

III Workshop do POP-RS

Serviços disponibilizados pelo PoP-RS

César Loureiro

setembro/2010



III Workshop do POP-RS

Agenda

Serviços Internos:

- Backup de roteadores
- Registro e análise de logs
- Diagnóstico de Sites
- IPv6

Serviços Externos:

- DNS Secundário
- Multicast
- PlanetLab
- Medição de Banda
- Flows
- Estatísticas
- NTP
- Mirror
- BGP Multihomed
- Collocation

Capacidade de Atendimento

Disponibilidade

Serviços Internos

- **Backup de Roteadores**

A cada alteração realizadas nos equipamentos de clientes, possuímos uma rotina que realizar o backup das configurações de todos os roteadores, garantindo assim um resposta ao tratamento de incidentes que possam ocorrer nos equipamentos.

Serviços Internos

- **Registro e análise logs**

Possuímos um servidor de Logs que armazena uma replica dos logs de forma segura de todos os servidores internos e de todos os roteadores dos clientes.

Sobre estes logs é realizada uma análise on-line utilizando a ferramenta OSSEC.

Serviços Internos

- Registro e análise logs - Exemplo

Top entries for 'Source ip':

218.15.221.82 |71 |

Top entries for 'Group':

authentication_failures |71 |
pure-ftpd |71 |

Top entries for 'Location':

virgo-> |71 |

Top entries for 'Rule':

11306 - FTP brute force (multiple failed log.. |71 |

Serviços externos

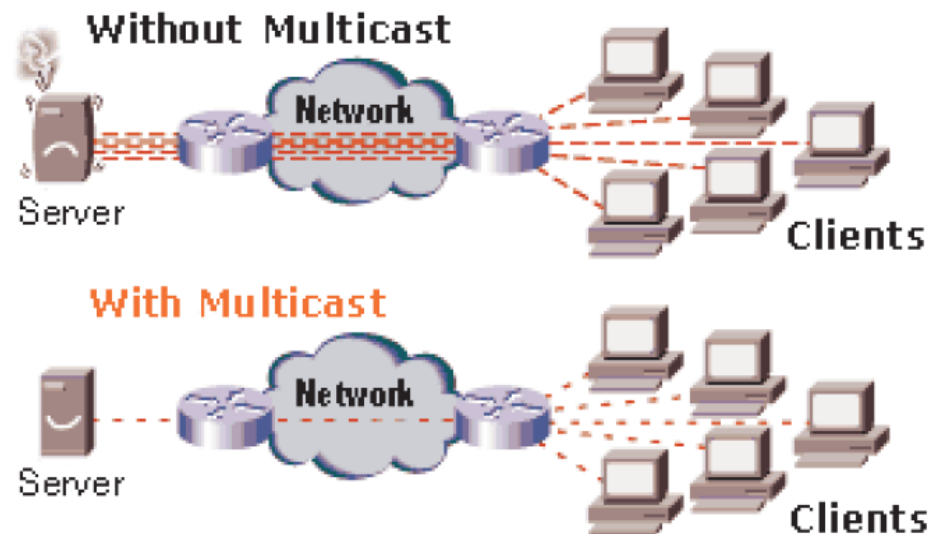
- **DNS Secundário**

Serviço de DNS secundário para os clientes da Rede Tchê.

Serviços externos

- **Multicast**

O PoP-RS transmite multicast para a Rede IPE, permitindo que seus clientes que possuam roteadores com esta funcionalidade utilizem este recurso para transmissões como por exemplo de vídeos sob demanda.



Serviços externos

- **PlanetLab**

O PlanetLab é um consórcio formado por instituições acadêmicas, governamentais e industriais que visa a criação de uma grande malha de computadores espalhados pelo mundo em diversas redes. Onde o PoP-RS possui 2 nós desta rede.

Para submissão de projetos acesse:

<http://www.rnp.br/pd/planetlab/>

Serviços externos

- **Medição de banda**
- **Web100 - Network Diagnostic Tool (NDT)**

Solução para medição de banda de entrada e saída da rede.

Serviços externos

- **Medição de banda**

TCP/Web100 Network Diagnostic Tool v3.5.6

click START to begin

** Starting test 1 of 1 **

Connecting to 'ndt.pop-rs.mp.br' [ndt.pop-rs.mp.br/200.132.0.83] to run test

Connected to: ndt.pop-rs.mp.br -- Using IPv4 address

Checking for Middleboxes Done

checking for firewalls Done

running 10s outbound test (client-to-server [C2S]) 246.0kb/s

running 10s inbound test (server-to-client [S2C]) 831.84kb/s

Your PC is connected to a Cable/DSL modem

click START to re-test

START

Statistics

More Details...

Report Problem

Options



Serviços Externos

- **Flows**

Análise de fluxo obtendo estatísticas por:

- IP/Rede de Origem/Destino
- Porta de Origem/Destino

- Acessado pelo endereço:

<http://rrd.pop-rs.rnp.br>

Usuario: tche

Senha:

Serviços Externos Flows

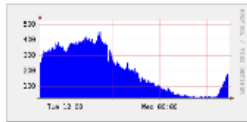
[graphs](#)
[SmokePing](#)
[FLOWS](#)
[weathermap](#)

FLOWS

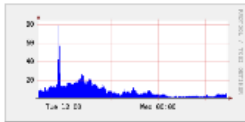
[Home](#)
[Graphs](#)
[Details](#)
[Alerts](#)
[Stats](#)
[Plugins](#)
 continuous / shadow
 [Bookmark URL](#)
 Profile: [ufrgs](#)

Profile: ufrgs

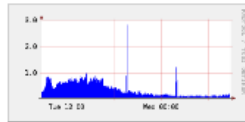
TCP



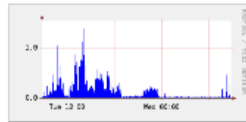
UDP



ICMP

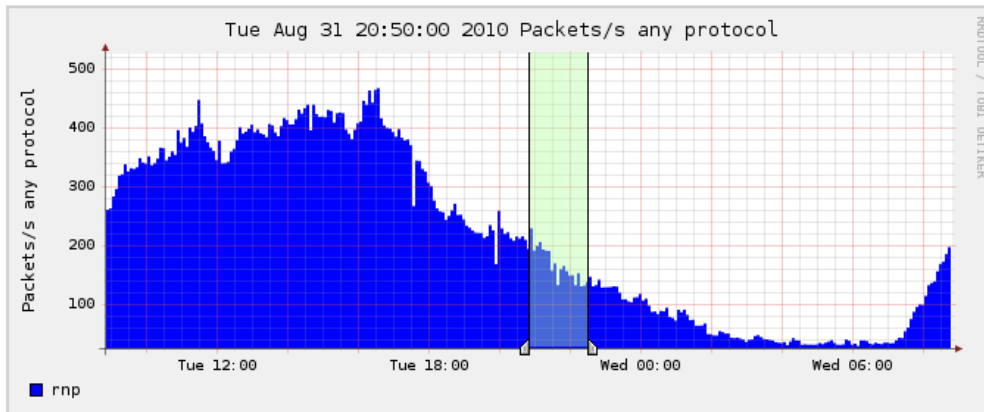


other



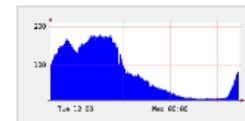
Profileinfo:

Type: continuous / shadow
Max: unlimited
Exp: never
Start: Jul 07 2008 - 17:25 BRT
End: Sep 01 2010 - 08:50 BRT



tstart 2010-08-31-20:50
tend 2010-08-31-22:30

Flows



Traffic



Select [Time Window](#) Display: [1 day](#)

Lin Scale
 Stacked Graph
 Log Scale
 Line Graph

Statistics timeslot Aug 31 2010 - 20:50 - Aug 31 2010 - 22:30

Channel:	Flows:					Packets:					Traffic:			
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:
<input checked="" type="checkbox"/> rmp	53.0 /s	49.5 /s	3.2 /s	0.2 /s	0.0 /s	173.3 /s	166.0 /s	6.9 /s	0.2 /s	0.1 /s	1.2 Mb/s	1.2 Mb/s	14.8 kb/s	138.7 b/s

All None Display: Sum Rate



Serviços Externos Flows

Netflow Processing

Source: **Filter:**

and

Options:

List Flows Stat TopN

Top:

Stat: **order by**

Aggregate

proto srcPort

dstPort

Packets

Limit:

Output: / IPv6 long

```
** nfdump -M /usr/local/var/nfsen/profiles/live/rnp -T -R nfcapd.201008312050:nfcapd.201008312230 -n 10 -s record/bytes -A proto,srcip
nfdump filter:
(( ident rnp) and (
(src net 143.54.0.0/16) or (dst net 143.54.0.0/16)
))
```

Aggregated flows 252630

Top 10 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2010-08-31 20:46:16.008	6301.432	TCP	141.76.2.4:873	->	143.54.196.9:36515	6499	9.3 M	108
2010-08-31 20:46:18.109	5338.503	TCP	174.140.157.13:80	->	143.54.29.120:53065	5709	8.2 M	118
2010-08-31 20:46:17.109	4314.570	TCP	95.211.104.24:80	->	143.54.247.67:1560	5488	7.9 M	111
2010-08-31 21:01:53.561	1525.307	TCP	209.222.128.172:80	->	143.54.121.59:44239	5082	7.3 M	44
2010-08-31 21:00:49.659	2300.695	TCP	69.5.92.49:80	->	143.54.196.97:42722	5068	7.2 M	66
2010-08-31 21:41:14.392	1409.927	TCP	95.211.94.230:80	->	143.54.10.187:55940	5017	7.2 M	44
2010-08-31 21:17:29.458	1368.623	TCP	174.140.157.14:80	->	143.54.10.187:51013	4961	7.1 M	45
2010-08-31 21:36:26.995	1505.636	TCP	69.5.93.15:80	->	143.54.121.59:38240	4901	7.0 M	47
2010-08-31 20:46:16.003	1818.093	TCP	174.140.129.35:80	->	143.54.10.187:50292	4523	6.5 M	50
2010-08-31 20:46:16.256	1722.477	TCP	174.140.157.39:80	->	143.54.121.21:59867	4220	6.0 M	47

Summary: total flows: 320963, total bytes: 872.6 M, total packets: 1048123, avg bps: 1.1 M, avg pps: 164, avg bpp: 872

Time window: 2010-08-31 20:45:15 - 2010-08-31 22:31:17

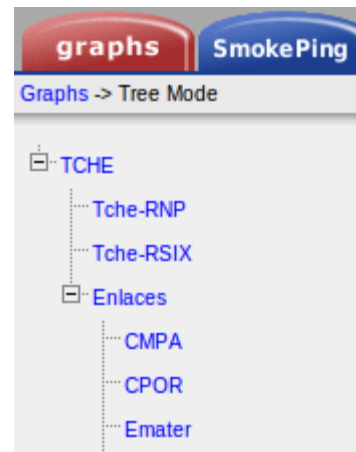
Total flows processed: 2923148, Records skipped: 0, Bytes read: 152006000

Serviços Externos

- **Estatísticas**

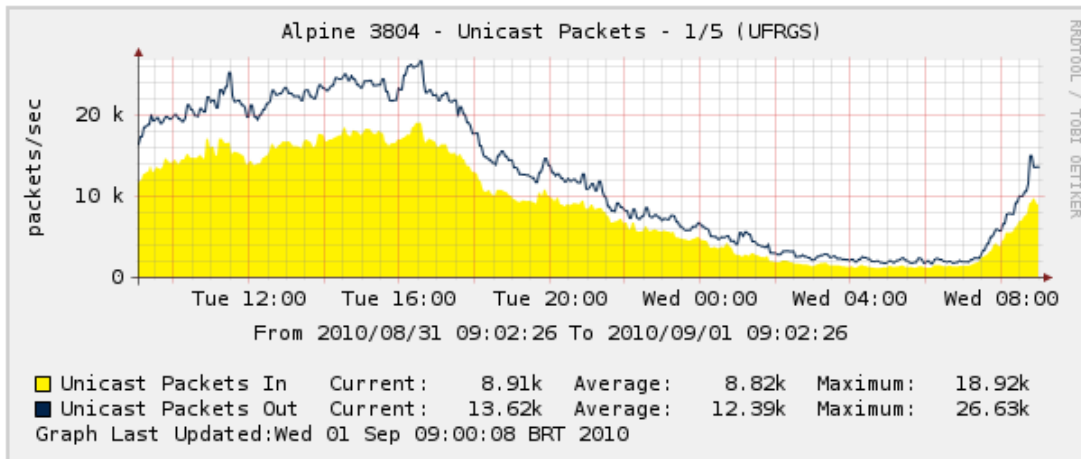
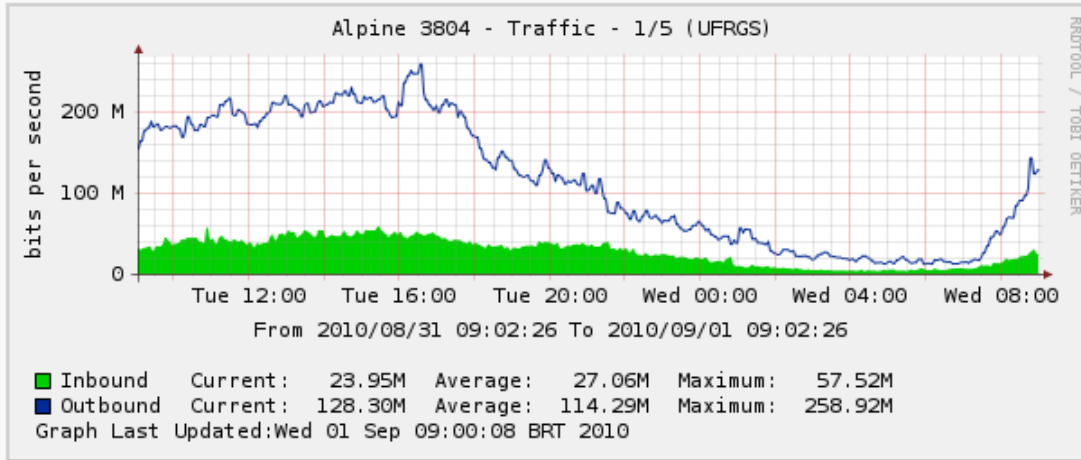
Estatísticas de uso do link.

Onde é possível ver o uso agregado da rede Tchê ou por cliente.



Serviços Externos Estatísticas

Showing All Graphs



Showing All Graphs

Serviços Externos

- **Diagnóstico de sites**

Consulta Integrada onde é possível consultar informações sobre determinado IP/domínio em uma única interface:

- Ping** - Envio de pacotes ICMP
- Traceroute** - Verificação de Rota
- Reverso** - Consulta DNS Reverso
- SPF** - Verifica se o host pode enviar e-mail (DNS)
- Whois** - Consulta na base whois
- Blacklist** - Verifica o IP/Domínio nas seguintes Blacklists:
 - zen.spamhaus.org
 - b.barracudacentral.org
 - t1.dnsbl.net.au
 - bl.spamcop.net
 - cbl.abuseat.org

Serviços Externos

- Diagnóstico de sites

PING

PING 200.132.0.132 (200.132.0.132) 56(84) bytes of data.
64 bytes from 200.132.0.132: icmp_seq=1 ttl=64 time=0.303 ms
64 bytes from 200.132.0.132: icmp_seq=2 ttl=64 time=0.310 ms
64 bytes from 200.132.0.132: icmp_seq=3 ttl=64 time=0.332 ms
64 bytes from 200.132.0.132: icmp_seq=4 ttl=64 time=0.303 ms

--- 200.132.0.132 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.303/0.312/0.332/0.011 ms



TRACEROUTE

traceroute to 200.132.0.132 (200.132.0.132), 20 hops max, 40 byte packets
1 delta.pop-rs.rnp.br (200.132.0.132) 0.491 ms 0.462 ms



REVERSO

132.0.132.200.in-addr.arpa domain name pointer delta.pop-rs.rnp.br.



SPF

132.0.132.200.in-addr.arpa domain name pointer delta.pop-rs.rnp.br.



BLACKLIST

Checando 200.132.0.132...

zen.spamhaus.org [Não Listado]
b.barracudacentral.org [Não Listado]
t1.dnsbl.net.au [Não Listado]
bl.spamcop.net [Não Listado]
cbl.abuseat.org [Não Listado]

Serviços Externos

- **IPv6**
- Disponibilidade de endereço IPv6 na interfaces do roteador do cliente.
- Disponibilidade de faixas de IP's para redes dos clientes.

Previsão para término de endereços IPv4 disponibilizados pelo IANA (outubro/ 2011)

Serviços Externos

- **NTP**(Network Time Protocol)

Disponibilização de um servidor de tempo para uso dos clientes da rede Tchê.

ntp.pop-rs.rnp.br

Serviços Externos

- **QoS (Qualit of Services)**

Possibilidade de marcação de pacotes para tratamento interno de QoS pelo cliente.

Serviços Externos

- **Mirror**

Disponibilização dos sistemas:

- **FreeBSD** (ftp://ftp4.br.freebsd.org)
- **CTAN**(Comprehensive teX Archive Network)

<http://mirror.pop-rs.rnp.br>

Serviços Externos

- **BPG Multihomed**
- Conexão a outros Backbones com BGP
 - Utilizando o AS2716 (Rede Tchê)
 - Não necessita solicitar Sistema Autônomo próprio.
 - Deve possuir um /24 da RNP e conexão com outra operadora

Serviços Externos

- **Collocation**

Disponibilizada a rede 200.132.1.0/24 para os clientes proverem serviços nas dependências do PoP-RS.

- Maior velocidade de banda.
- Para o uso do espaço físico do Datacenter é necessário realizar um convênio com a UFRGS.

Capacidade de Atendimento

Atualmente o PoP-RS possui a seguinte capacidade de atendimento :

E1 – 2 Mbps → +100

E3 – 34 Mbps → 8

Ethernet – 10/100/1000 Mbps → +100

Disponibilidade

- **Disponibilidade do PoP-RS**

Média dos últimos 12 meses: **99,93%**

- **Disponibilidade dos Clientes**

Enviado Relatório Mensal gerado através da ferramenta de Gerência.

Dúvidas/Questionamentos?

César Loureiro

cesar@pop-rs.rnp.br

Obrigado!