Uma Proposta de Infra-estrutura de Medições para o Tráfego do Backbone da RNP2

Leobino Nascimento Sampaio
e-mail: leobino@unifacs.br

José A. Suruagy
e-mail: suruagy@unifacs.br

RNP

Abril - 2003

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Roteiro

- Apresentação do GT-QoS
- Infra-estrutura de medições
- Proposta de implantação na RNP2
- Ambiente de visualização
- Experimentos realizados
- Trabalhos futuros

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

GT-QoS

- Formação
  - Base: coordenadores de Projetos de Redes Avançadas (Edital CNPq/RNP) relacionados
- Articulação com os Projetos de Redes Avançadas
  - Atividades/objetivos comuns
  - Necessidade de QoS: definição de uma arquitetura mínima de serviços

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

GT-QoS

- Objetivos
  - Definição/detalhamento de uma arquitetura de serviços com diferenciação de QoS para a RNP2
  - Implementação de uma infra-estrutura de medições com a finalidade de monitorar a QoS que está sendo oferecida para as diversas classes de serviços

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Infra-estrutura de medições

- Motivações
  - Necessidade de monitorar o tráfego para checar se os objetivos de QoS estão sendo atendidos.
  - Falta de informações específicas sobre o tráfego e sua tendência.
  - Necessidade de visualização das características do tráfego
  - Necessidade de visualização dos fluxos de tráfego entre os diversos POPs

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Infra-estrutura de medições

- Objetivos
  - Desenvolver um ambiente de coleta, acompanhamento e visualização de resultados sobre as características da rede.
  - Obter um ambiente de visualização que permita uma análise mais precisa da rede a fim de definir a prioridade dos serviços.
  - Saber a composição, origem e destino do tráfego (Matriz de tráfego) e a sua evolução

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Infra-estrutura de medições

- Métricas de interesse
  - Largura de banda
  - Atraso
  - Jitter
  - Perda de pacotes
  - Utilização
  - Caracterização do tráfego

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Tipos de Medições

- Ativas
  - São gerados pacotes de teste e depois medido o desempenho do mesmo através da rede.
    - Problemas: Falta de sincronização dos relógios e tráfego extra na rede
    - Ideais para medições de jitter, atraso, perda e latência

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Tipos de Medições

- Passivas
  - São coletadas informações sobre todos os pacotes que trafegam na rede sem fazer nenhuma interferência
    - Requer maiores investimentos na infra-estrutura de equipamentos.
    - Ideais para caracterização do tráfego e medições da largura de banda utilizada.

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Modelo RTFM

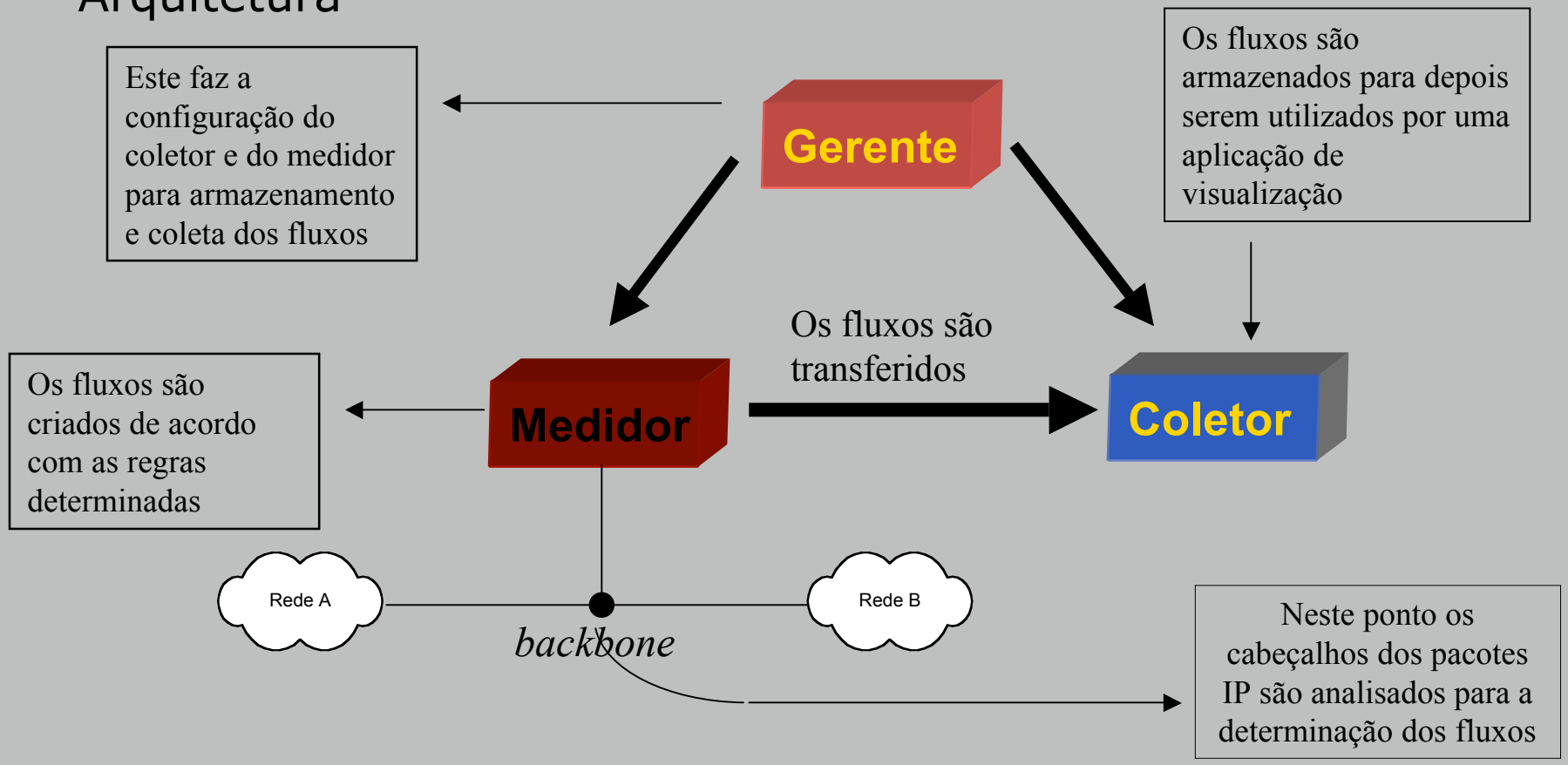
- Medições por fluxo de tráfego (passivas)
- RFCs 2720 - 2724
- O Netramet é a sua principal implementação
- Formado por três componentes:
  - Medidor
  - Coletor
  - Gerente

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Modelo RTFM

- Arquitetura



RNP

UNIVERSIDADE SALVADOR

Cisco Netflow

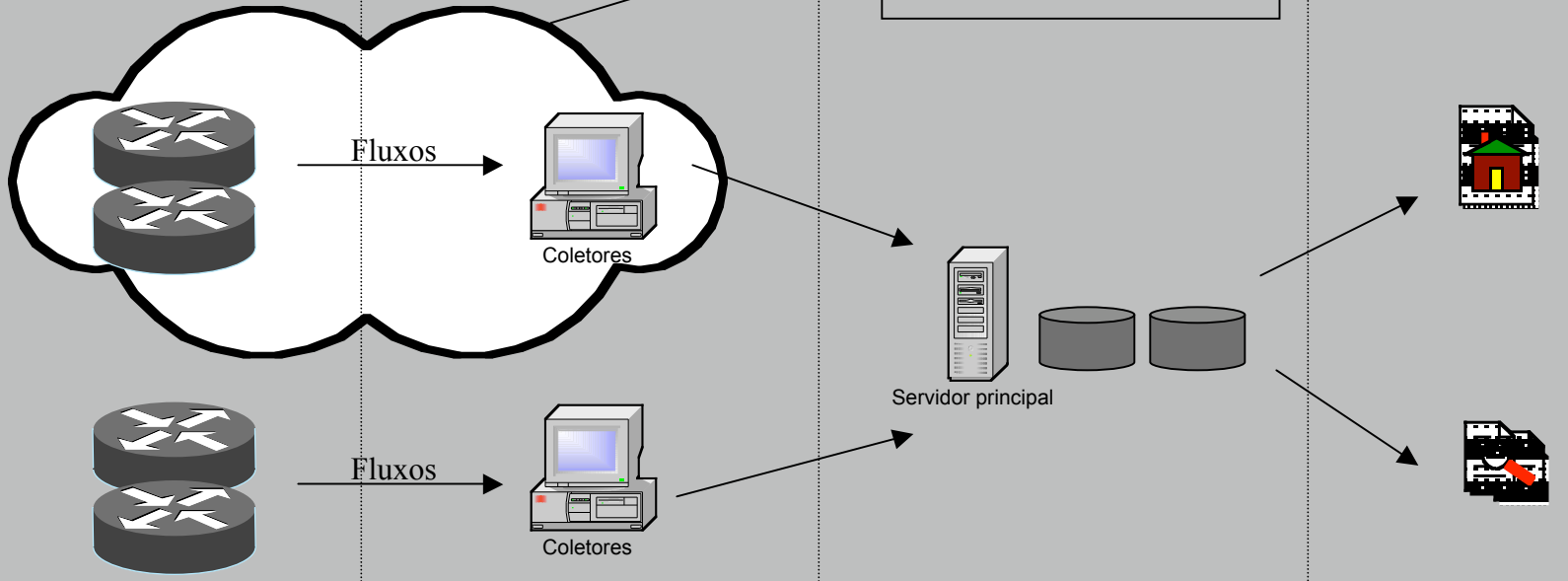
- Fácil implementação
- Baixo custo
- Todos os fluxos identificados são provenientes do tráfego que passa pelo roteador
- Versões 1,5,7,8 (recentemente lançada versão 9)
  - Cada versão possui um formato de cabeçalho
  - Suporte a fluxos agregados a partir da versão 8
  - Suporte ao campo ToS

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Cisco Netflow

Arquitetura



Ciscos da rede com Netflow ativo

Maquinas que recebem os fluxos através de uma porta UDP

Servidor que concentra todos os fluxos de interesse

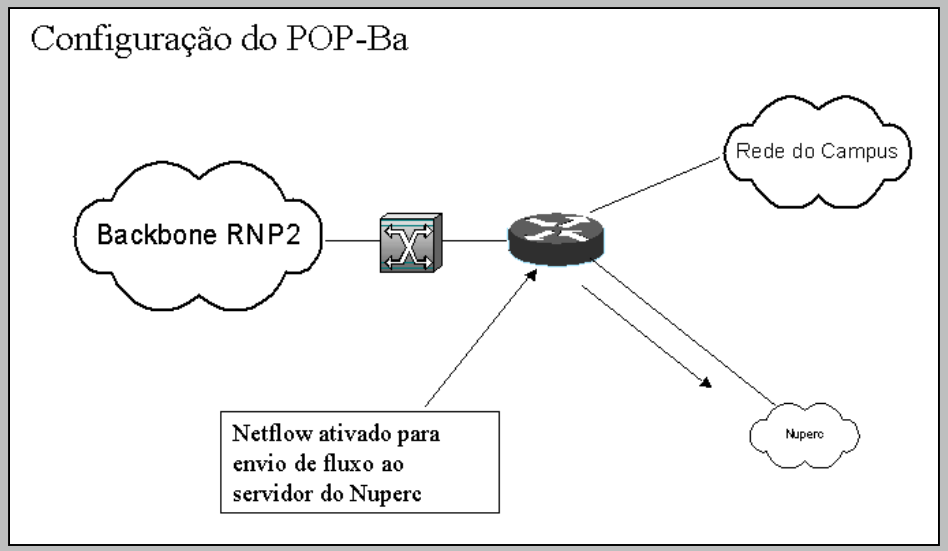
Dados são utilizados pelas aplicações para contabilidade, provisão, diagnósticos, etc.

RNP

UNIVERSIDADE SALVADOR

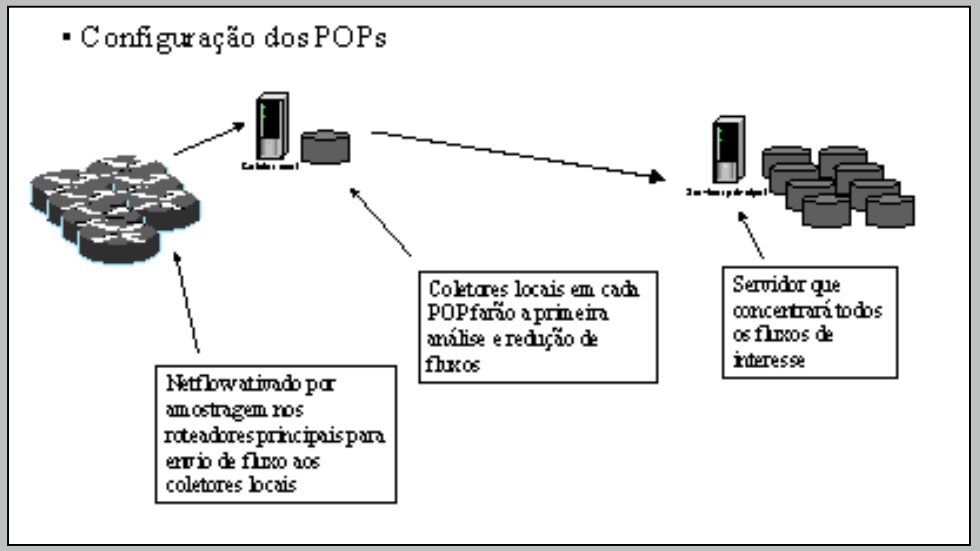
Testes realizados na RNP2

- Experimentos iniciais no POP-Ba
- Netflow habilitado no principal roteador
- Fluxos enviados a um servidor de coleta
- Coleta feita através do pacote flow-tools



Estágio atual

- Máquinas coletoras estão sendo configuradas nos POPs para coleta local.
- Transferência dos dados realizadas para um servidor central num horário de menor tráfego.
- Estudos estão sendo direcionados para o gerenciamento e análise dos dados coletados



RNP

UNIVERSIDADE SALVADOR

Ambiente de visualização

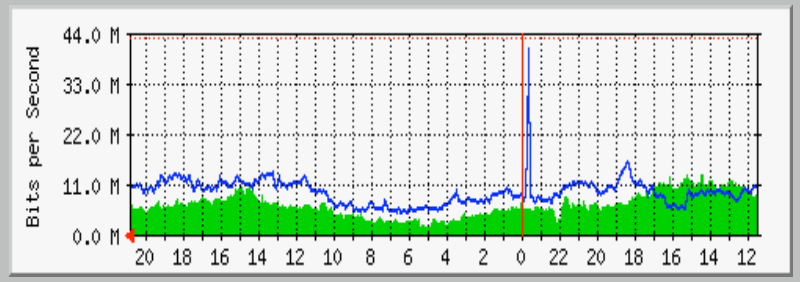
- Com um bom ambiente de gerência e visualização, pode-se identificar:
  - As anomalias na rede;
  - O uso indevido (Ex.: tentativas de varreduras);
  - Tendências do tráfego;
  - Serviços que consomem maior banda;
  - Características das subredes dos POPs.

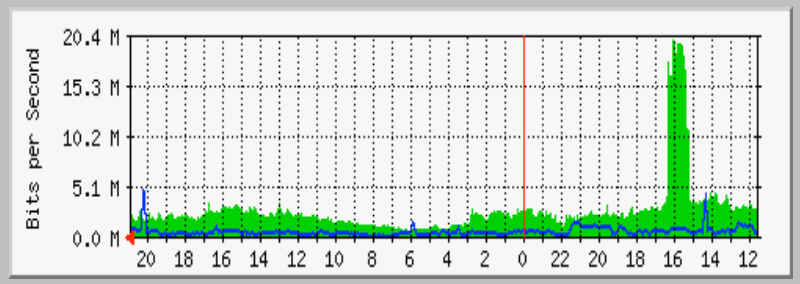
RNP

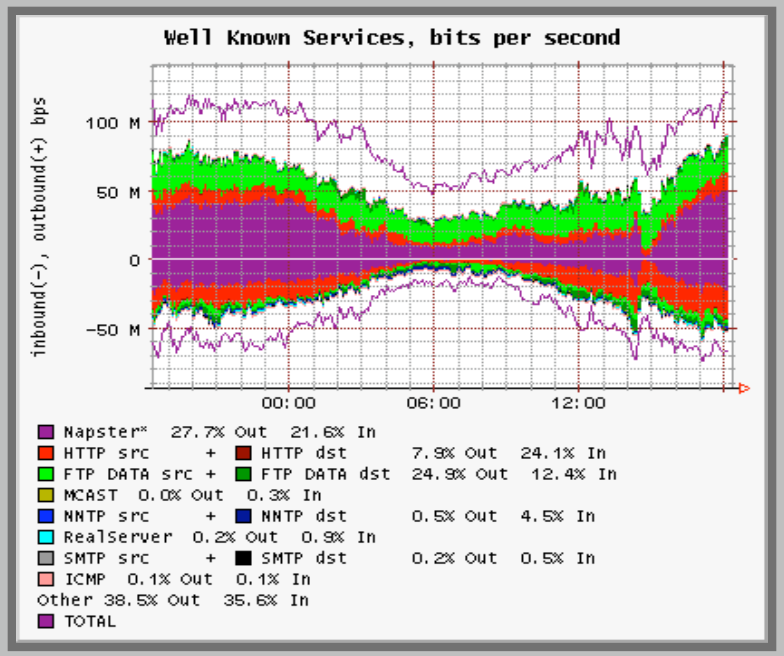
UNIFACS UNIVERSIDADE SALVADOR BAHIA

Ambiente de visualização (Estágio atual)

MRTG -> Flowscan







RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Experimentos

- Técnica de Mapas em árvores em conjunto com medições por fluxo.
  - Pacote flow-tools para seleção e coleta de fluxos.
  - Visualização dos dados através de hierarquias.
  - Utilização dos parâmetros: Cor e Tamanho para identificação de outras características

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Técnica de Mapas em Árvore

- Explora a capacidade do sistema visual humano de perceber pequenas diferenças nas cores, tamanho e posição.
- Representação de dados hierárquicos
- Pode ser utilizado para a visualização de todo o backbone numa única cena visual.

RNP

UNIVERSIDADE SALVADOR
UNIFACS
BAHIA

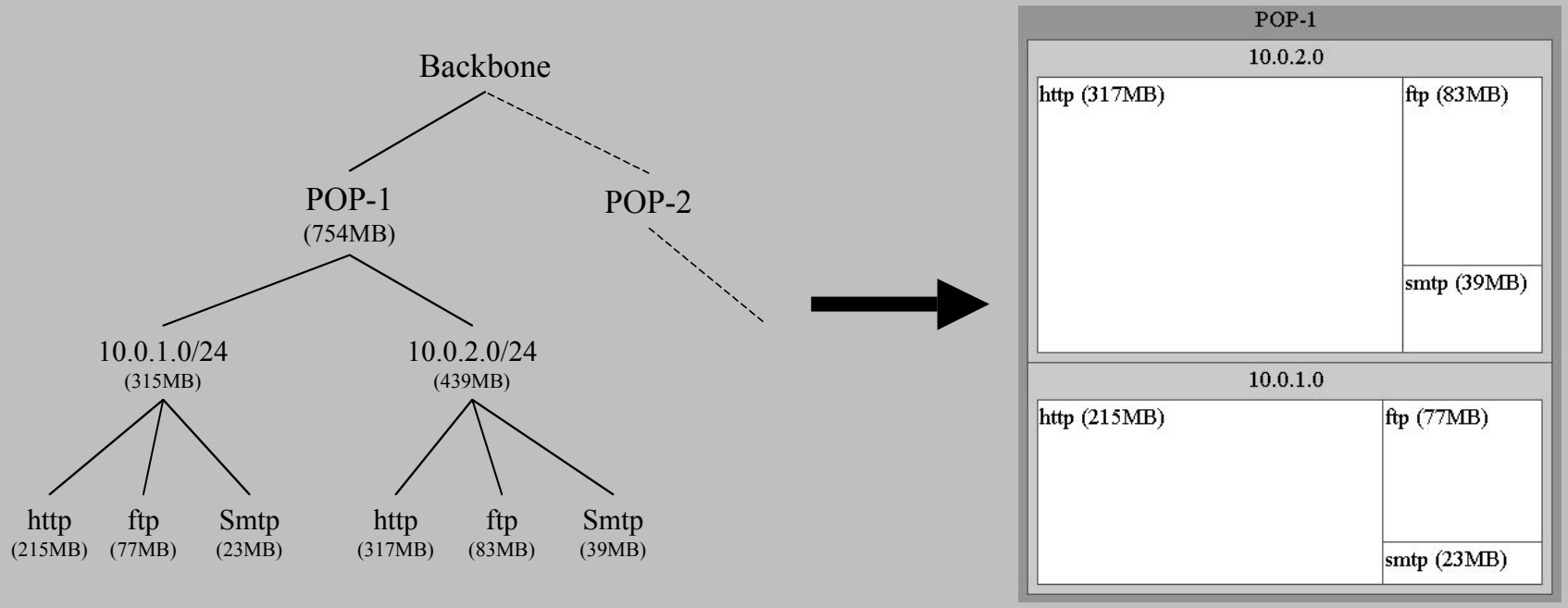
Técnica de Mapas em Árvore

- Redes IP podem ser representadas através de hierarquias
- Cada nível da hierarquia pode mostrar dados mais específicos. (ex. Subredes, serviços, etc.)
- Cor, tamanho e outros atributos podem ser utilizados para representar outros detalhes da rede.

RNP

UNIVERSIDADE SALVADOR UNIFACS BAHIA

Técnica de Mapas em Árvore



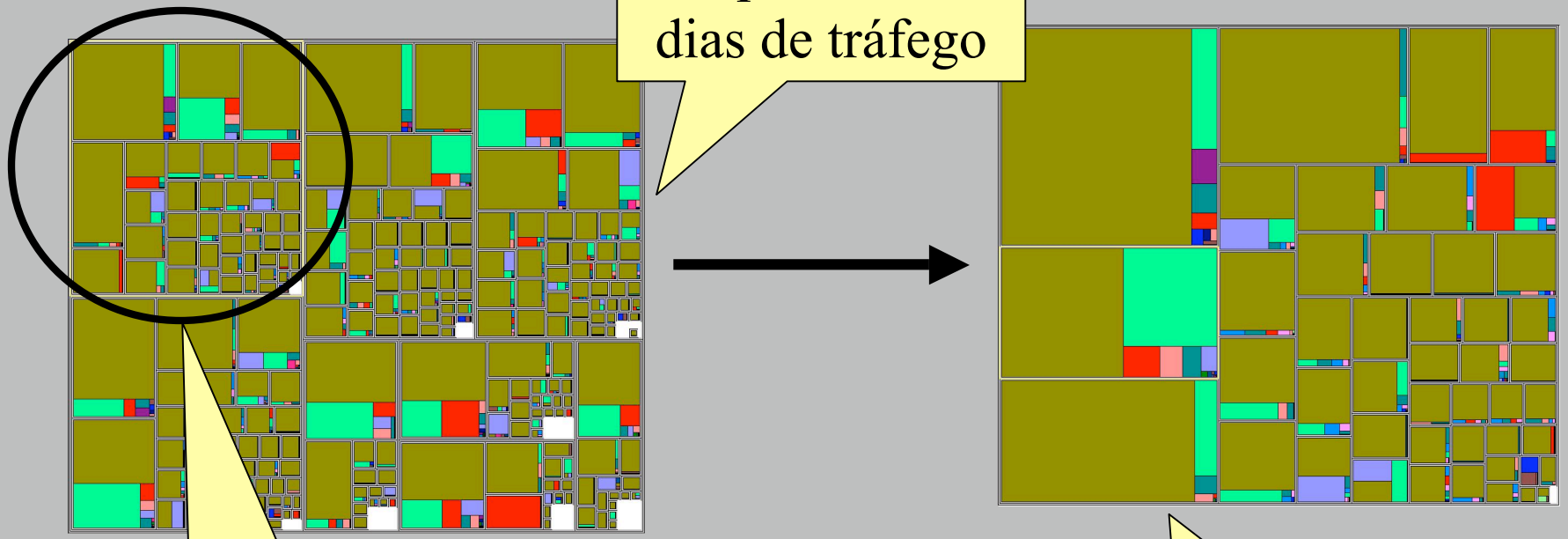
Experimento 1

- Caracterização do tráfego
  - Fluxo agregados a partir das redes
  - 7 dias de testes
  - Hierarquia “Data –> Rede”
  - Cor representa os serviços
  - Tamanho o volume do tráfego

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Experimento 1



Representa 7 dias de tráfego

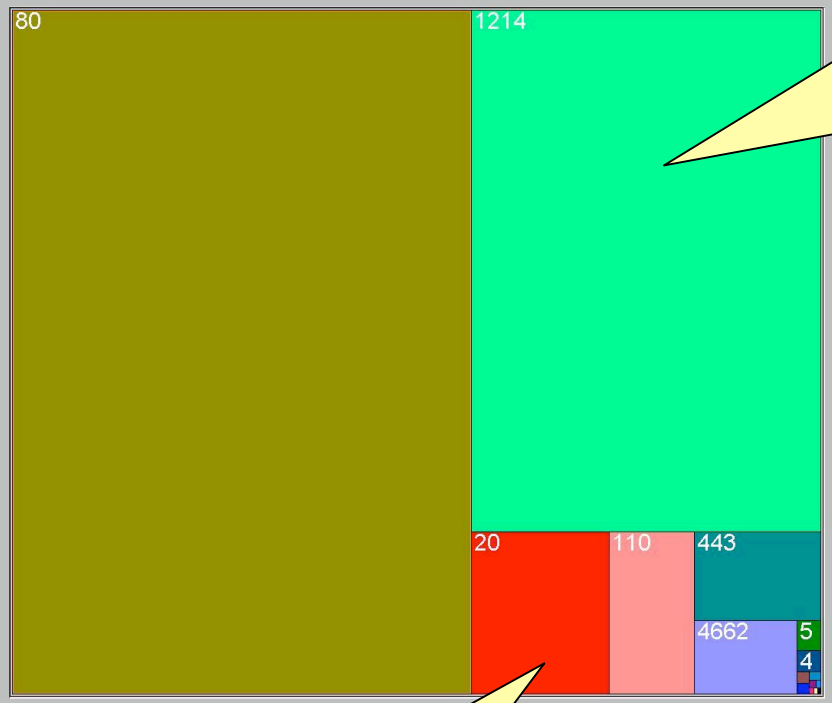
Quadro que representa 1 dia

Com um zoom é possível verificar mais detalhes do dia

RNP

UNIVERSIDADE SALVADOR
UNIFACS
BAHIA

Experimento 1



Representação de apenas uma rede

O tamanho representa o volume do tráfego

A cor representa o serviço

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Experimento 2

- Identificação de anomalias
  - Relação fluxo/octetos criada.
  - Detecção de ataques
  - Portscan/hostscan significa:
    - Uma origem – Diversos dest em 1 porta
    - Uma origem – 1 dest em muitas portas

RNP

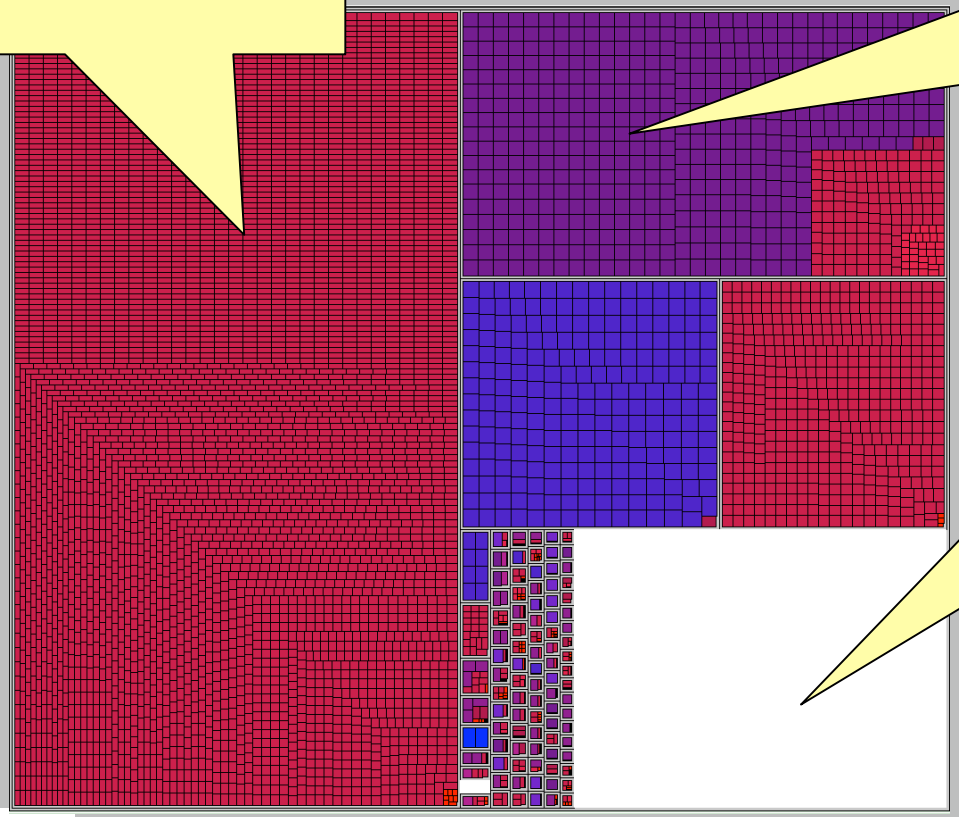
UNIVERSIDADE SALVADOR

Experimento 2

- Identificação de anomalias
  - Port 25
  - 12.360 flows
  - Hierarquia “Origin IP -> Dest IP”
  - Cor representa a relação fluxo/octetos
  - Tamanho representa o volume de destinos vindo de uma única origem.

Experimento 2

Quadros maiores representam uma origem para vários destinos



Cores escuras representam baixo número de octetos por fluxo

Quadros brancos representam situações normais

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Trabalhos Futuros

- Testes com novas ferramentas e técnicas de visualização.
- Análise estatística dos dados coletados.
- Medições dos serviços diferenciados na rede de produção
- Implantação do piloto de medições ativas.

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA

Dúvidas?

leobino@unifacs.br

suruagy@unifacs.br

RNP

UNIFACS UNIVERSIDADE SALVADOR BAHIA