

PTTrix

Uso do sFlow para efetuar medições membro a membro no PTT

PRIX - PTT-Metro de Curitiba/PR

LACNIC XI - NAPLA 2008 - Salvador - BA - Brasil

27 de Maio de 2008

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro



[Introdução](#)

[Sobre o sFlow](#)

[Criando a Matriz de
Tráfego](#)

[Resultados](#)

[Conclusão](#)

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

Agenda

- 1 Introdução
- 2 Sobre o sFlow
- 3 Criando a Matriz de Tráfego
- 4 Resultados
- 5 Conclusão

PTTriX
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

Sobre o sFlow

Criando a Matriz de
Tráfego

Resultados

Conclusão

PRiX: PaRaná Internet eXchange

- Criado em 2002
- Operado pela equipe do PoP-PR/RNP
- Hospedado no datacenter do CCE da UFPR
- Absorvido pelo projeto PTT-Metro em 2005
- Conta atualmente com 15 Sistemas Autônomos participantes
- Tráfego agregado na ordem de 750Mbps

Introdução

[Sobre o sFlow](#)

[Criando a Matriz de Tráfego](#)

[Resultados](#)

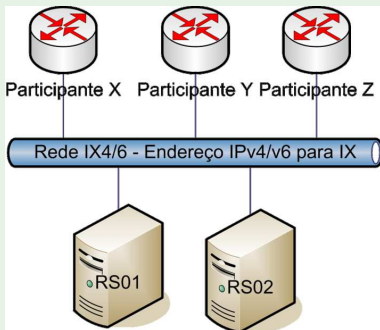
[Conclusão](#)

Ambiente de um PTT

Equipamentos

- Switch Ethernet: VLANS
- Route Servers: BGP Speakers
- Gerência: Looking Glass, Estatísticas, Monitores, etc.

Topologia Simplificada



PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

Sobre o sFlow

Criando a Matriz de
Tráfego

Resultados

Conclusão

Monitoramento Efetuado em um PTT

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



O que pode ser contabilizado:

- Uso dos links, medição com SNMP: MRTG, RRDTool, ...
- Mudanças das tabelas de roteamento BGP: Rotas, Mensagens, ...
- Status da porta de conexão, erros, loss, RTT ...

Difícil de contabilizar:

- Qual a quantidade de tráfego do participante X para o Y ?
- Qual a quantidade de tráfego na VLAN Z ?
- Qual a quantidade de tráfego ARP, IPv4, IPv6, Multicast, Broadcast ?

Introdução

Sobre o sFlow

Criando a Matriz de Tráfego

Resultados

Conclusão

O que é o sFlow?

- Tecnologia de Amostragem (Packet Sampling)
 - Permite uma visão geral da rede
 - É escalável
 - Baixo custo de implementação
 - Definido na RFC3176
- Implementado em Switchs e Roteadores
- Comparável ao Netflow
- Aplicável em interfaces de alta velocidade (> 1Gbps)
- Disponível em equipamentos de diversos fabricantes

Introdução

Sobre o sFlow

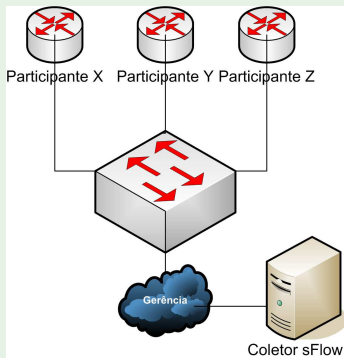
Criando a Matriz de Tráfego

Resultados

Conclusão

O que é necessário?

Coleta dos dados:



- Suporte no hardware do switch
- Coletor
- Ferramentas para analisar os dados coletados

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

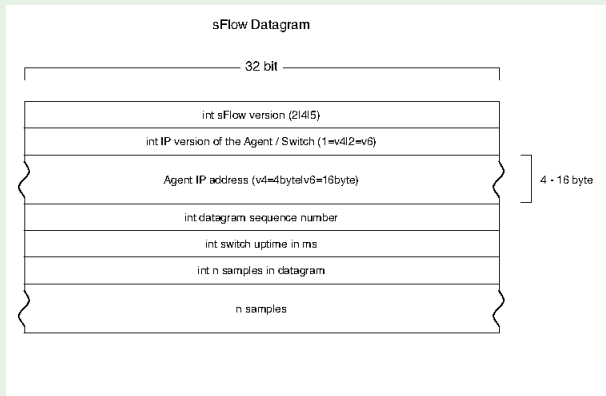
Sobre o sFlow

Criando a Matriz de
Tráfego

Resultados

Conclusão

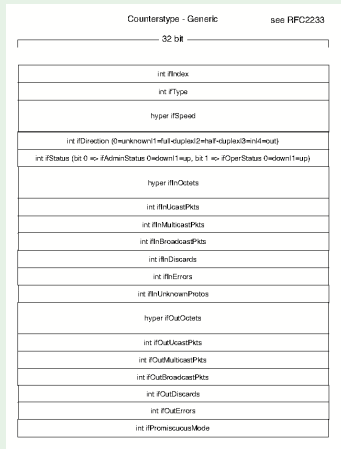
Datagrama sFlow



- Encapsulados via UDP
- Dois tipos de informações:
 - Counter Samples
 - Flow Samples

Counter Samples

Formato Counter Sample



- Intervalo de Polling
- Contadores de Interfaces (bytes, pacotes, erros)

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

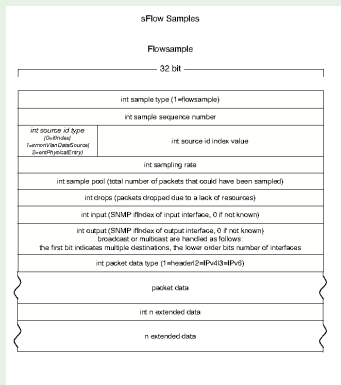
Sobre o sFlow

Criando a Matriz de Tráfego

Resultados

Conclusão

Formato Flow Sample



- Taxa de amostragem: 1 a cada N
- Até 256B L2 até L7 capturados
- Dados estendidos: Switch, Router, Gateway...

Decodificando um probe sFlow

Informações Disponíveis:

```
startSample -----  
sampleType FLOWSAMPLE  
sampleSequenceNo 56845174  
meanSkipCount 512  
inputPort 148  
outputPort 143  
flowSampleType HEADER  
headerProtocol 1  
sampledPacketSize 1518  
strippedBytes 4  
headerLen 128  
headerBytes 50-4F-29-23-23-72-98  
dstMAC 0a0c9620b260  
srcMAC 0af21e5dd11b  
IPSize 1500  
ip.tot_len 1500  
srcIP aaa.xxx.yyy.zzz  
dstIP bbb.xxx.yyy.zzz  
IPProtocol 6  
IPTOS 0  
IPTTL 121  
TCPsrcPort 1276  
TCPdstPort 4669  
TCPFlags 24  
extendedType SWITCH  
in_vlan 10  
in_priority 0  
out_vlan 10  
out_priority 0  
endSample -----
```

PTTriX
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

Sobre o sFlow

Criando a Matriz de
Tráfego

Resultados

Conclusão

Software livre

- InMon - sflowtools
- Pmacct - Promiscuous mode IP Accounting package
- sFlow2MySql
- Módulo Perl: Net::sFlow

Introdução

Sobre o sFlow

Criando a Matriz de Tráfego

Resultados

Conclusão

Manipulando probes sFlow

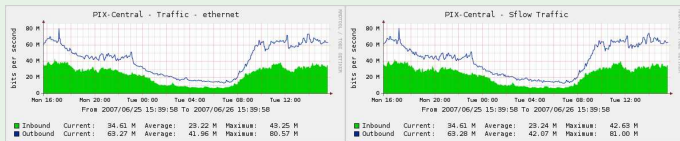
PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Imitando o SNMP:



- Feito utilizando sFlow com amostragem 1:512

- Re-escalado:

$$bps = \frac{\sum_i \text{Tamanho Amostra } i \times \text{Amostragem}}{\text{intervalo}}$$

- Não é perfeito mas é aceitável para as necessidades de administração de um PTT
- Nada muito elegante: sflowtools | awk

Introdução

Sobre o sFlow

Criando a Matriz de Tráfego

Resultados

Conclusão

Fazendo medições membro a membro

Matriz de tráfego:

A matriz de tráfego é uma representação das medições feitas entre cada par de membros

No PTT:

- Infra-estrutura camada 2.
- Mais de uma VLAN (IX4, IX6, Mcast, Trânsito, etc...)
- Um ASN = Um MAC (em geral)
- Necessidade de medir MAC a MAC

- Mapeamento de ASN para MAC

Formato do arquivo desejado:

```
SRC-AS : DST-AS : BITS : PACOTES
```

```
A : B : bps : pps :
```

```
A : C : bps : pps :
```

```
A : D : bps : pps :
```

```
B : A : bps : pps :
```

```
B : C : bps : pps :
```

```
B : D : bps : pps :
```

```
...
```

Criando o PTTrix

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

Informações necessárias

- ASN participantes
- Controle do MAC de cada participantes
- VLAN que cada ASN utiliza

Cuidado com os dados

- Apenas o valor estatístico é armazenado
- Amostras recebidas não são armazenadas
- Apenas dados camada 2 são necessários
- Demais dados não precisam ser decodificados

ptt.br
Curitiba



UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

Introdução

Sobre o sFlow

Criando a Matriz de
Tráfego

Resultados

Conclusão

Primeira versão

- Arquivo da matriz gerado com: `sflowtools | awk`
VLAN IX4:
SRC-MAC:DST-MAC:BITS:PACOTES
A:B:bps:pps:
A:C:bps:pps:
A:D:bps:pps:
B:A:bps:pps:
B:C:bps:pps:
B:D:bps:pps:
...
- Contabiliza tráfego na VLAN IX4 MAC a MAC
- Integrado com o RRDTool via parser PHP
- Interface Web para visualizar os gráficos

[Introdução](#)

[Sobre o sFlow](#)

[Criando a Matriz de Tráfego](#)

[Resultados](#)

[Conclusão](#)

Segunda geração

- Arquivo da matriz gerado com daemon personalizado

```
SRC-MAC:SRC-VLAN:DST-MAC:DST-VLAN:BITS:PACOTES
```

```
A:X:B:Y:bps:pps:
```

```
A:X:C:Y:bps:pps:
```

```
A:X:D:Y:bps:pps:
```

```
B:X:A:Y:bps:pps:
```

```
B:X:C:Y:bps:pps:
```

```
B:X:D:Y:bps:pps:
```

```
...
```

- Daemon implementado com Net::sFlow
- Contabiliza tráfego MAC a MAC em TODAS vlans
- Está versão é a que está em uso atualmente

[Introdução](#)

[Sobre o sFlow](#)

[Criando a Matriz de Tráfego](#)

[Resultados](#)

[Conclusão](#)

Interface de Gerência - Primeira Versão

Matriz de Tráfego do PRIX

PTTrix
Uso do sFLOW para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



PTTrix
Matriz dos ASs

	BCAST	LG	RS1	RS2	1916	6140	8167	10412	10881	11751	11835	13522	14868	18881	19723	22148	28573	
BCAST	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	BCAST
LG	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	LG
RS1	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	RS1
RS2	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	RS2
1916	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	1916
6140	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	6140
8167	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	8167
10412	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	10412
10881	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	10881
11751	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	11751
11835	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	11835
13522	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	13522
14868	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	14868
18881	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	18881
19723	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	19723
22148	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	22148
28573	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	Bits Pacotes	28573

- Bits e Pacotes para cada MAC conhecido
- Representação não escalar

Introdução

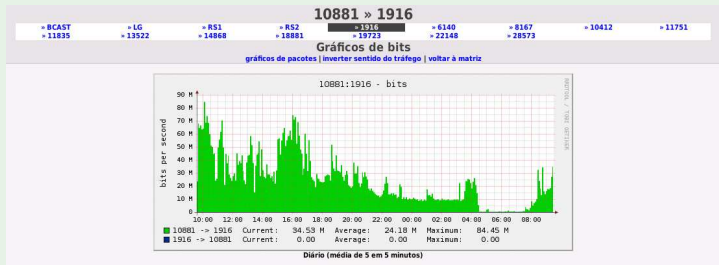
Sobre o sFLOW

Criando a Matriz de Tráfego

Resultados

Conclusão

Navegação Simplificada

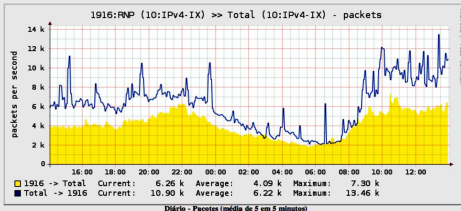
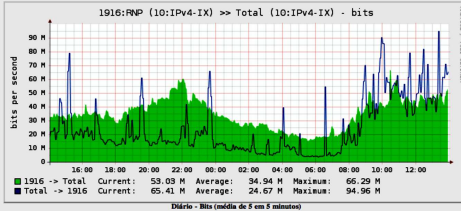


- Navegação para todos os ASN disponíveis
- Representação do tráfego: ASN1 -> ASN2

Interface de Gerência - Segunda Versão

Nova Navegação

VLAN de Entrada:	VLAN de Saída:	AS de Origem:	AS de Destino:
10:IPv4-IX	10:IPv4-IX	1916-RNP	Total
10:IPv4-IX			
20:IPv6-IX	Trocar Senha	Logout	



- Representação escalar

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

Sobre o sFLOW

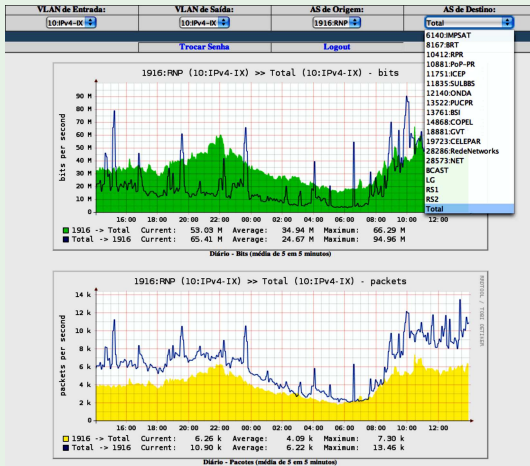
Criando a Matriz de Tráfego

Resultados

Conclusão

Interface de Gerência - Segunda Versão

Nova Navegação



- Interface do Usuário e Interface de Administração
- Visualiza apenas política de cada participante

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Introdução

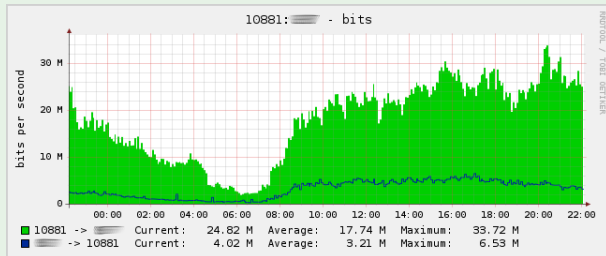
Sobre o sFlow

Criando a Matriz de Tráfego

Resultados

Conclusão

Exemplo de medição membro a membro



- Tráfego entre o AS10881 e o ASXXXXX
- Característica normal

Introdução

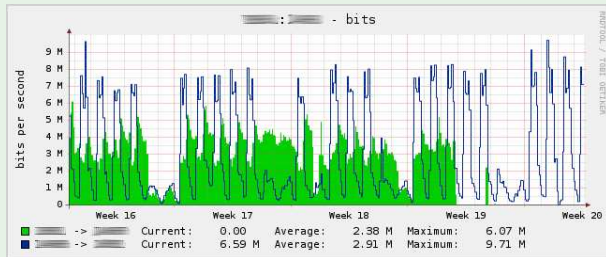
Sobre o sFLOW

Criando a Matriz de Tráfego

Resultados

Conclusão

Tráfego Assimétrico



- Participante não está trocando tráfego nos dois sentidos
- Característica normal

Introdução

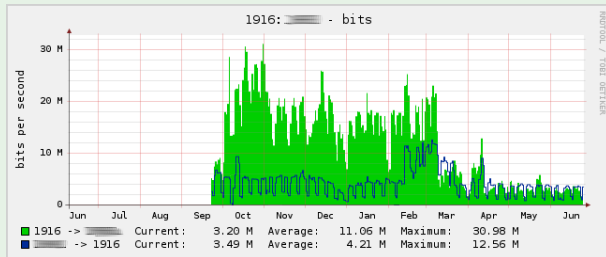
Sobre o sFLOW

Criando a Matriz de Tráfego

Resultados

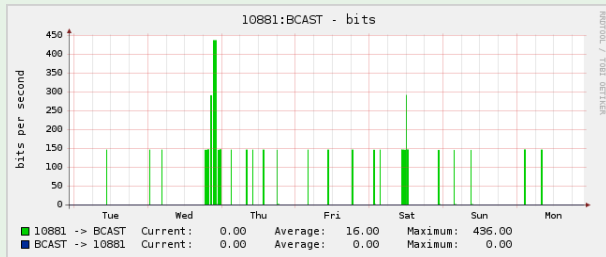
Conclusão

Diminuição do Tráfego Trocado



- Participante diminuiu a quantidade de tráfego trocado
- Entrada em outro PTT

Tráfego para Broadcast



- Amostragem não permite precisão
- Característica normal

[Introdução](#)

[Sobre o sFlow](#)

[Criando a Matriz de Tráfego](#)

[Resultados](#)

[Conclusão](#)

Conclusão...

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Conclusão

A Medição membro a membro ajuda a entender as políticas de roteamento adotadas pelos participantes. Problemas são facilmente percebidos. As medições podem ser feitas para contabilizar diversos tipos de tráfego: ARP, IPv4, IPv6, Multicast, Não IP, HTTP, etc. O seu uso não se limita em PTTs.

[Introdução](#)

[Sobre o sFlow](#)

[Criando a Matriz de Tráfego](#)

[Resultados](#)

[Conclusão](#)

Considerações Finais

PTTrix
Uso do sFlow para
efetuar medições
membro a membro
no PTT

Christian / Pedro

ptt.br
Curitiba



Uso atual

Em uso no PTT-Metro de Curitiba (PRIX) a 2 anos.

Trabalhos Futuros

- Contabilizar diversos tipos de tráfego
- Expandir para outros PTT

Introdução

Sobre o sFlow

Criando a Matriz de Tráfego

Resultados

Conclusão

- PoP-PR: <http://www.pop-pr.rnp.br>
- PRiX: <http://pr.ptt.br>
- sflowtools:
<http://www.inmon.com/technology/sflowTools.php>
- Net::sFlow: <http://search.cpan.org/elisa/Net-sFlow-0.06/>
- AMS-IX: <http://www.ams-ix.net>

PTTrix

Uso do sFlow para efetuar medições membro a membro no PTT

PRIX - PTT-Metro de Curitiba/PR

LACNIC XI - NAPLA 2008 - Salvador - BA - Brasil
27 de Maio de 2008

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

Introdução

Sobre o sFlow

Criando a Matriz de
Tráfego

Resultados

Conclusão