Criando um monitor de tráfego de baixo custo para redes de alta velocidade

RNP / PoP-PR

GTER 26 - São Paulo/SP - 07 de Novembro de 2008

Pedro R. Torres Jr. `torres@pop-pr.rnp.br`
PoP-PR - Ponto de Presença da RNP no Paraná

Agenda

1. Introdução
2. Sobre o PFRING
3. PFRING em ação
4. Desempenho
5. Conclusão

Captura de Tráfego Passiva

Sistemas de monitoramento passivo capturam o tráfego passando na rede para:

- Detectar problemas de comunicação
- Detectar problemas com segurança da informação (IDS, IPS)
- Computar estatísticas de uso de cada protocolo na rede
- Engenharia de Tráfego

Alternativas para captura de tráfego passiva

Equipamentos

- Acesso direto a interface
- Network TAP
- Espelhamento de porta do switch (ethernet)

Software para manipular tráfego

- Libpcap
  - ethereal
  - tcpdump
  - wireshark
  - nTop
  - fprobe
  - nprobe

Espelhamento de porta

Vantagens

- Fácil de usar
- Disponível em diversos equipamentos

Desvantagens

- Ocupa recurso do switch
- Limitado a velocidade da porta (TX+RX)
- Limita outras features do equipamento

Alternativa

SO Padrão

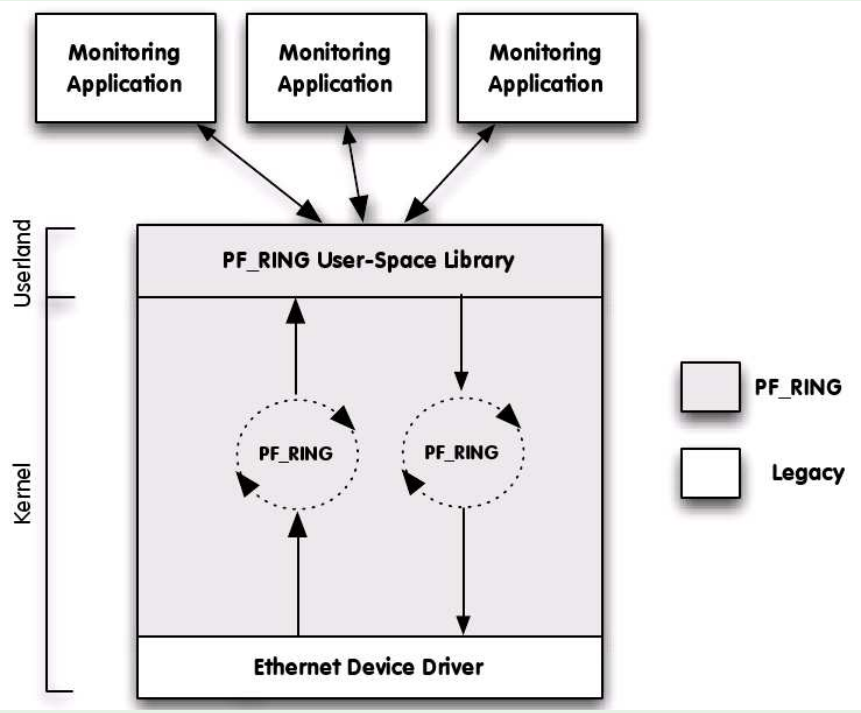
- Dificuldade para manipular grande quantidade de tráfego
- Sistema Operacional não adaptado para monitoramento da rede
- Muitos drivers da interfaces de rede não são otimizados

O que é o PFRING?

- Otimização para captura de pacotes em ambiente Linux
- Melhora consideravelmente a velocidade de captura de pacotes
  - Disponível para kernel 2.4 e 2.6
  - Independente do dispositivo de rede
  - Suporte a libpcap

Funcionamento

Coleta dos dados:



Importante

libpcap

- Aplicações que são bcap-based precisam ser recompiladas com a nova libpcap e também serem linkadas com o PFRING.
- Somente desta maneira as aplicações terão acesso aos benefícios do PFRING.

NAPI - Controle de Interrupções

- Suporte a NAPI no driver do dispositivo de rede é altamente recomendável

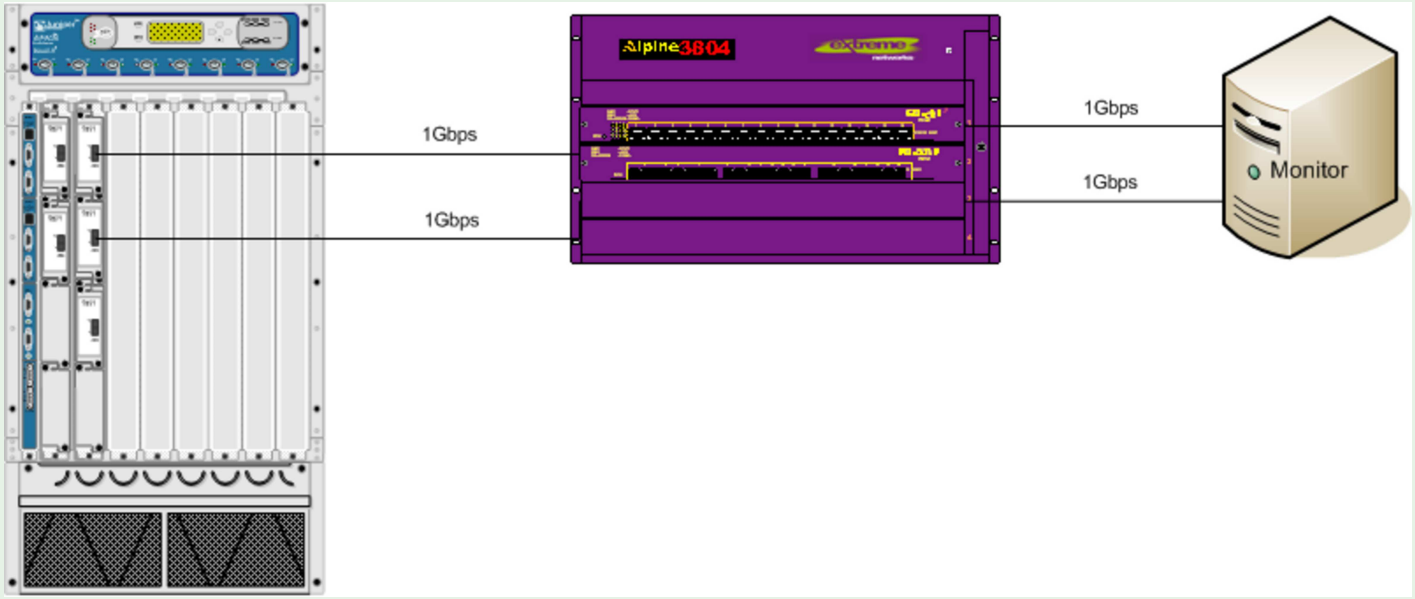
Uso no PoP-PR

Ambiente de uso

- Tráfego do PoP-PR > 1.5Gbps (TX+RX)
- Provedor de Trânsito: RNP
- Link-aggregation - 2Gbps
- Não há um bom suporte a sFlow/NetFlow nos equipamentos utilizados

Uso no PoP-PR

Topologia



Solução

Configuração do Switch-Router do PoP-PR

- Porta a ser espelhada é um link-aggregation
- Porta com o espelho do tráfico também é um link-aggregation (2 portas).
- Suporte a espelhamento de até 2Gbps (TX+RX)

Host - Hardware

- Intel Core2Duo 6700 @2.66Hz
- Memória RAM 4GB
- Duas Interfaces Intel e1000e

Solução

Host - Software

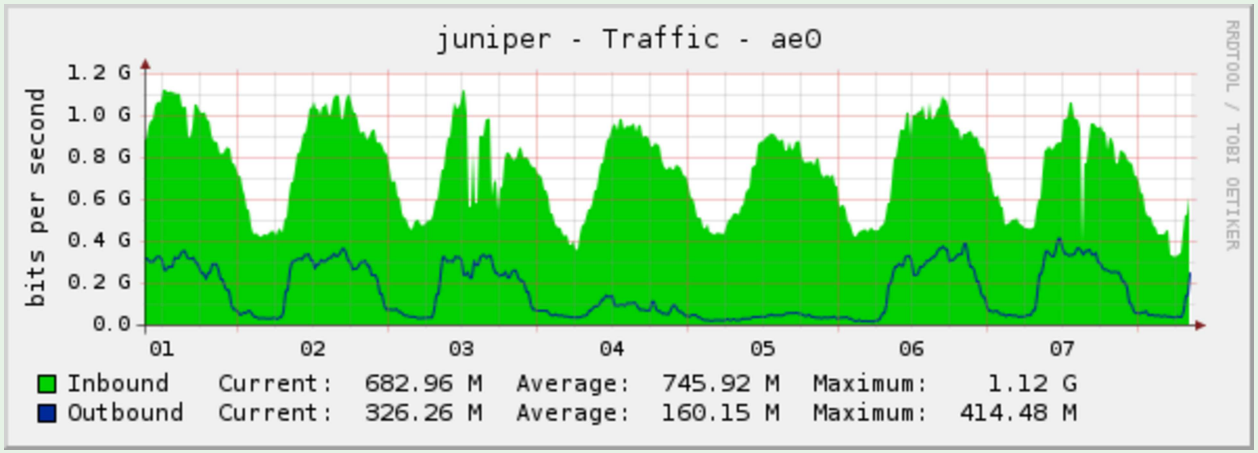
- GNU/Linux 2.6.25
- PFRING 3.8.2
- Suporte a NAPI no driver das interfaces
- Suporte a link-aggregation (bonding)

Host - Software - Coleta

- nProbe 4.9.4 (sendo migrado para 5.0)
- Probes NetFlow são enviados para outro host

Desempenho

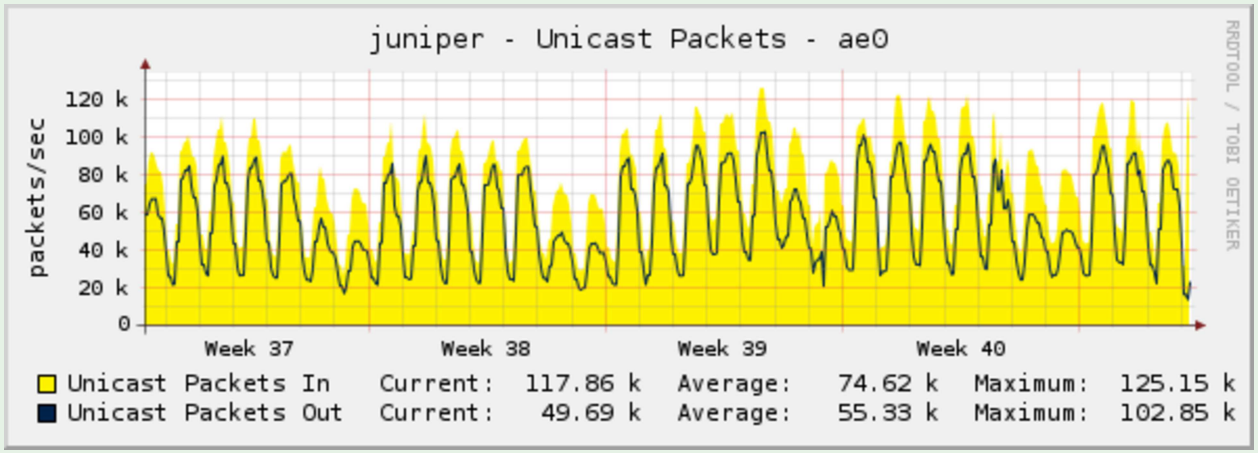
Tráfego a ser manipulado - bps



- TX + RX aprox. 1.5Gbps
- Pode chegar até a 4Gbps (2Gbps full-duplex)

Desempenho

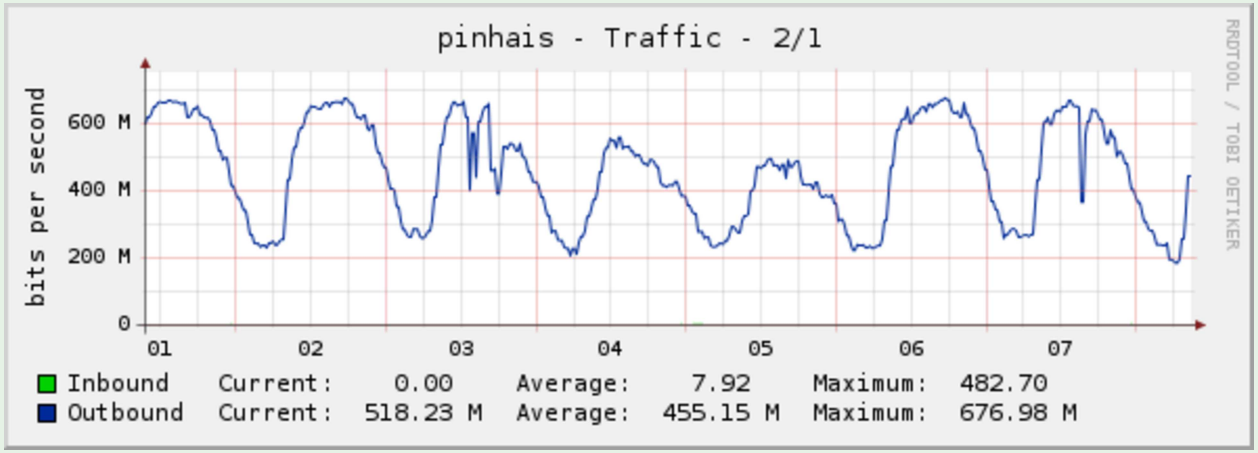
Tráfego a ser manipulado - pps

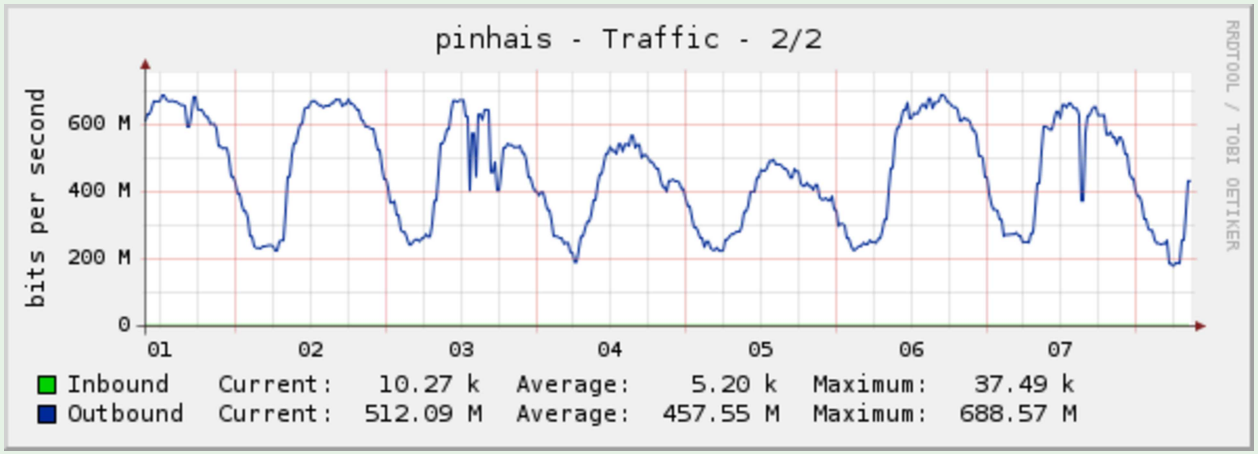


- TX + RX aprox. 230kpps
- Suporta naturalmente condições de ataque (+150kpps)

Desempenho

Tráfego Espelhado

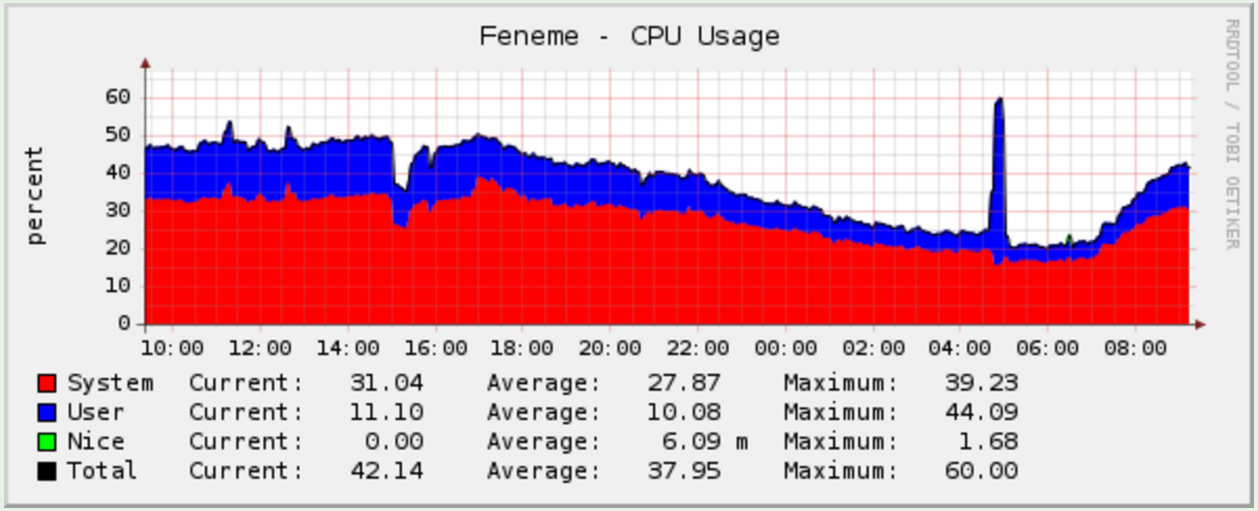




- Capacidade de espelhar 2Gbps

Desempenho

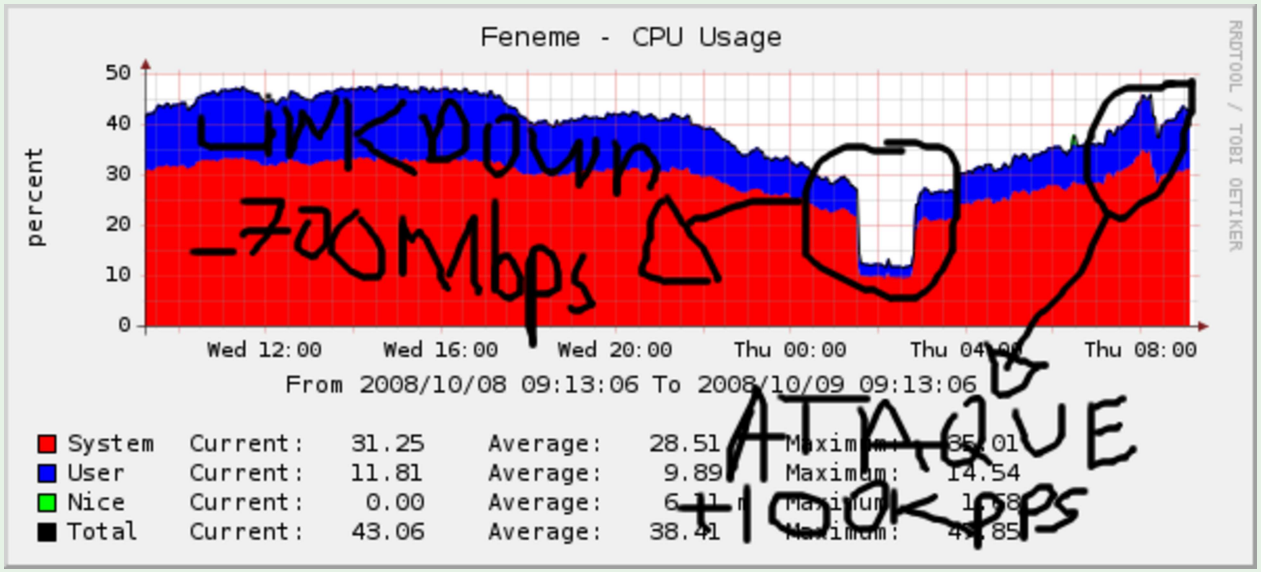
Uso da CPU



- 50% de utilização total
- Prevalece o uso da CPU pelo sistema (atender interrupções)

Desempenho

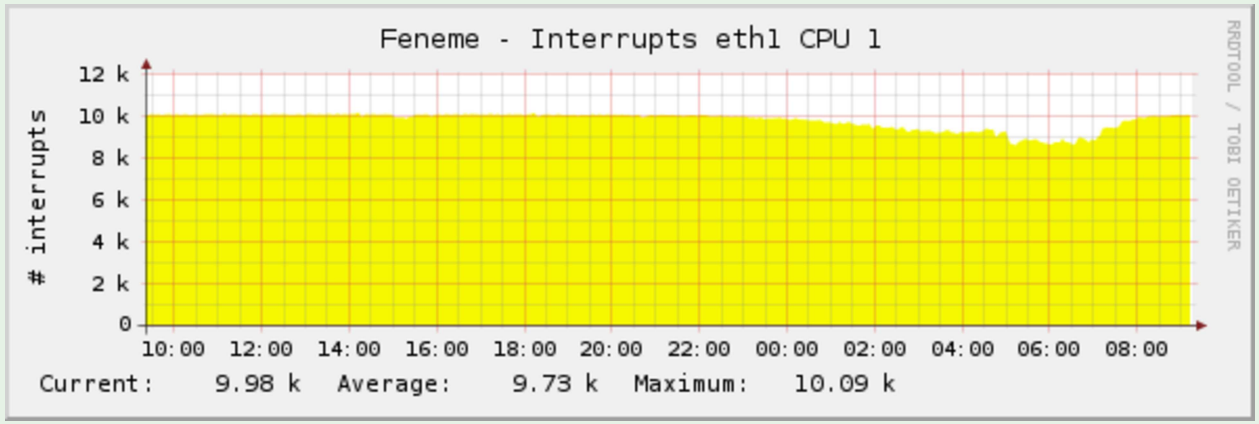
Uso da CPU - Ataque na rede

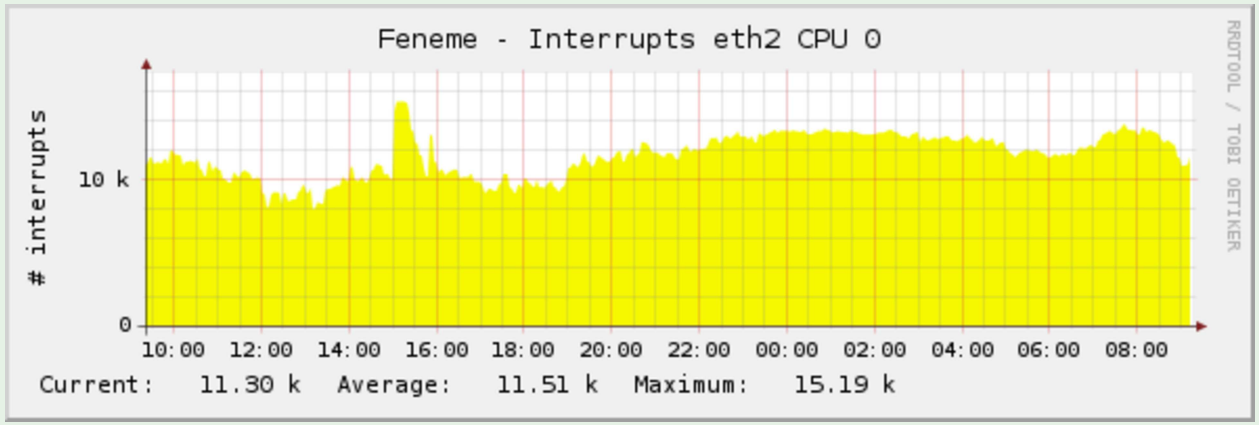


- Ataque de +100kpps na rede
- Uso da CPU não sobe muito (<50%)
- Controle de interrupções mantém CPU estável
- Host de monitoramente já passou por ataques maiores
- Um ataque em um link 1Gbps pode atingir quase 2Mpps!!!

Desempenho

Interrupções no sistema





- Interrupções estão balanceadas em cada CPU (dual-core)

Desempenho

NetFlow

- nProbe consegue capturar 100% do tráfego
- Um outro host captura e manipula os probes NetFlow
- Ferramentas nfsen/nfdump, flow-tools e scripts
- Amostragem obtida é de 1:1

Conclusão...

Conclusão

É possível utilizar um computador de propósito geral de custo reduzido para manipular grande quantidade de tráfego e auxiliar no monitoramento da rede.

Considerações Finais

Trabalhos Futuros

- Criar plugins para o PFRING para tratar tráfego diferenciado (contabilizar VoIP, por exemplo)
- Utilizar mais interfaces de rede para receber todo o tráfego
- Substituir o port-mirror por networks TAPs.

Referências

- PoP-PR: http://www.pop-pr.rnp.br
- PFRING: http://www.ntop.org/PF_RING.html
- Instalando PFRING: http://gentoo-wiki.com/Pfring

Criando um monitor de tráfego de baixo custo para redes de alta velocidade

RNP / PoP-PR

GTER 26 - São Paulo/SP - 07 de Novembro de 2008

Pedro R. Torres Jr. `torres@pop-pr.rnp.br`
PoP-PR - Ponto de Presença da RNP no Paraná