados

Características/ Correlatos	Bennertz (2014)	Karing (2002)	Lingnau (2012)	Ramos (2018)
Possui agente	✖	✔	✖	✖
Intercepta os pacotes TCP/IP	✔	✖	✖	✖
SNMP V2	✖	✔	✔	✖
SNMP V3	✖	✔	✖	✖
Envia alerta	✔	✖	✔	✖
Cria representações gráficas	✖	✔	✔	✔
Armazena os dados	✔	✖	✔	✔

Conclusões

- Os objetivos foram alcançados com resultados satisfatórios
- A ferramenta proporciona agilidade no monitoramento
- Serve como base para outros trabalhos com foco no monitoramento de desempenho, contabilização e segurança que utilizem fluxo de dados.

Sugestões

Sugere-se para trabalhos futuros:

- persistir os dados em banco de dados
- implementar controle de acesso
- emitir alerta no navegador
- enviar alerta por e-mail
- enviar relatório diário, semanal e mensal

Obrigado!

Perguntas?

Guilherme Henrique Ramos
ghrramos@gmail.com