Pacheco Tecnologia

Grupo de Trabalho de Engenharia e Operação de Redes
(GTER39)

Conexão com PTT's utilizando Vyatta/Vyos/EdgeMAX

Elizandro Pacheco <elizandro@pachecotecnologia.net>

Pacheco Tecnologia

Elizandro Pacheco

- **Consultor desde 2003**
- **Usuário Linux desde 1998**

AUTHORIZED
TRAINING PARTNER

Motivação

- Aumento na quantidade de ativações utilizando hardwares e SO's alternativos.
- Novos roteadores baseados em Linux homologados
- Falta de documentação em pt-br
- Dificuldades de ativação com configurações default
- Desvendar mitos criados em redes sociais e fóruns

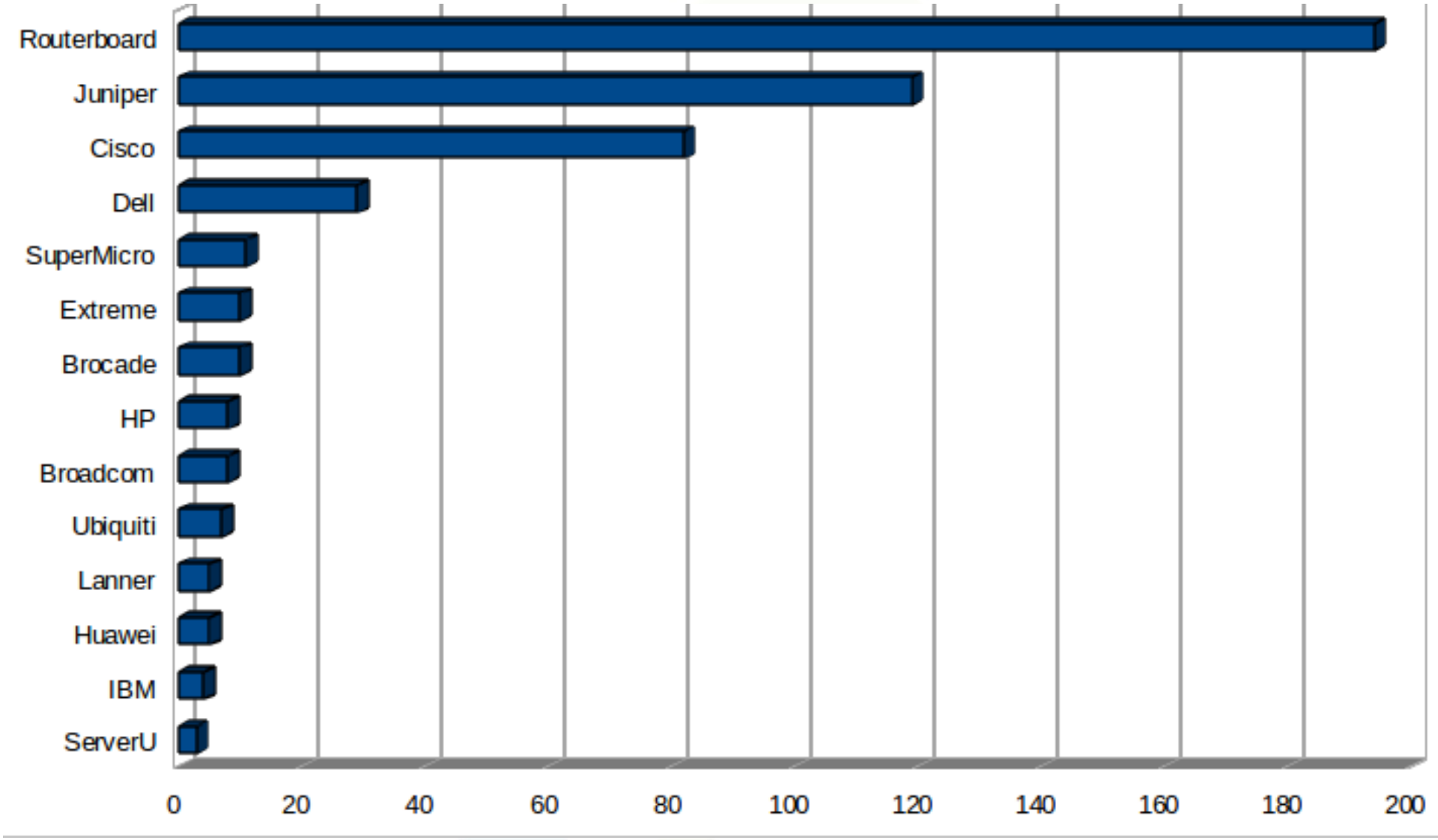
Resumo

- Demonstração de configuração básica para conexões com PTT's utilizando soluções baseadas em linux (EdgeRouter) apresentando as principais dificuldades encontradas durante o processo de ativação e testes de quarentena.

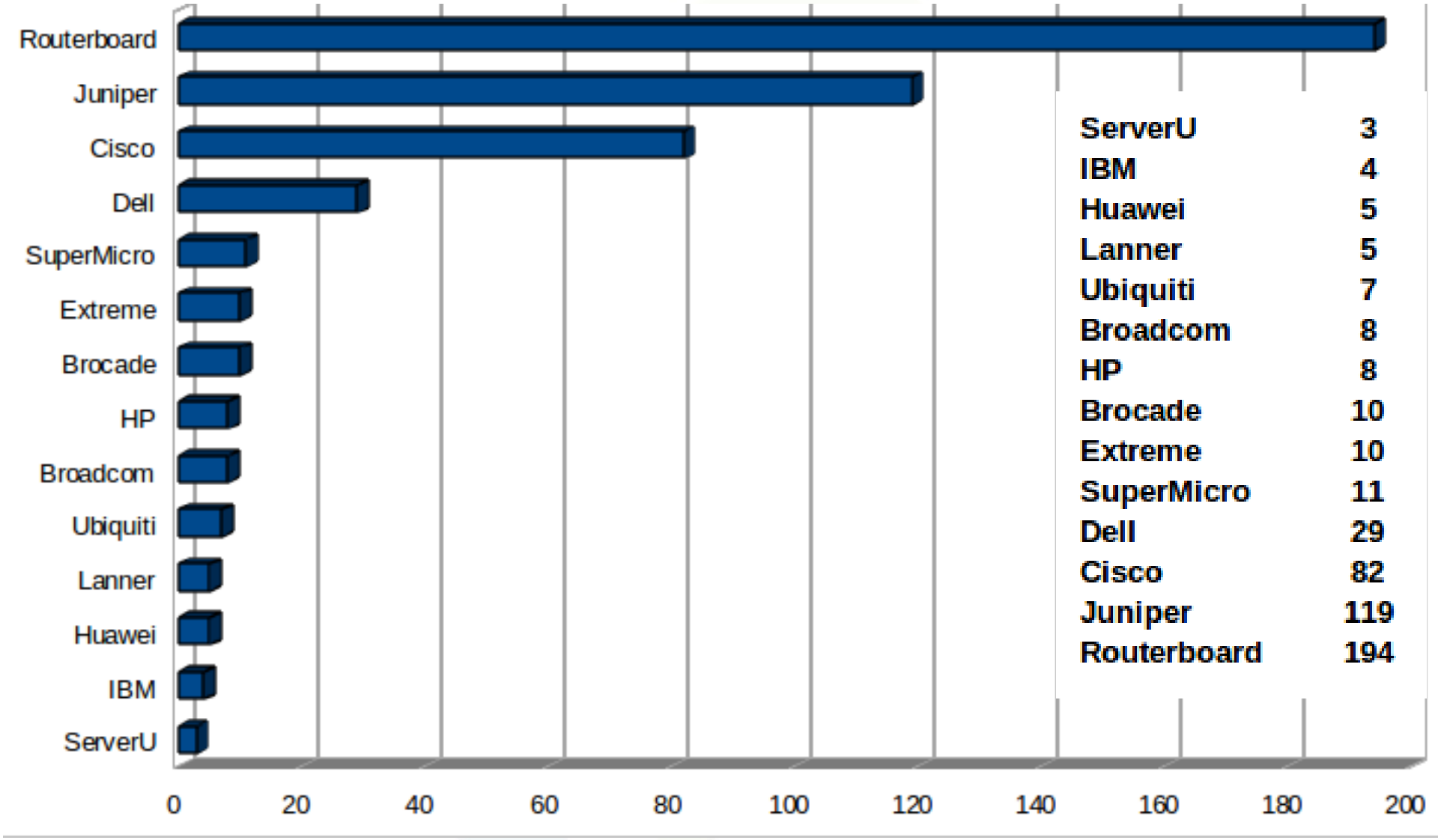
  Foco nos requisitos e ajustes necessários nas plataformas para ativações com agilidade e sem maiores complicações.

  Apesar de conter uma configuração base completa,
  o foco da apresentação não é o protocolo em si.

Dados não oficiais – PTT-SP – Maio de 2015



Dados não oficiais – PTT-SP – Maio de 2015



Fonte de Dados

- *Tabela Arp + Script*

```php
<?php

$macs = file('./arptable');

foreach ($macs as $line_num => $line) {
    $result = explode(" ", $line);
    $url = "http://api.macvendors.com/" . urlencode($result[3]);
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    $response = curl_exec($ch);
    if($response) {
        echo $result[0] .';'.$result[1].';'.$result[3].';'.$response . PHP_EOL;
    } else {
        echo $result[0] .';'.$result[1].';'.$result[3].';Not Found' . PHP_EOL;
    }
}

?>
```

http://pastebin.com/SxBGvkuP

Configuração Básica

Dados Ativação

ASN: 65530

Bloco v4: 10.1.0.0/22
Bloco v6: 2001:db8:8000::/33

Vlan v4: 1004
Vlan v6: 1006

Lan: 192.168.0.30/21 — 2001:db8::30/64

- rs1 (192.168.0.201 — 2001:db8::201 — ASN: 65531)
- rs2 (192.168.0.202 — 2001:db8::202 — ASN: 65531)
- lg: (192.168.0.210 — 2001:db8::210 — ASN: 65532)

Configuração Básica

Configuração Endereçamento

Vlan **v4:** 1004 - 192.168.0.30/21
Vlan **v6:** 1006 – 2001:db8::30/64

```
configure
set interfaces ethernet eth0 vif 1004 address '192.168.0.30/21'
set interfaces ethernet eth0 vif 1006 address '2001:db8::30/64'
commit
save
```

Configuração Básica - Filtros

Criação prefix-list (IPv4)

```
configure

set policy prefix-list MEU-BLOCO rule 10 action 'permit'
set policy prefix-list MEU-BLOCO rule 10 prefix '10.1.0.0/22'

set policy prefix-list MEU-BLOCO-IN rule 10 action 'permit'
set policy prefix-list MEU-BLOCO-IN rule 10 le '24'
set policy prefix-list MEU-BLOCO-IN rule 10 prefix '10.1.0.0/22'

set policy prefix-list MEU-BLOCO-0-22 rule 10 action 'permit'
set policy prefix-list MEU-BLOCO-0-22 rule 10 prefix '10.1.0.0/22'

set policy prefix-list MEU-BLOCO-0-23 rule 10 action 'permit'
set policy prefix-list MEU-BLOCO-0-23 rule 10 prefix '10.1.0.0/23'

set policy prefix-list MEU-BLOCO-2-23 rule 10 action 'permit'
set policy prefix-list MEU-BLOCO-2-23 rule 10 prefix '10.1.2.0/23'

commit&&save
```

Configuração Básica - Filtros

Criação prefix-list (IPv6)

```
configure

edit policy prefix-list6 MEU-BLOCO-V6
set rule 10 action 'permit'
set rule 10 prefix '2001:db8:8000::/33'
commit&&save

edit policy prefix-list6 MEU-BLOCO-V6-IN
set rule 10 action 'permit'
set rule 10 le '48'
set rule 10 prefix '2001:db8:8000::/33'
commit&&save

edit policy prefix-list6 MEU-BLOCO-V6-1-34
set rule 10 action 'permit'
set rule 10 prefix '2001:db8:8000::/34'
commit&&save

edit policy prefix-list6 MEU-BLOCO-V6-2-34
set rule 10 action 'permit'
set rule 10 prefix '2001:db8:c000::/34'
commit&&save
```

Configuração Básica

Criação route-map (IPv4)

```
configure

edit policy route-map PTT-IN
set rule 10 action 'deny'
set rule 10 match ip address prefix-list 'MEU-BLOCO-IN'

set rule 20 action 'permit'
set rule 20 set local-preference '500'
commit&&save

edit policy route-map PTT-OUT
set rule 10 action 'permit'
set rule 10 match ip address prefix-list 'MEU-BLOCO'

set rule 20 action 'permit'
set rule 20 match ip address prefix-list 'MEU-BLOCO-0-23'

set rule 30 action 'permit'
set rule 30 match ip address prefix-list 'MEU-BLOCO-2-23'
commit&&save
```

Configuração Básica

Criação route-map (IPv6)

```
configure
edit policy route-map PTT-IN-V6

set rule 10 action 'deny'
set rule 10 match ipv6 address prefix-list 'MEU-BLOCO-V6-IN'

set rule 20 action 'permit'
set rule 20 set local-preference '500'

commit&&save

edit policy route-map PTT-OUT-V6

set rule 10 action 'permit'
set rule 10 match ipv6 address prefix-list 'MEU-BLOCO-V6'

set rule 20 action 'permit'
set rule 20 match ipv6 address prefix-list 'MEU-BLOCO-V6-1-34'

set rule 30 action 'permit'
set rule 30 match ipv6 address prefix-list 'MEU-BLOCO-V6-2-34'

commit&&save
```

Configuração Básica

Criação neighbors (IPv4)

```
configure
edit protocols bgp 65530

set neighbor 192.168.0.201 description 'rs1.ptt.br'
set neighbor 192.168.0.201 'nexthop-self'
set neighbor 192.168.0.201 remote-as '65531'
set neighbor 192.168.0.201 route-map export 'PTT-OUT'
set neighbor 192.168.0.201 route-map import 'PTT-IN'
set neighbor 192.168.0.201 update-source 'eth0.1004'

set neighbor 192.168.0.202 description 'rs2.ptt.br'
set neighbor 192.168.0.202 'nexthop-self'
set neighbor 192.168.0.202 remote-as '65531'
set neighbor 192.168.0.202 route-map export 'PTT-OUT'
set neighbor 192.168.0.202 route-map import 'PTT-IN'
set neighbor 192.168.0.202 update-source 'eth0.1004'
.
set neighbor 192.168.0.202 description 'rs2.ptt.br'
set neighbor 192.168.0.202 'nexthop-self'
set neighbor 192.168.0.202 remote-as '65531'
set neighbor 192.168.0.202 route-map export 'PTT-OUT'
set neighbor 192.168.0.202 route-map import 'PTT-IN'
set neighbor 192.168.0.202 update-source 'eth0.1004'

commit&&save
```

Configuração Básica

Criação neighbors (IPv6)

```
configure
edit protocols bgp 65530

set neighbor 2001:db8::201 address-family ipv6-unicast 'nexthop-self'
set neighbor 2001:db8::201 address-family ipv6-unicast route-map export 'PTT-OUT-V6'
set neighbor 2001:db8::201 address-family ipv6-unicast route-map import 'PTT-IN-V6'
set neighbor 2001:db8::201 description 'rs1.ptt.br'
set neighbor 2001:db8::201 remote-as '65531'
set neighbor 2001:db8::201 update-source 'eth0.1006'

set neighbor 2001:db8::202 address-family ipv6-unicast 'nexthop-self'
set neighbor 2001:db8::202 address-family ipv6-unicast route-map export 'PTT-OUT-V6'
set neighbor 2001:db8::202 address-family ipv6-unicast route-map import 'PTT-IN-V6'
set neighbor 2001:db8::202 description 'rs2.ptt.br'
set neighbor 2001:db8::202 remote-as '65531'
set neighbor 2001:db8::202 update-source 'eth0.1006'

set neighbor 2001:db8::210 address-family ipv6-unicast 'nexthop-self'
set neighbor 2001:db8::210 description 'lg.ptt.br'
set neighbor 2001:db8::210 remote-as '65532'
set neighbor 2001:db8::210 update-source 'eth0.1006''

commit
save
```

Configuração Básica

Networks (IPv4 e IPv6)

```
configure

edit protocols bgp 65530

set network '10.1.0.0/22'
set network '10.1.0.0/23'
set network '10.1.2.0/23'

set address-family ipv6-unicast network '2001:db8:8000::/33'
set address-family ipv6-unicast network '2001:db8:8000::/34'
set address-family ipv6-unicast network '2001:db8:c000::/34'

commit
save
```

Configuração Básica

Anúncios

Para que uma rede seja anunciada no bgp, ele deve (ou deveria) estar na FIB. Para tal, existem três maneiras básicas de fazermos isso.

1 – Utilizando-a em uma interface
2 – Colocando-a em blackhole
3 – Criando uma rota estática

```
configure
set protocols static route 10.1.0.0/22 'blackhole'
set protocols static route 10.1.0.0/23 'blackhole'
set protocols static route 10.1.2.0/23 'blackhole'
set protocols static route6 2001:db8:8000::/33 'blackhole'
set protocols static route6 2001:db8:8000::/34 'blackhole'
set protocols static route6 2001:db8:c000::/34 'blackhole'
apply&&save
```

Problemas Comuns (EdgeRouter)

NTP nosso de cada dia!

- Durante o boot, até a versão 1.6, o processo do ntp “sobe” antes do processo do bgp.
- Como nesse momento o roteador ainda não tem conectividade com a internet e, como por padrão o ntp vem configurado com os servidores da ubnt, ele simplesmente não consegue sincronizar.
- Além disso, não há um **timeout** setado, o que faz com que o processo “pendure” o boot.

Problemas Comuns (EdgeRouter)

BGPD

Como o processo do ntp “pendurou” o boot, o processo do bgp não sobe e quando qualquer comando relacionado ao bgp for executado, ele simplesmente retornará uma mensagem dizendo que não há nada referente a bgp configurado.

- No arquivo de configuração, as configurações de bgp ainda existem (cat /config/boot.config).
- Confuso!

Problemas Comuns (EdgeRouter)

BGPD

- Nem tanto!
- A configuração existe mas o processo não subiu.
- **Solução:**
- Desativar o ntp na inicialização:

```
configure
delete system ntp
commit
save
```

Problemas Comuns

Informações Adicionais!

- Problema reportado em Dez/14
- *Solucionado na versão 1.7alpha*

Problemas Comuns - Quarentena

Limite da Tabela ARP

- Um dos testes da “quarentena” é verificar a quantidade de macs permitidos.
- Por padrão, tanto o vyatta, quanto o vyos (incluindo a edgerouter) permitem 128 / 512 / 1024.
- PTT-SP utiliza um /21 (2048 ips)
- Comando para alterar (segundo documentação):

```
set system ip arp table-size
```

Problemas Comuns - Quarentena

Limite da Tabela ARP (Kernel Tuning)

- Porém, a forma como o comando aplica as configurações não são eficientes...

- Parâmetros:

```
net.ipv4.neigh.default.gc_thresh1
net.ipv4.neigh.default.gc_thresh2
net.ipv4.neigh.default.gc_thresh3
```

Problemas Comuns - Quarentena

Limite da Tabela ARP (Kernel Tuning)

- `net.ipv4.neigh.default.gc_thresh1`

  Esse valor refere-se a quantidade mínima de macs na tabela antes que o “coletor de lixo” seja executado.

- `net.ipv4.neigh.default.gc_thresh2`

  Quantidade intermediária, o coletor permitirá que esse valor seja ultrapassado por 5 segundos antes de agir.

Problemas Comuns - Quarentena

Limite da Tabela ARP (Kernel Tuning)

- `net.ipv4.neigh.default.gc_thresh3`

  O valor máximo suportado. O coletor sempre será executado se houver mais do que o valor setado nesse parâmetro.

- O problema do comando recomendado na documentação oficial é que ele seta os valores de cima para baixo.

- Exemplo:

  `set system ip arp table-size 8192`

  (gc_thresh3 = 8192, 2 = 4096, 1 = 1024)

Problemas Comuns - Quarentena

Limite da Tabela ARP (Kernel Tuning)
Recomendações

```
gc_thresh3 = 8192
gc_thresh2 = 4096
gc_thresh1 = 2048
```

Ainda há outros parâmetros importantes que devem ser configurados:

```
net.ipv4.neigh.default.gc_interval
```

Indica de quanto em quanto tempo o coletor deve tentar rodar. Padrão 30, recomendável 60.

Problemas Comuns - Quarentena

Limite da Tabela ARP (Kernel Tuning)
Recomendações

```
net.ipv4.neigh.default.gc_stale_time
```

Determina a frequência de checagem por vizinhos “travados”, quando um vizinho é considerado “travado” será feita uma nova resolução antes de enviar dados novamente a ele.

- A forma mais rápida (eficiente) de se configurar todos esses parâmetros é adicionando diretamente ao arquivo sysctl.conf (geralmente em /etc) e executando o comando:

```
sysctl -p
```

Problemas Comuns - Quarentena

Limite da Tabela ARP (Kernel Tuning)
Recomendações

```
cat /etc/sysctl.conf

   net.ipv4.neigh.default.gc_thresh1 = 2048
   net.ipv4.neigh.default.gc_thresh2 = 4096
   net.ipv4.neigh.default.gc_thresh3 = 8192
   net.ipv4.neigh.default.gc_interval = 60
   net.ipv4.neigh.default.gc_stale_time = 120
```

Problemas Comuns

Neighbor IPv6

Tanto o VyOS (e EdgeRouter), quanto o Vyatta, aceitam que se configure vizinhos diferenciando maiúsculas de minúsculas.

Porém, o Quagga (que roda por baixo) não aceita.

Assim, se você adicionar um vizinho com letras maiúsculas e depois algum com minúscula, você conseguirá remover apenas o primeiro.

Ao tentar remover o segundo, você receberá uma mensagem informando que o vizinho não existe (apesar de aparecer na configuração).

Sugestões

Recomendações Adicionais

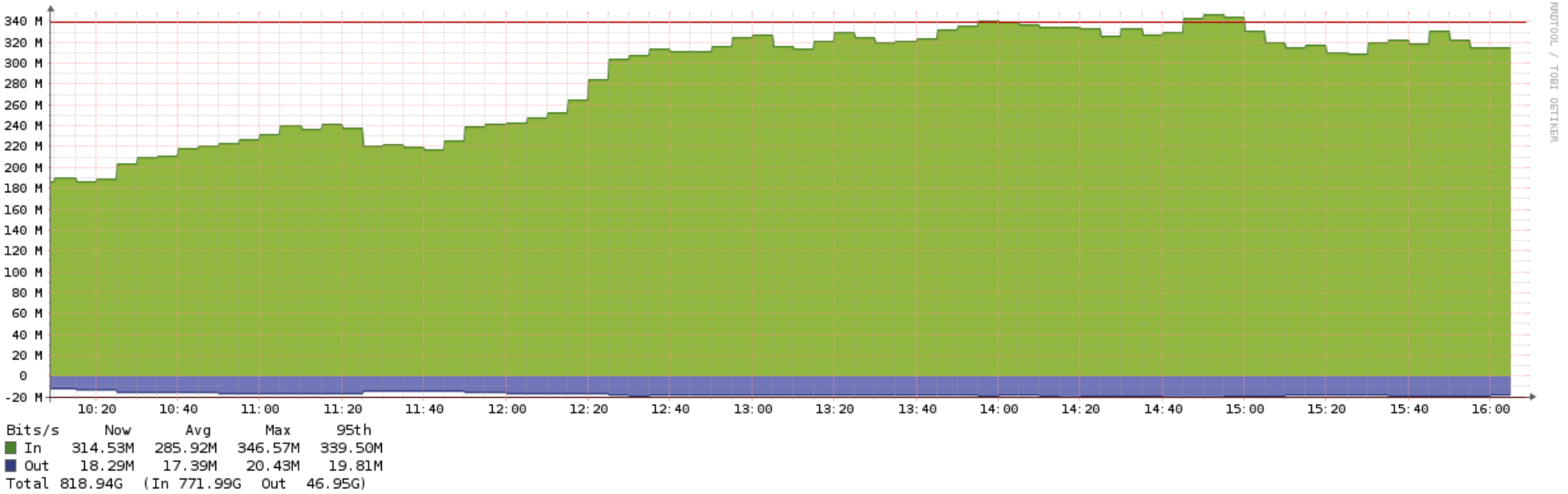
- Evitar deixar serviços nas portas default.

- Desabilitar a interface web quando se exige bastante do equipamento.

- Não utilizar nome de usuário padrão.

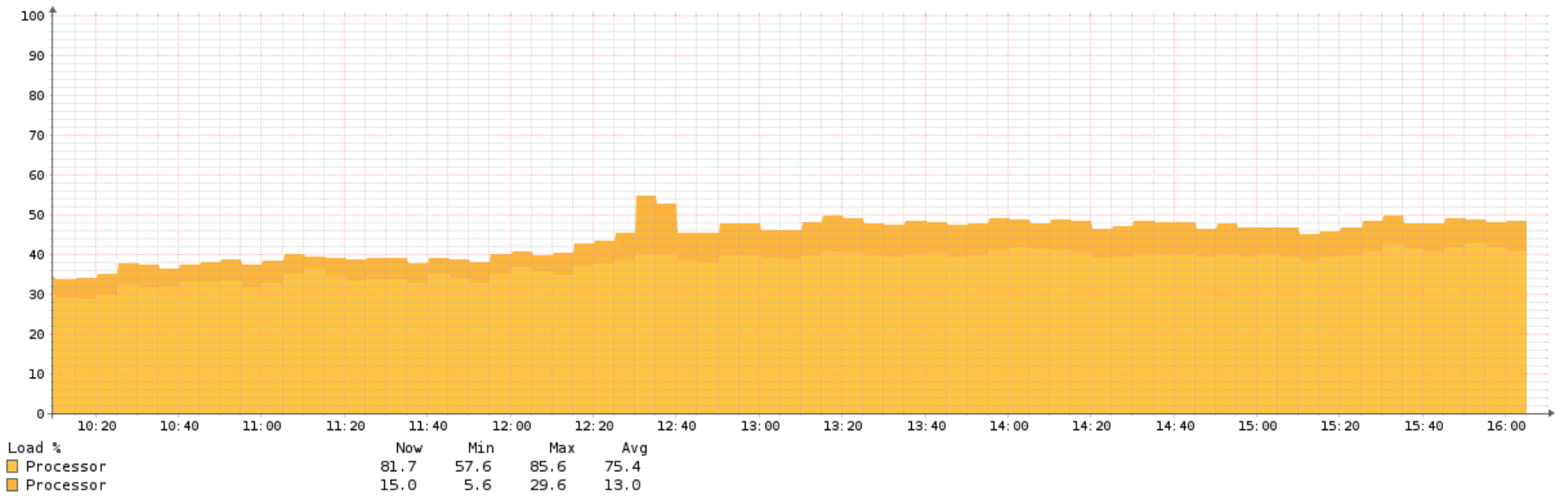
Case Real

Dados com Edgerouter 8 PRO
(VILAVNET – SP)



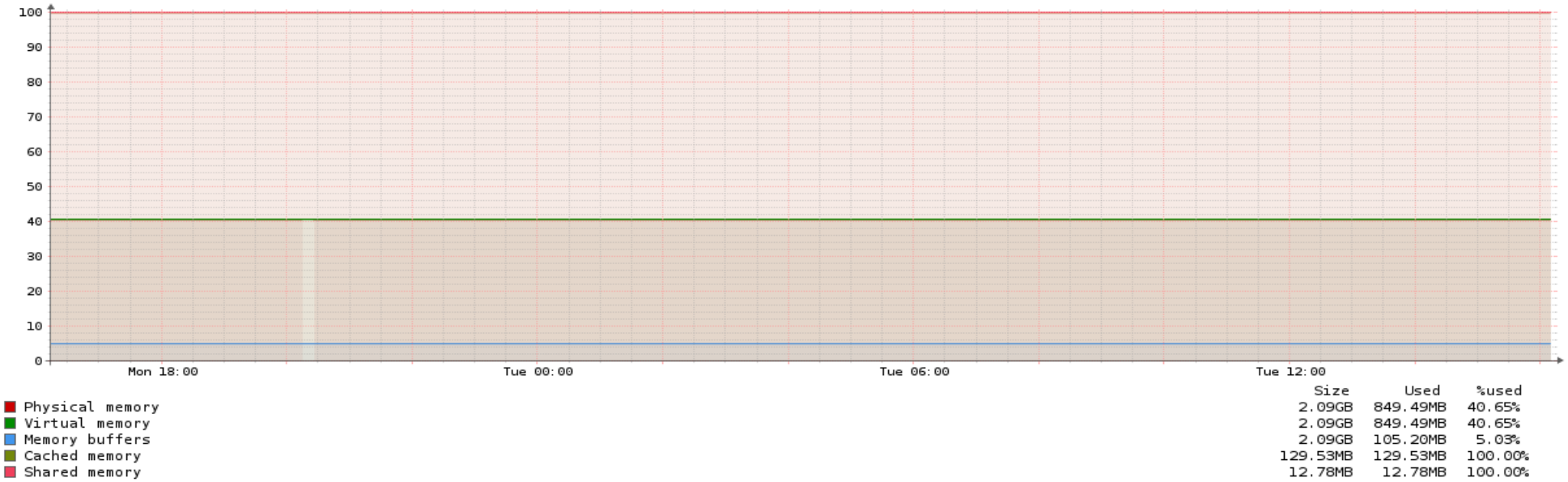
Case Real

Dados com Edgerouter 8 PRO
(VILAVNET – SP)



Case Real

Dados com Edgerouter 8 PRO
(VILAVNET – SP)



Fontes de Referência

Leitura Recomendada

Análise de Vulnerabilidades de Redes em Conexões com PTT
Eduardo Ascenço Reis
ftp://ftp.registro.br/pub/gter/gter27/06-vul-con-ptt.pdf

Estudo de Caso de Sistema Autônomo (AS) com Conexão a PTT Local, Remoto e Provedores de Trânsito
Antonio Galvao de Rezende Filho
Eduardo Ascenço Reis
ftp://ftp.registro.br/pub/gter/gter27/06-vul-con-ptt.pdf

Boas práticas para peering no PTTMetro
Luís Balbinot
ftp://ftp.registro.br/pub/gter/gter30/02-BoasPraticasPTTMetro.pdf

Configuração Completa desta Apresentação
http://pastebin.com/YL268YrJ

Agradecimentos

Rubens Kuhl

Marcelo Machado | Renato Mezari |Vagner Zanoni

Obrigado!

Elizandro Pacheco

elizandro@pachecotecnologia.net.br

Fone(s): 51 9871-8111 | 48 9687-7766

Skype: elizandropacheco