

Uma proposta de infra-estrutura para medição passiva de tráfego na rede RNP2

Eduardo Leivas Bastos
elbastos@ieee.org

Luís Felipe Balbinot
hades@inf.ufrgs.br

III Workshop RNP2
Florianópolis, 2001

“In today’s Internet, with the phenomenal growth that is being experienced, the ‘practice’ of networking has outrun the ‘theories’ on the basis of which advanced networks are designed, built and operated.

Network traffic monitoring and measurement *is the critical technology needed now to allow us to see and understand what is really actually happening within and among networks.*

This, in turn, will help both network researchers and operators identify and mitigate nascent problems before they become infrastructure failures. It may even, in the longer run, allow us to develop reasonable predictive models to anticipate problems before they arise.”

Aubrey Bush

NSF Division

Director for Advanced Networking
Infrastructure and Research (ANIR)

Histórico

- Grupo de Gerenciamento Distribuído é formado no PRAV/UNISINOS no contexto RMAVs/RNP2.
- Necessidade de uma ferramenta para a coleta e análise de tráfego ATM nativo nos switches IBM da rede METROPOA (RMAV/RS).
- Requisitos:
 - gerenciamento passivo, baixo custo, independência de fornecedor, código aberto, flexível, escalável, robusta.
- Escolha do pacote CoralReef (CAIDA) e compra dos equipamentos (placas ATM, splitters óticos, estação de coleta).
- Montagem e implantação da ferramenta no link OC3c entre a UNISINOS e a CRT.

CoralReef

<http://www.caida.org/tools/measurement/coralreef/>

- Coleta e análise de tráfego (em arquivos ou real-time) gerados por monitores passivos de tráfego
- Evolução do OC3mon/Coral
- Pacotes
 - captura, análise e ferramentas para a geração de relatórios
 - bibliotecas (C e Perl)
- Hardware/SO
 - Fore ATM (OC3) / FreeBSD
 - AppTel (OC3 e OC12) / FreeBSD
 - WAND DAG (OC3, OC12, OC48) / Linux
- Libpcap

Arquitetura

HTML Report Generation	
Analysis Programs in C/C++	Analysis Programs in Perl
	Perl API (CRL.pm)
C API (libcoral)	
Drivers	Other input (traces)

Hardware utilizado



Placas ATM Fore PCA-200EPC

Estação de coleta
e análise

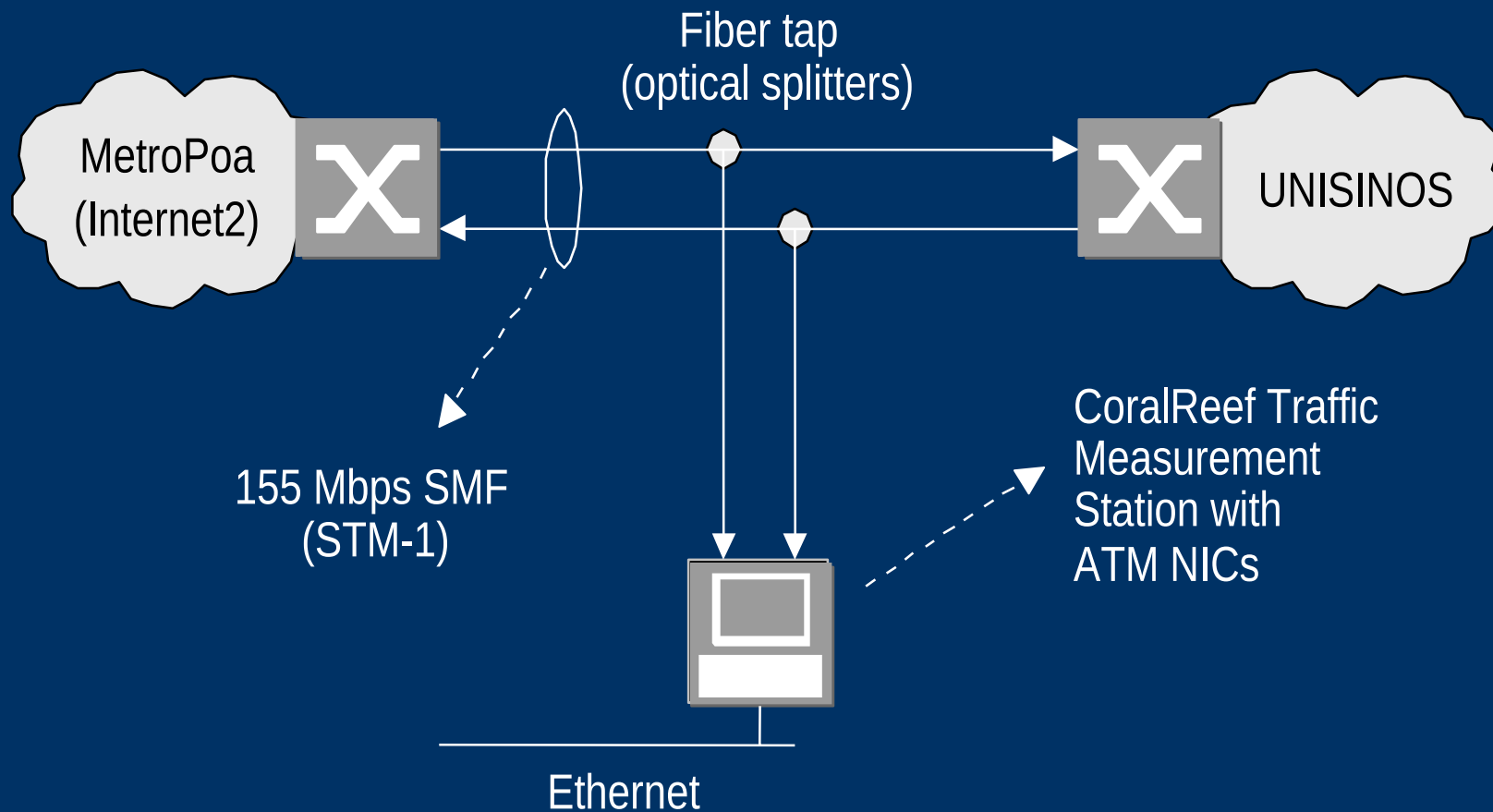
PPro 200 MHz
128 MB ECC
20 GB RAID-5



Splitters óticos
ADC

Ratio: 90/10

Metodologia de Medição



Exemplos de Relatórios

crl_print : Prints ATM cells in hex and ascii.

```
cell 0, interface 0
time: 0.000001625
gfc: 0 (0x0000)
vp:vc: 1:4350 (0x01:0x10fe)
pti: 0 0 0 (user data, no congestion, not last cell)
payload:
aa aa 03 00 00 00 08 00 45 00 04 30 16 10 40 00 |.....E..0..@.|
3d 06 65 c1 00 01 00 01 00 02 00 01 12 5b 00 19 |=.e.....[..|
c0 17 b7 0c 93 2f cb bb 70 18 44 10 62 08 00 00 |...../..p.D.b...|
```

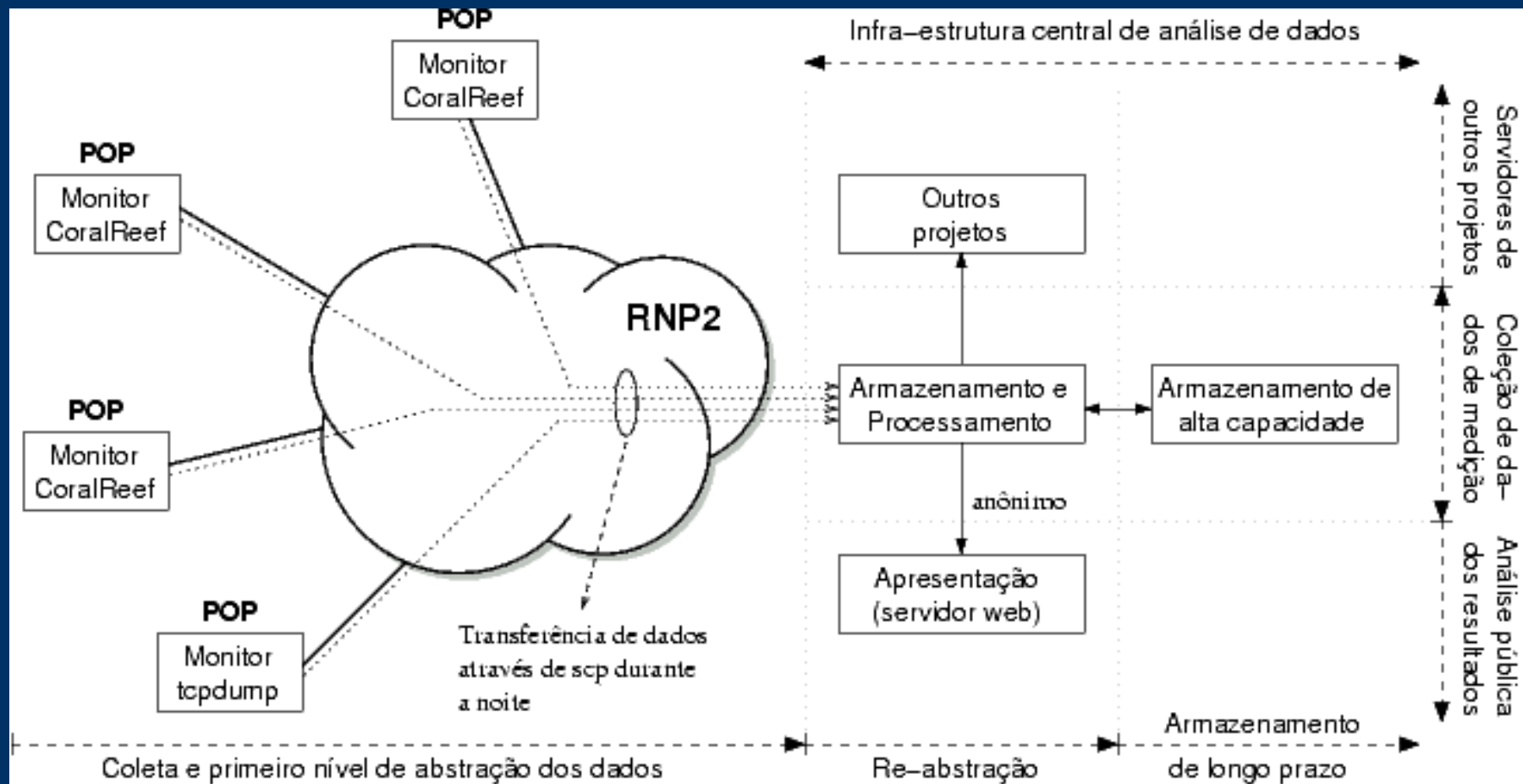
crl_time : Outputs to stdout one line per cell in trace

If	cell	high	low	seconds	difference	comment
0	0:	0000018a	0000397f	1.033436120	0.000010560	
0	1:	0000018a	00003b2f	1.033453400	0.000017280	
0	2:	0000018a	0000409d	1.033509000	0.000055600	
0	3:	00000001	00000187	0.002637080	-1.030871920	XXX major
error: negative diff						
0	4:	00000001	000002e5	0.002651080	0.000014000	
0	5:	00000001	000003f1	0.002661800	0.000010720	
0	6:	00000001	000004ef	0.002671960	0.000010160	
0	7:	00000001	000005ec	0.002682080	0.000010120	
0	8:	00000001	000008e6	0.002712560	0.000030480	

Proposta

- Implantação de uma infra-estrutura de medição passiva de tráfego no backbone RNP2 através da instalação de diversos *probes* CoralReef em pontos específicos da rede.
- Benefícios
 - Informações mais precisas para a Engenharia de Tráfego (dimensionamento de enlaces, equipamentos, *traffic shaping*, *traffic policing*, etc)
 - Fonte de traces reais de tráfego para simulações
 - Primeiro passo em direção a criação de uma infra-estrutura de medição ativa
 - Valor agregado ao backbone da RNP2 – “backbone monitorado”
 - Dados topológicos + dados de desempenho tornados públicos – novo patamar para a medição da qualidade de backbones

Arquitetura



Desafios Técnicos

- Periodicidade e sincronismo da coleta
- Tecnologias de armazenamento
- Ferramentas de visualização
- Segurança e Privacidade
- Correlação de eventos, fluxos, etc...
- Escalabilidade
- Garantia de funcionamento (POST, *spare kits*, etc)
- Gerenciamento de configuração dos probes (script MIB, objetos distribuídos, etc...)

Outras ferramentas

- Netflow
- NetraMet
- cflowd
- RMON2
- tcpdump, snoop,...
- rrdtool
- flowstat

Sugestões...

- Criação de Infra-estrutura de Análise de Tráfego Internet Nacional (IATIN) para o backbone RNP2, com os seguintes objetivos:
 - Monitoramento Passivo (proposta apresentada)
 - Monitoramento Ativo
 - Gerenciamento SNMP
 - Gerenciamento de roteamento (especialmente BGP)
- Criação de um fórum para discussões de assuntos relacionados à ET (congressos, seminários, listas de discussão, etc). GTER poderia ser esse fórum?
- Estender a IATIN para os outros provedores/operadores de backbone no Brasil de forma a obter-se análises *inter-clouds*.

Obrigado!!

elbastos@ieee.org

hades@inf.ufrgs.br

Agradecimentos:

MCT/RNP2, PRAV/UNISINOS, UFRGS, PROCEMPA,
PROCERGS, PUC, CRT

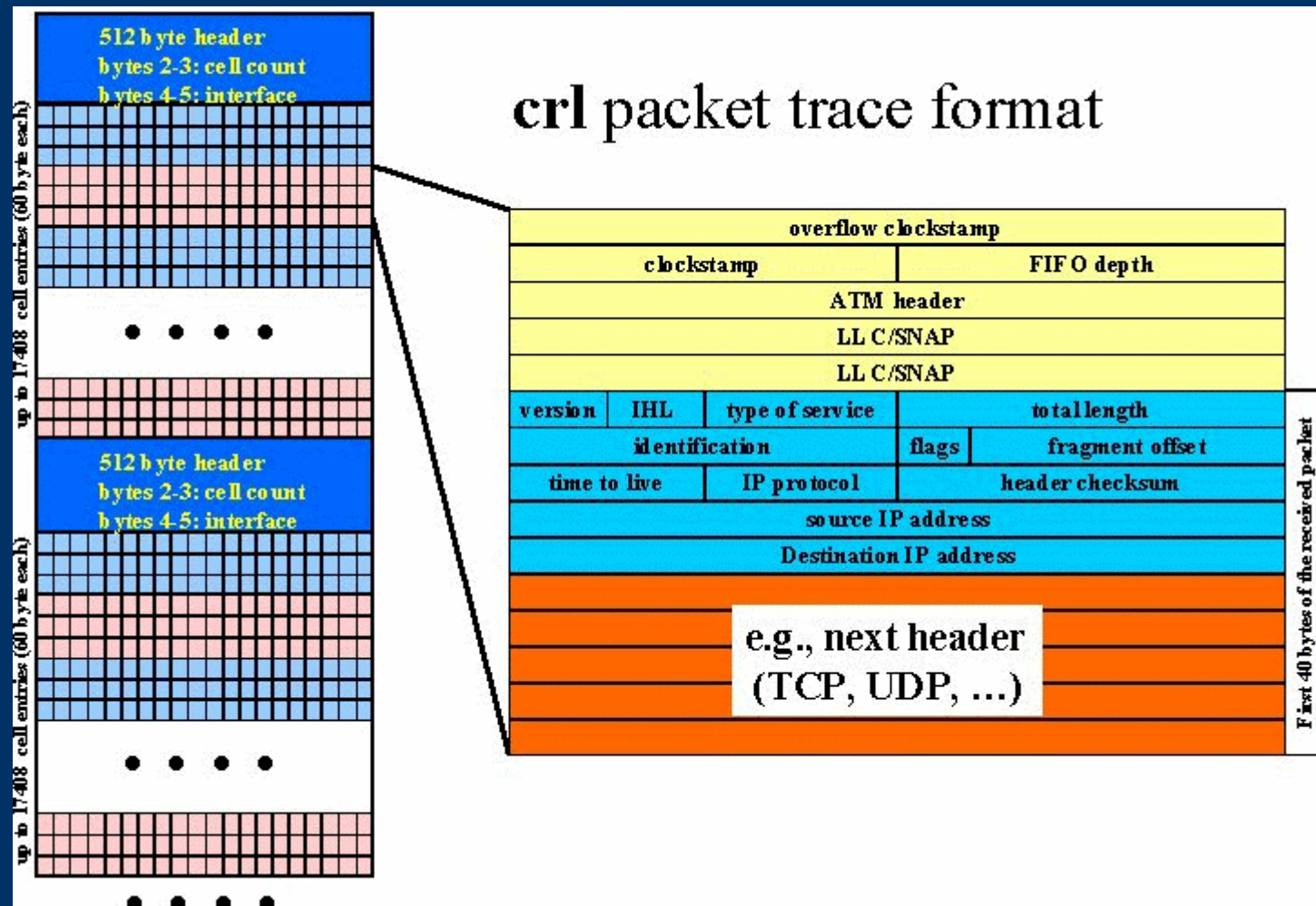
Uma proposta de infra-estrutura para medição passiva de tráfego na rede RNP2

Eduardo Leivas Bastos
elbastos@ieee.org

Luís Felipe Balbinot
hades@inf.ufrgs.br

III Workshop RNP2
Florianópolis, 2001

Formato *trace* CoralReef



Placas DAG



DAG4

The DAG Project

<http://dag.cs.waikato.ac.nz/>



DAG3

NAI system

