BRAS de alta capacidade + CGNAT Com Mikrotik

MUM 2019 Brasil
Foz Iguaçu - PR

Flávio Gomes Figueira Camacho Junior

- Brasil, Rio de Janeiro
- 8 anos de experiencia com Telecomunicações
- Engenheiro de Rede na empresa TELECALL
- Consultor de Tecnologia empresa COMTXAI
- Trainer Oficial Mikrotik
- Certificações: MTCNA, MTCWE, MTCTCE, MTCUME, MTCIP
  MTCINE e MTCSE
- Contato: flaviocamacho95@gmail.com
- Contato: +55 (21) 96978-4675
- https://mikrotik.com/consultants

Objetivo

- Apresentar como implementar uma solução com alta capacidade de cliente banda larga em dispositivos Mikrotik.
  - Switch de agregação
  - BRAS para autenticação e limitação de banda
  - Solução CGNat para todos clientes

Sumári

- Apresentação
  - Descrever o que é um BRAS
  - Tipos de BRAS
  - Importância de uma boa solução BRAS para ISP

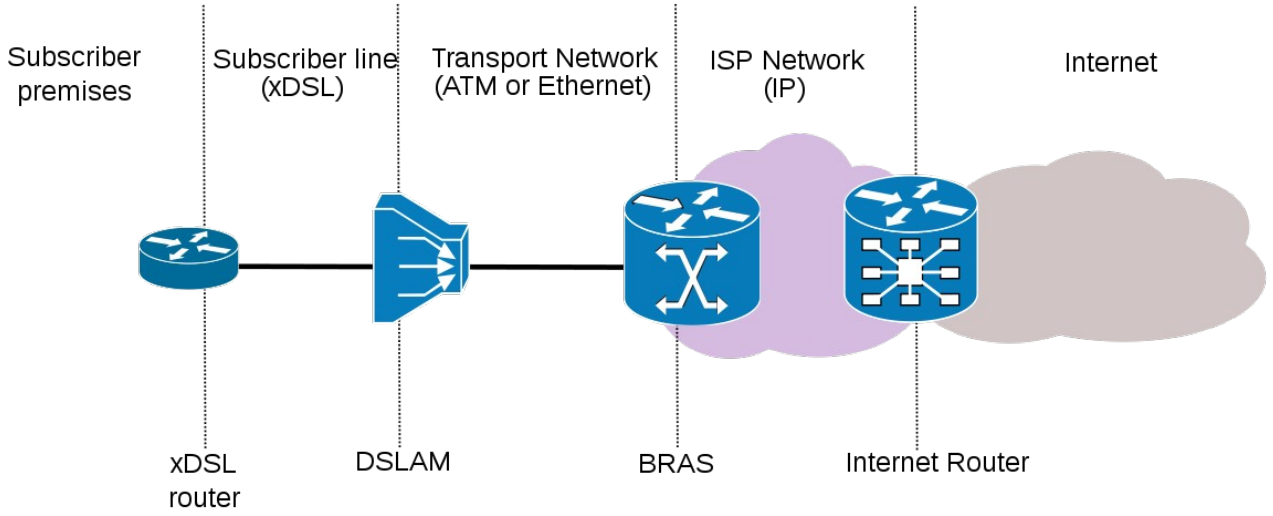
Introduçã

O

- Importância de uma boa solução BRAS para ISP
  - Autenticação de Usuários
  - Exaustão do IPv4
  - Mais com menos
  - IPv6 Ready
  - Pay as you grow (simples)
  - Menos configurações necessárias
  - Estável e resiliente
  - Pronto para mudanças e upgrades
  - Qualidade para os clientes

O que é um BRAS?

Broadband remote access server



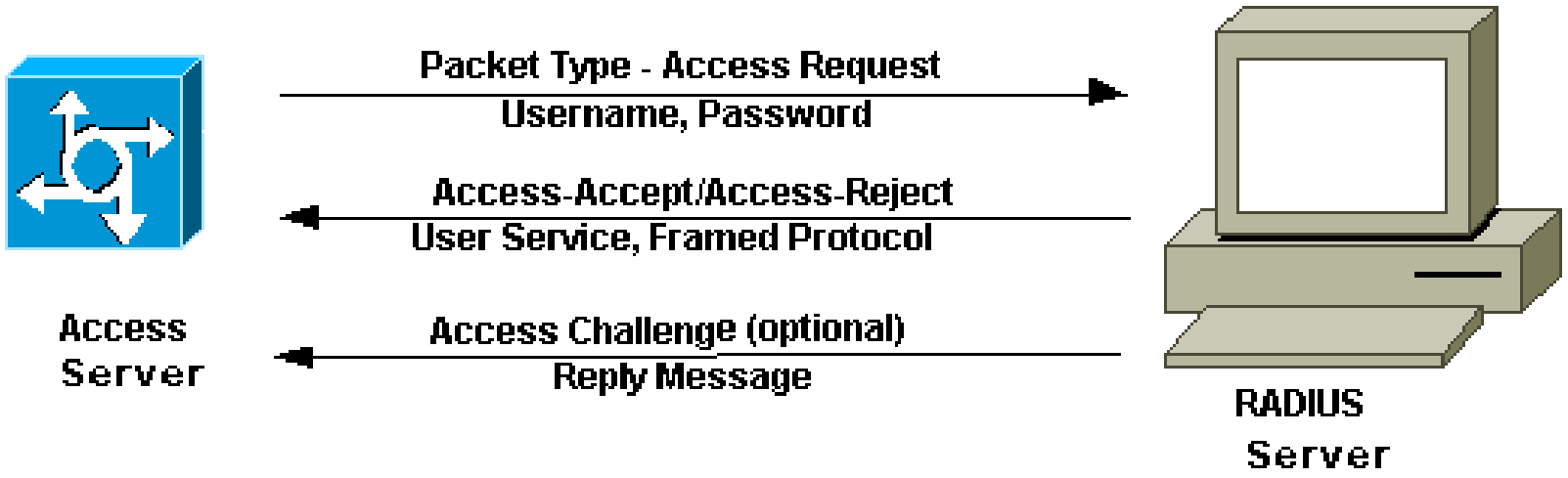
Tipos

- PPPoE (PPPoE, PPPoA)
- DHCP
- DHCP + option 82 (IPoE)
- Hotspot

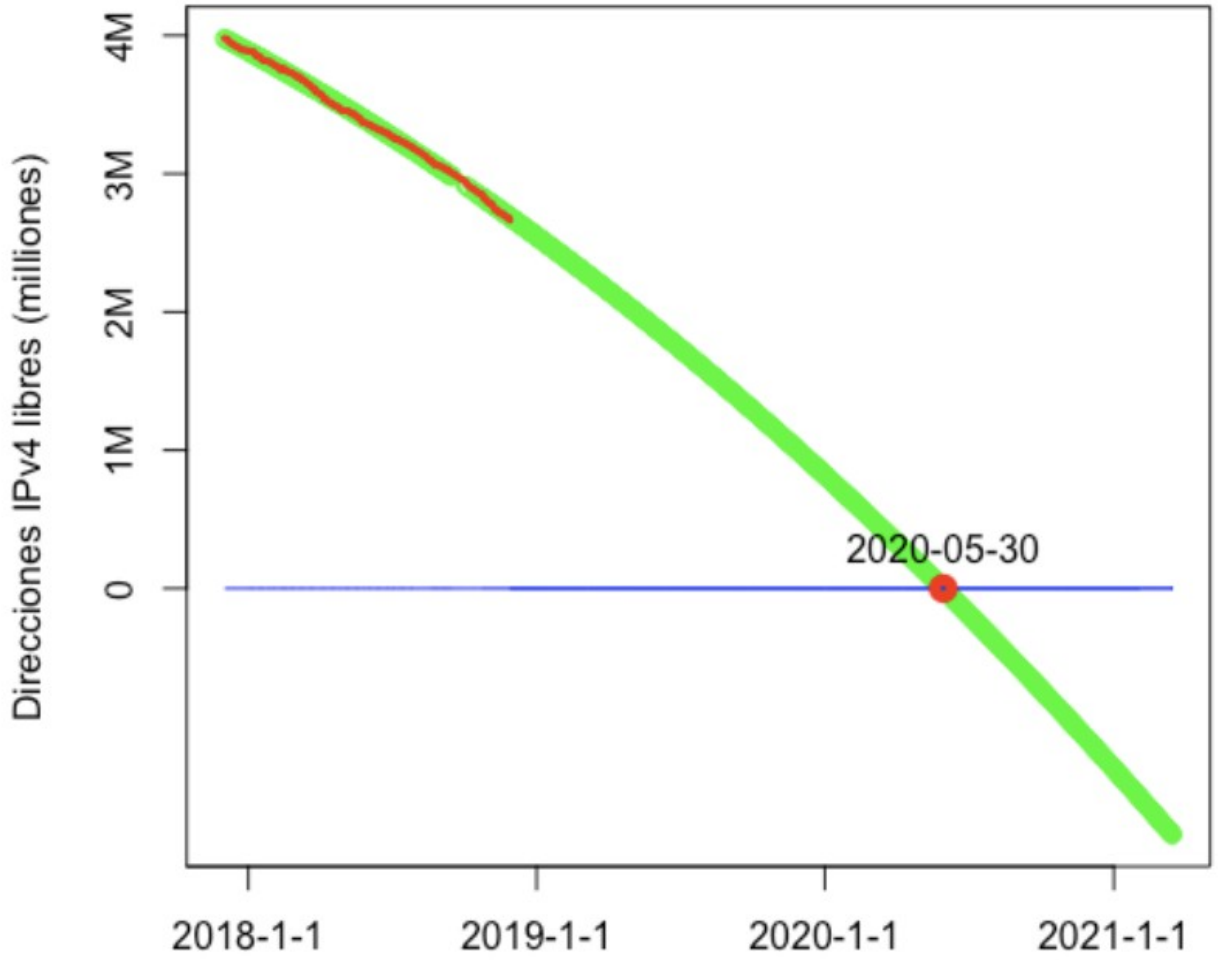
Autenticação dos clientes

- Bloqueio Automático
- Bandwidth (Limitação de Banda)
- Upgrade pelo sistema Radius (CoA)
- Sem interações/configurações no BRAS

Radius – O que é?



IPv4 Exhaustion



https://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4

Calculando

1 IP = 65535 tcp/udp ports

1 aproximadamente utiliza 300 portas

Então 65535/300 =~ 218

1 IP público atende 218 clientes

Quanto maior a quantidade de clientes por IP, maior poderá ser a perda de qualidade no serviço.

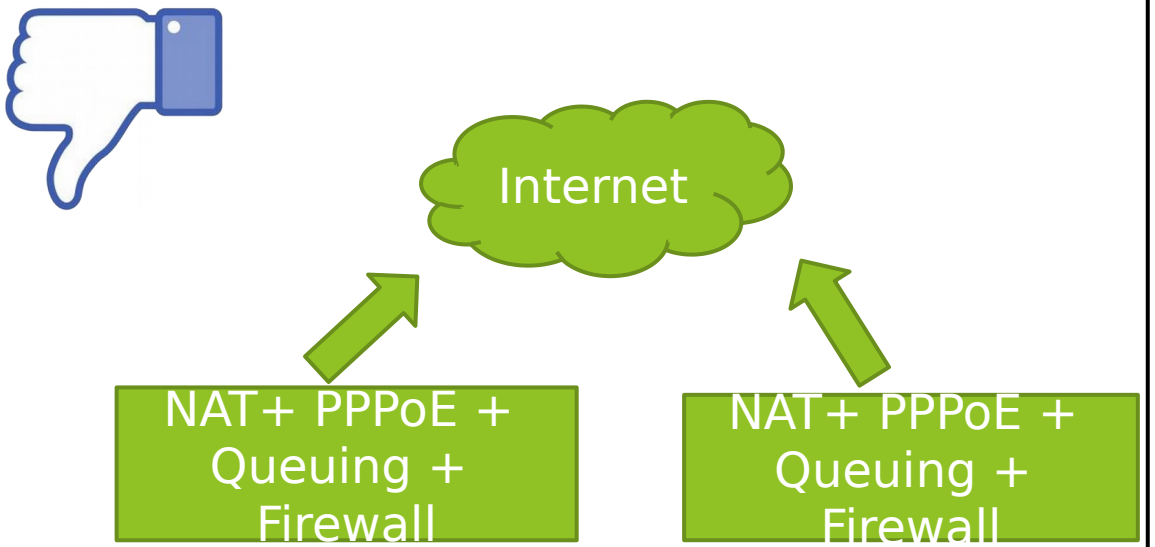
Obter melhor performance

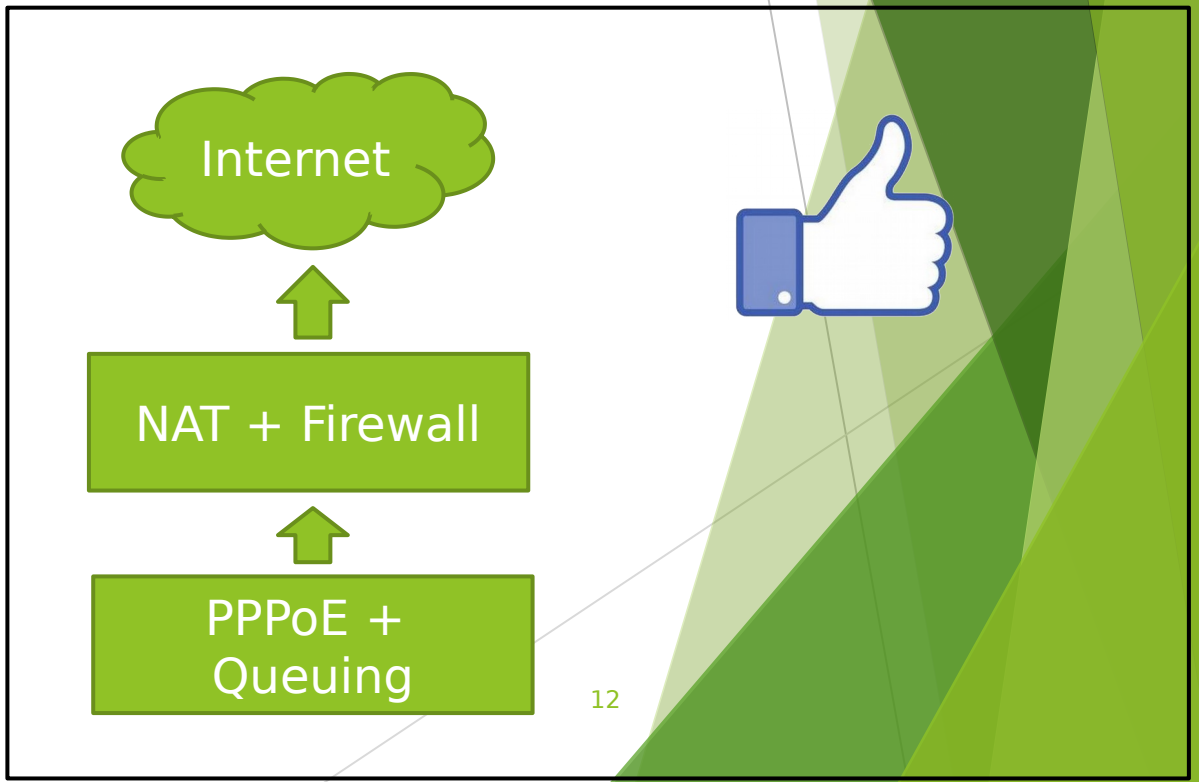
O que é melhor?

2 routers fazendo NAT + Queuing + PPPoE + Firewall

OU

2 routers uma fazendo Queue + PPPoE, e a outra fazendo NAT + Firewall





IPv6 Ready

Dual Stack Network

Pay as you grow

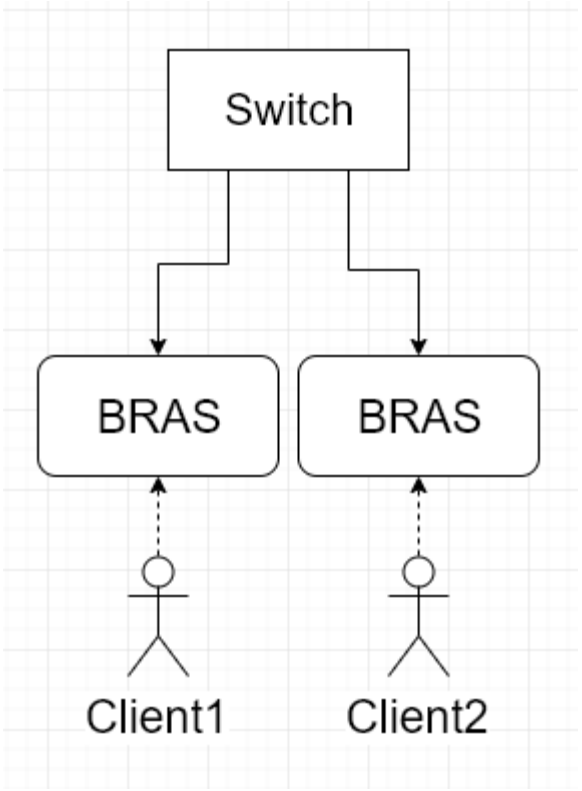
Integração ERP

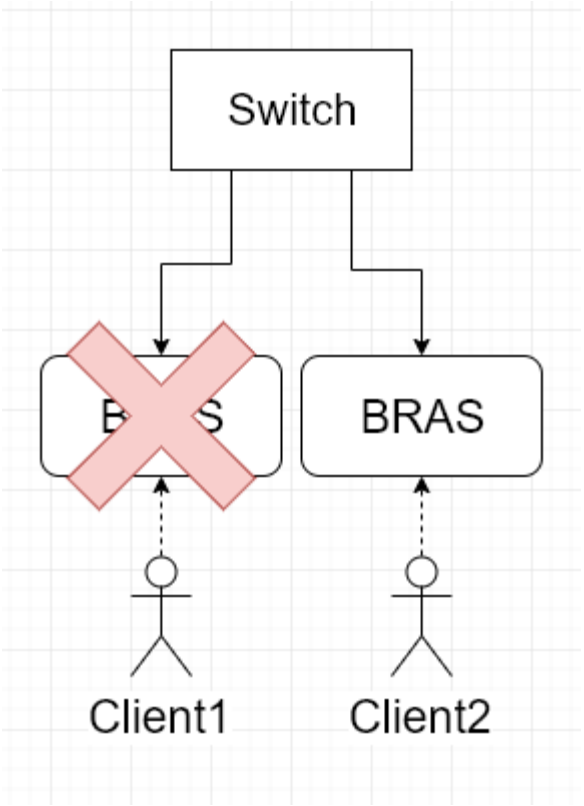
Integração com RADIUS faz o controle ficar mais SDN

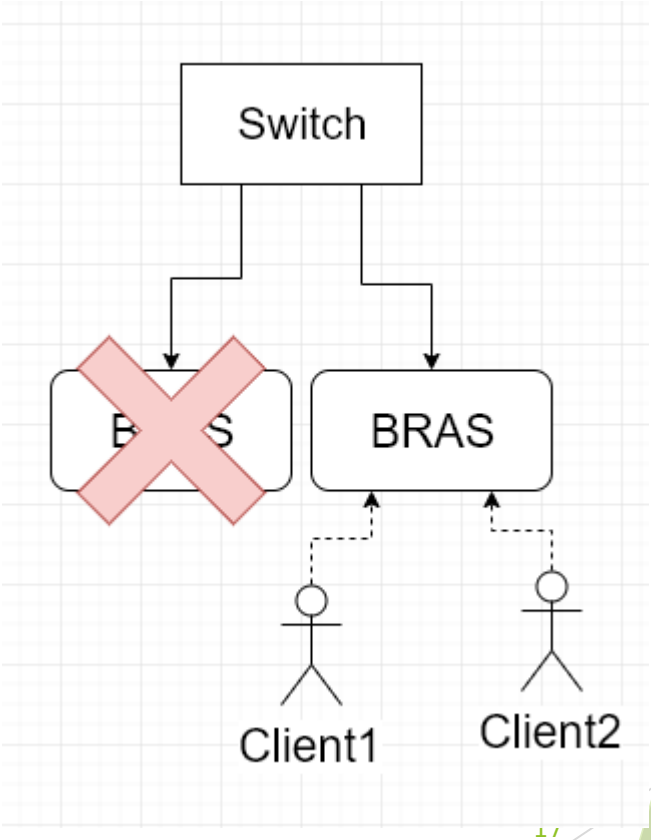
Escalável

O número e os tipos de BRAS são controlados conforme o crescimento.

Resiliente


Switch
BRAS
BRAS
Client1
Client2

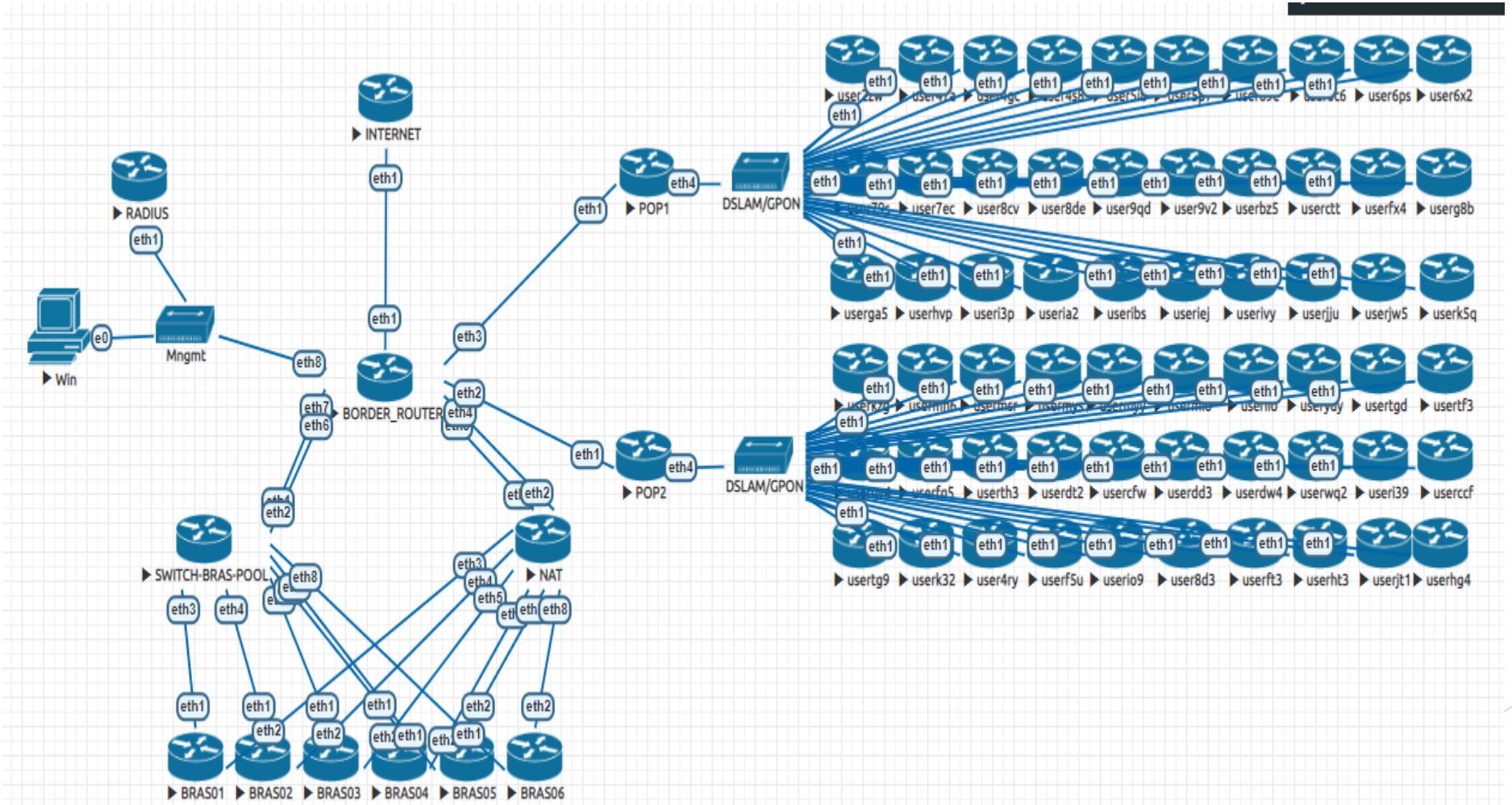

Switch
BRAS
Client1
Client2


Switch
BRAS
Client1
Client2

Qualidade para os cliente!

Como fazer isso?

Estudo de caso



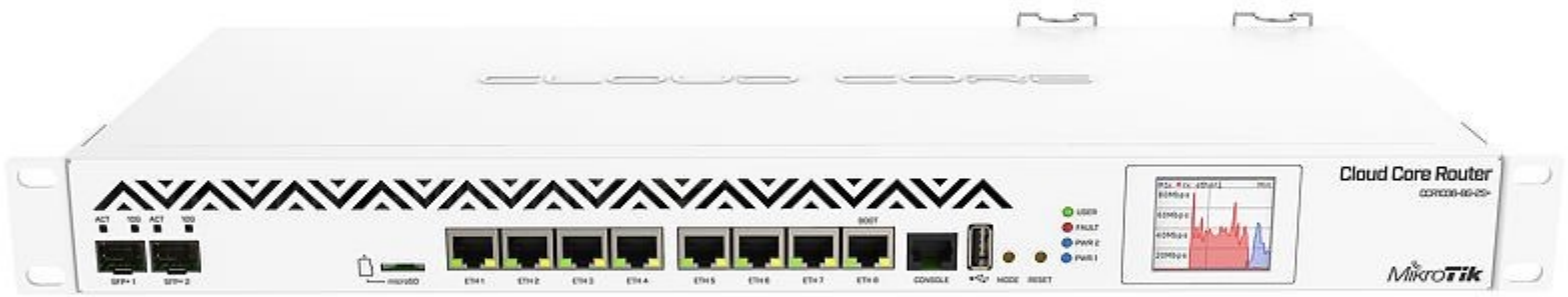
Switch Concentrador
SWITCH-BRAS-POOL

- CRS317-1G-16S+RM
  - 16 SFP+ ports
  - Bounding Hardware offload
  - 2 Power Supplies

BRAS para o Pool

BRAS

- CCR1036-8G-2S+EM
  - 36 Cores
  - 8GB RAM
  - 2 SFP+ ports
  - 2 Power Supplies



CGNat

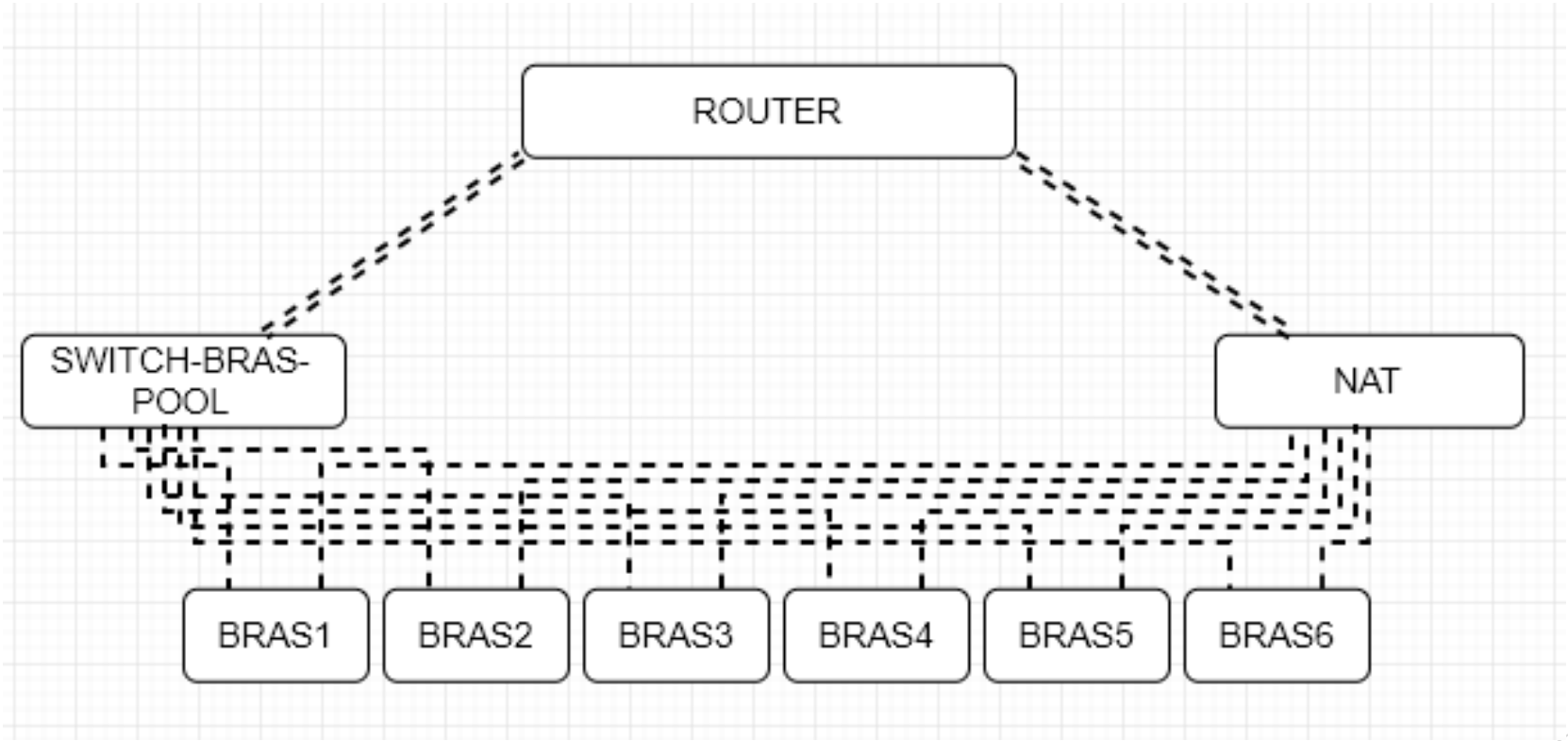
NAT

- CCR1072-1G-8S
  - 72 Cores
  - 16GB RAM ECC
  - 8 SFP+ ports
  - 2 Power Supplies Hot Swap

Direct Attach

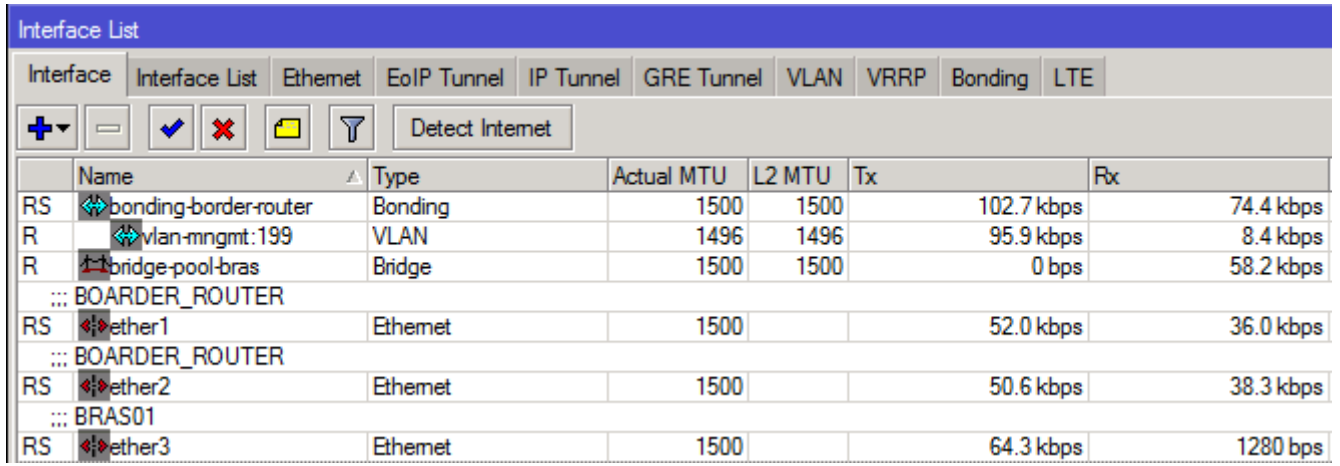
- S+DA0001
  - SFP+ direct attach cable, 1m

Diagrama de Conexões



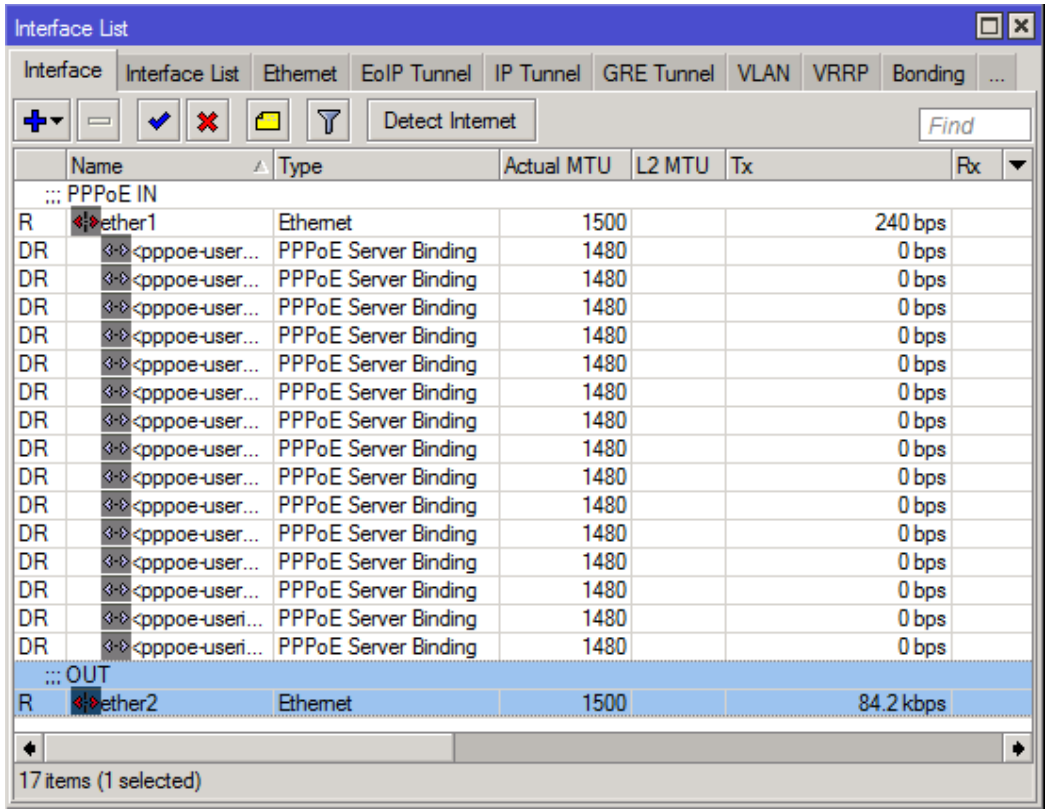
Switch - Cenário Logico

- Hardware Offload: configurada uma interface Bound para o router onde os clientes serão transportados.
- Criar uma vlan na bounding para gerência do switch
- Utilizar Hardware Offload em todas interfaces com bridge



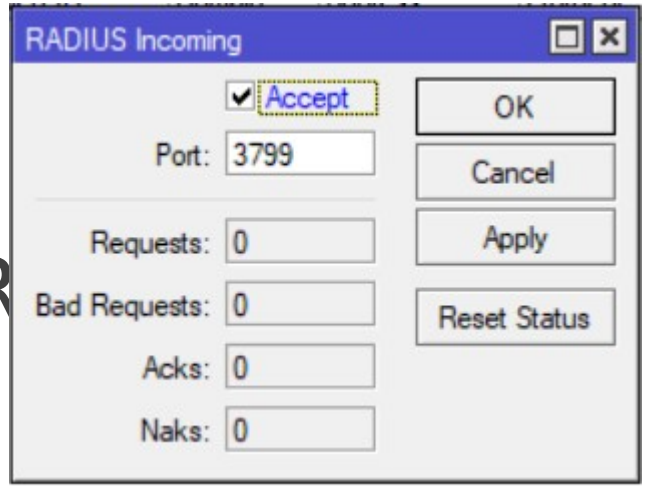
BRAS - Cenário Logico

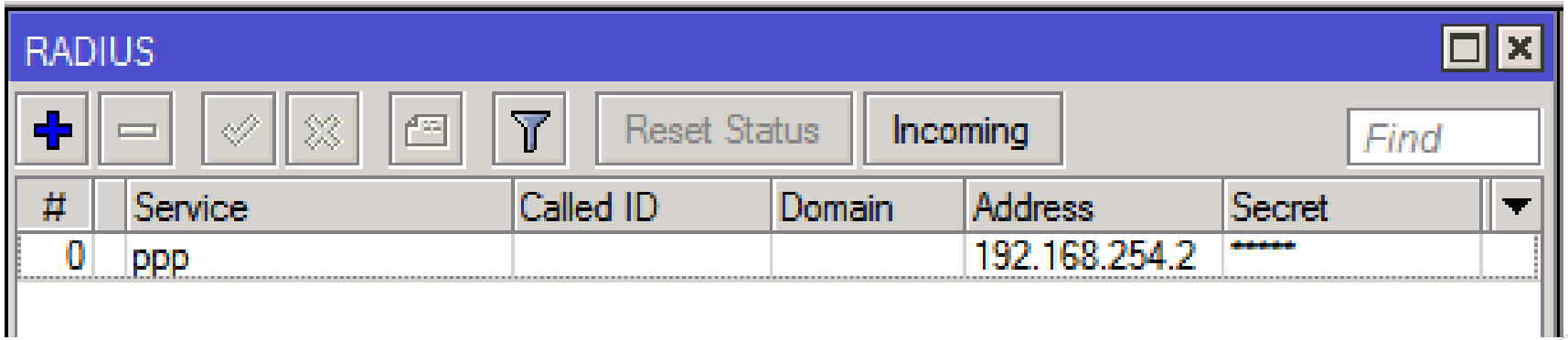
- Use uma das interfaces para PPPoE IN, e a outra para OUT traffic
- A interface PPPoE IN vai conecta com o Switch Concentrador e a interface OUT com o CGNat



BRAS - Cenário Logico

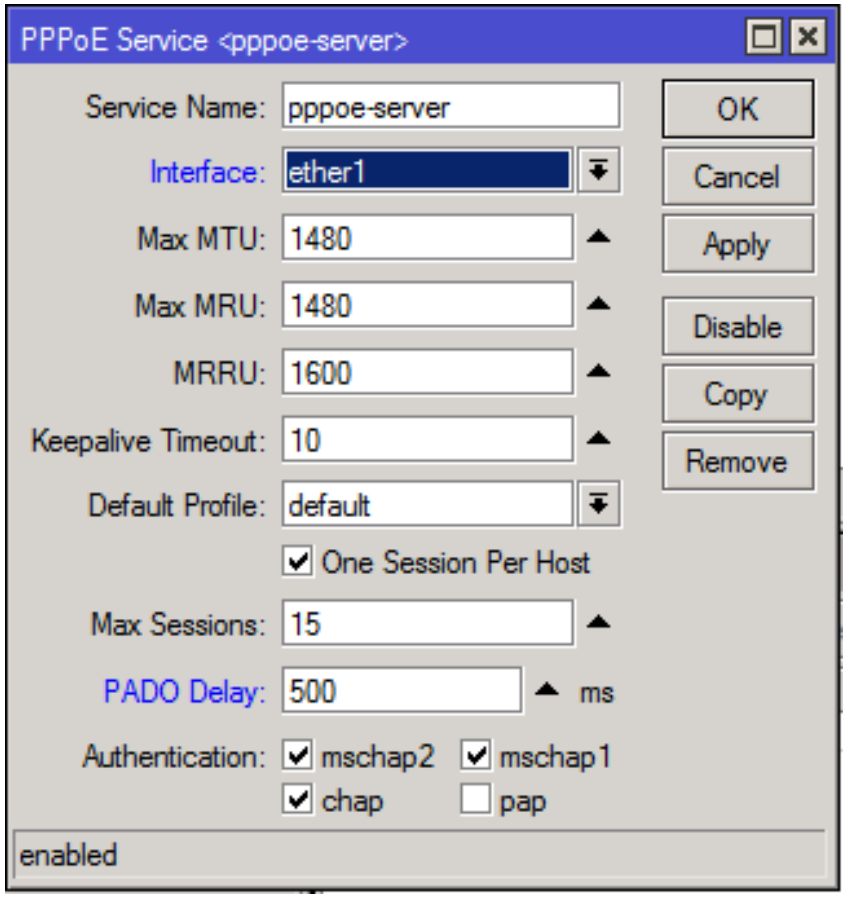
- Configurado RADIUS do ER

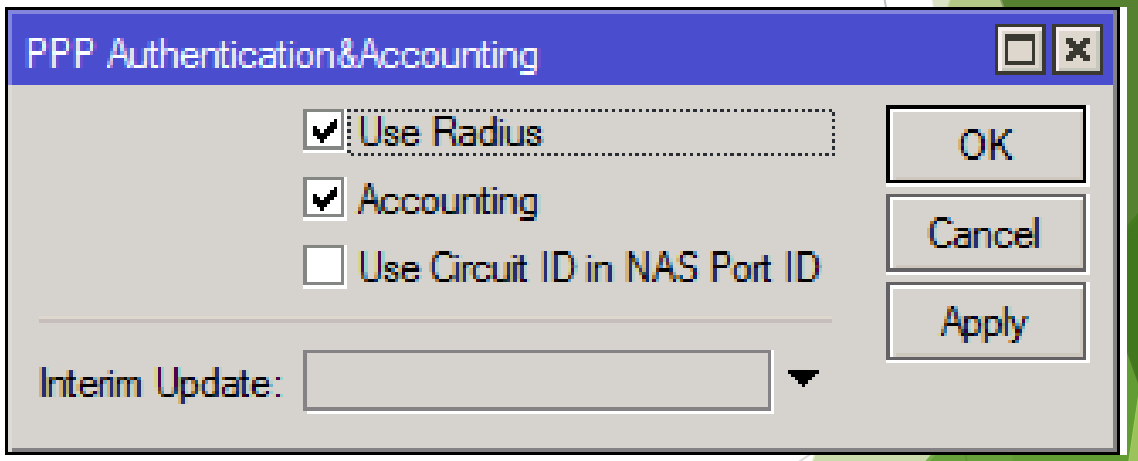




BRAS - Cenário Logico

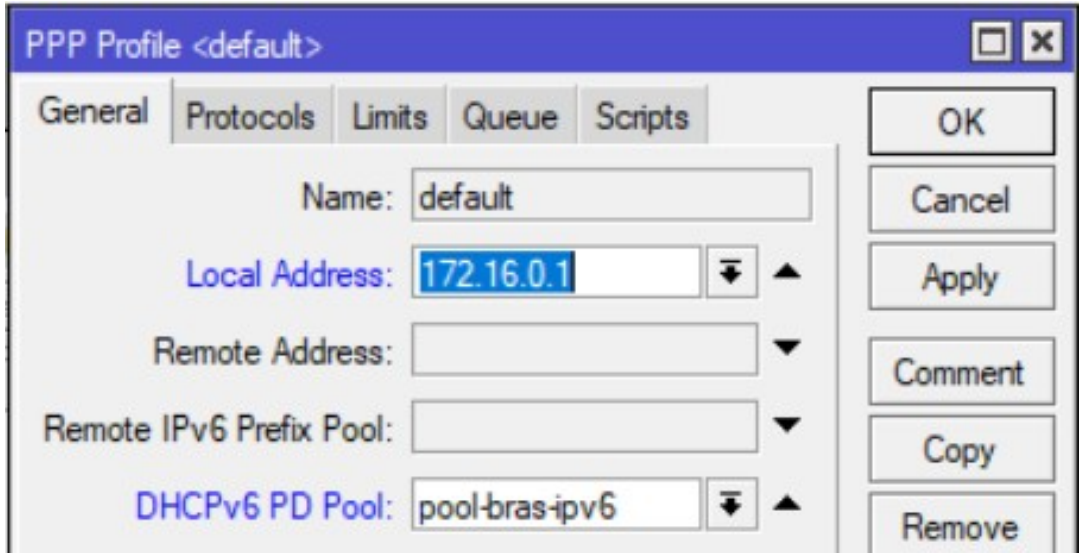
- Configurado ppp para usar Radius, PPPoE Server com PADO Delay para balancear usuário no Pool e Max Session para limitar a quantidade de usuários no BRAS

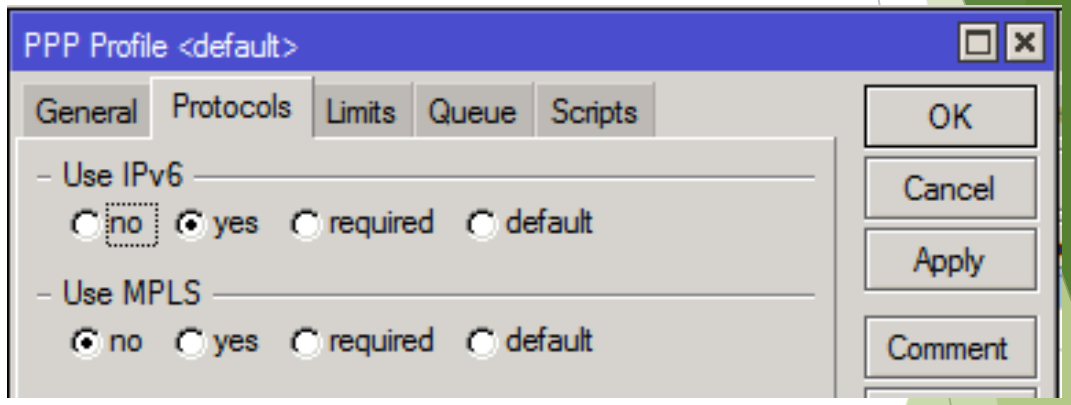


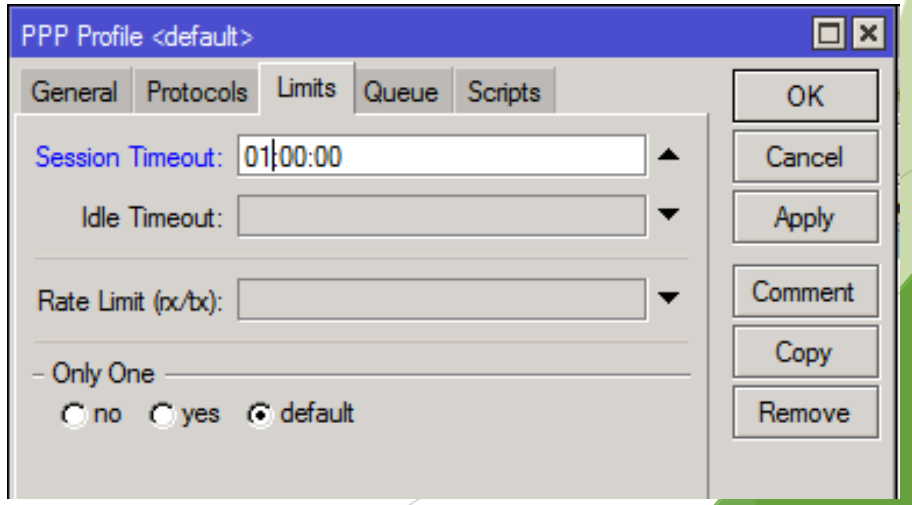


BRAS - Cenário Logico

- Configurado o ppp Profile Local Address, use IPv6 yes e a Session Timeout para janelas de manutenção
- Configurado o DHCPv6 PD pool

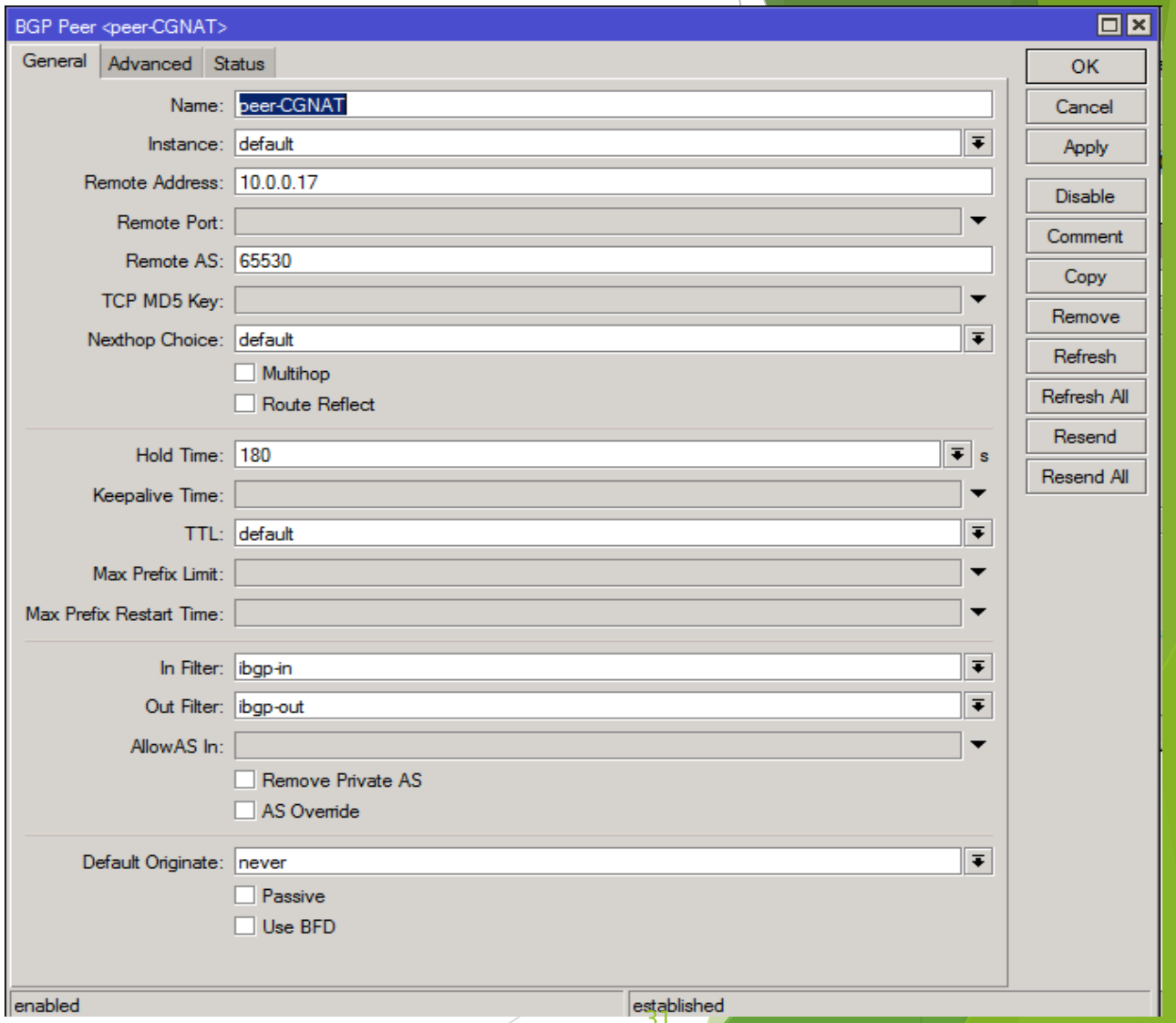


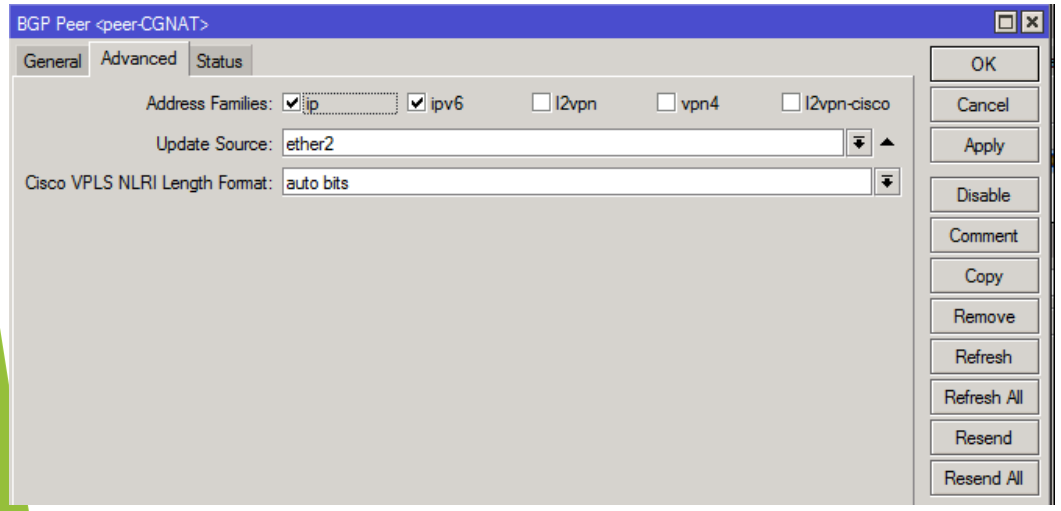




BRAS - Cenário Logico

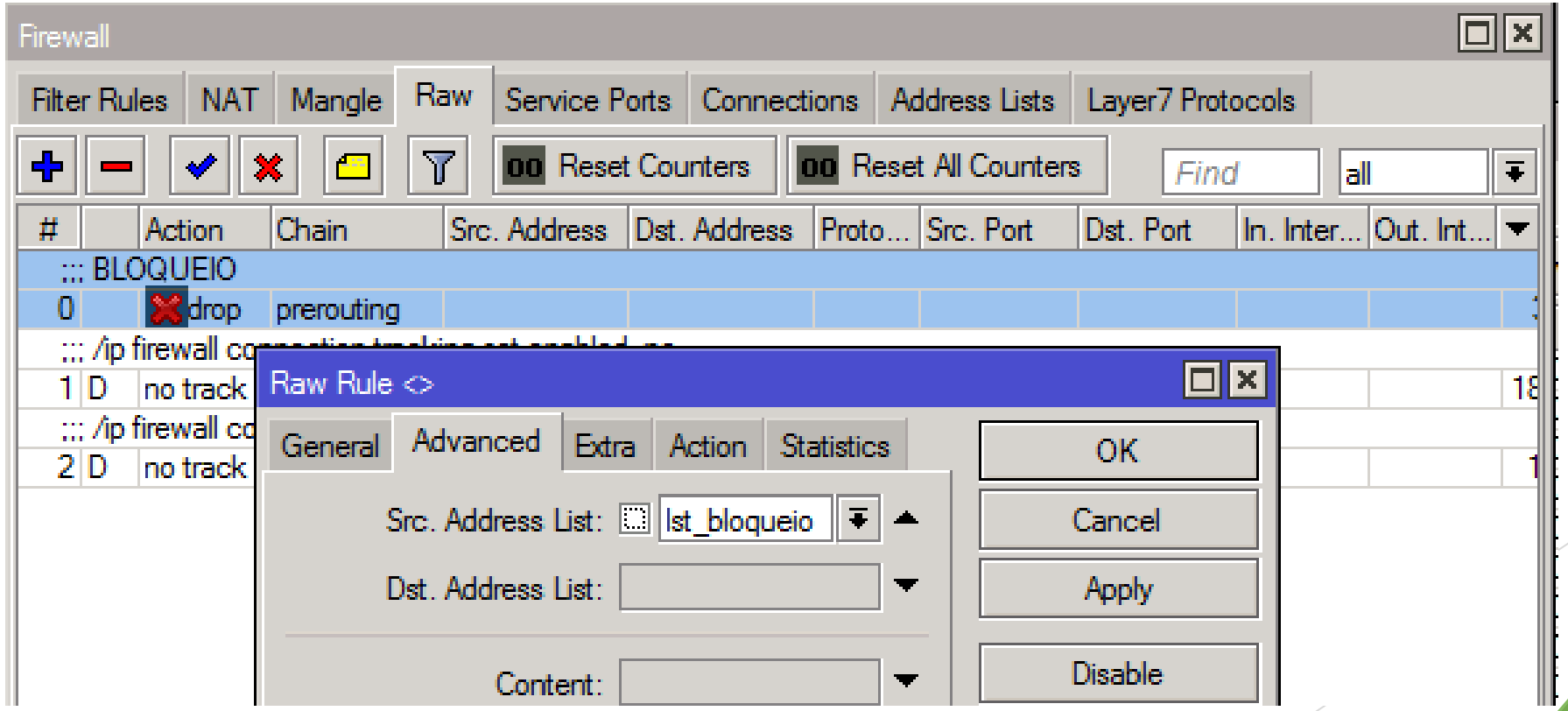
- Configurado iBGP com a router de CGNat para redistribuir a rota dos cliente conectados e receber a rota default.
- Selecionado ip e ipv6 para o dual-stack





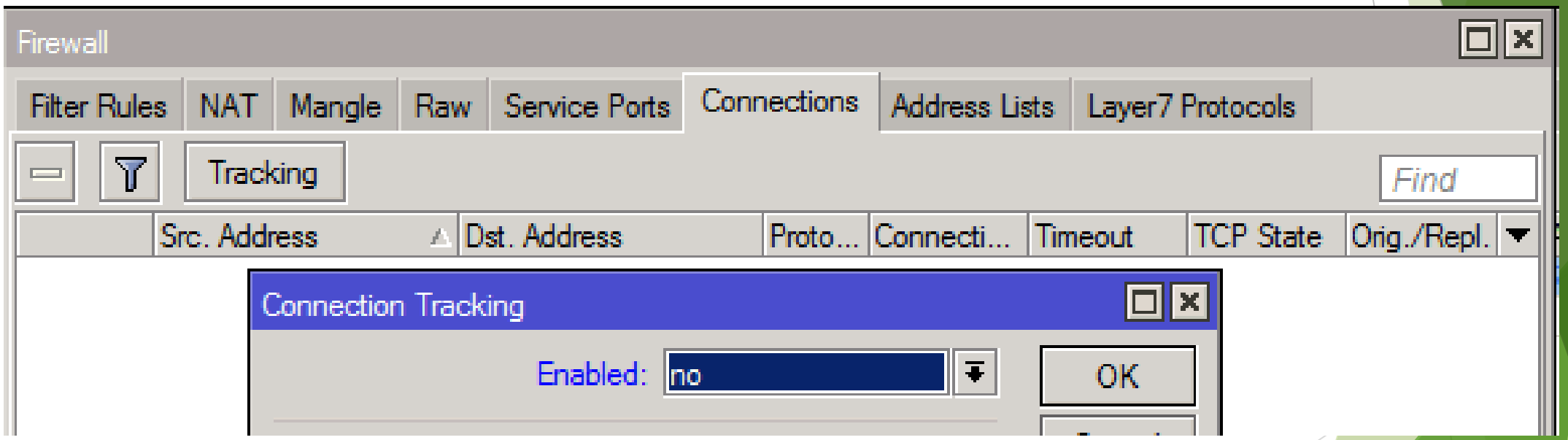
BRAS - Cenário Logico

- Configurado Firewall Raw com regra bloqueando ips da address-list lst_bloqueio, para bloqueio de clientes



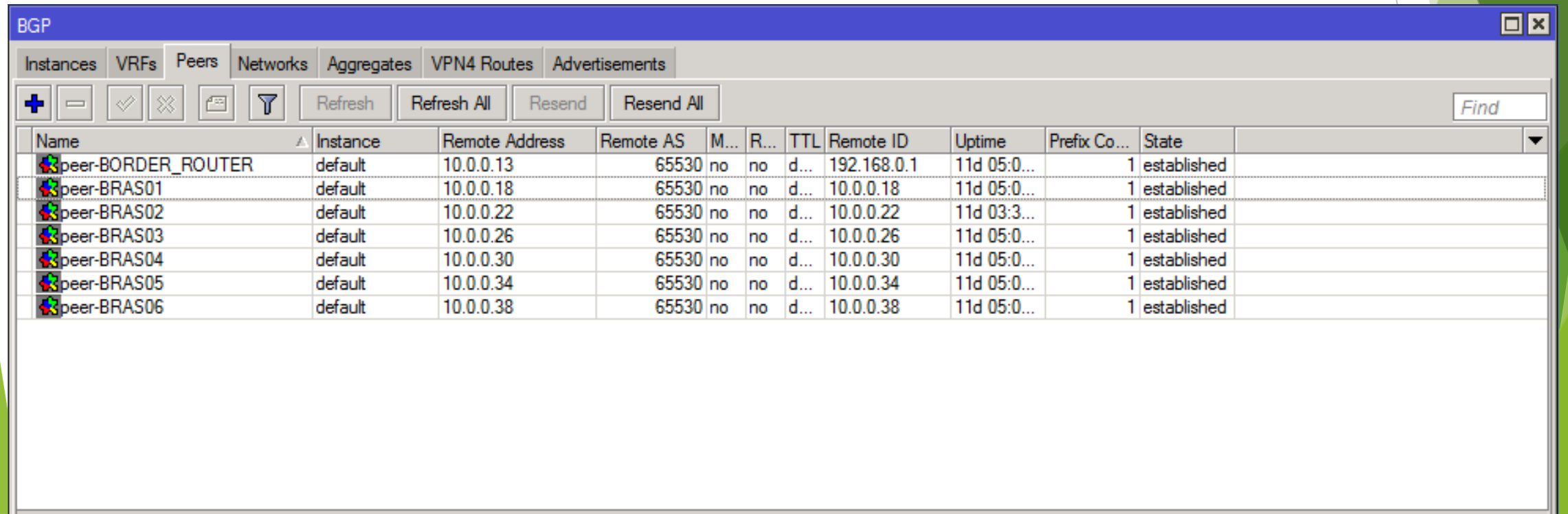
BRAS - Cenário Logico

- Desativado o Tracking para otimizar o BRAS



CGNAT - Cenário Logico

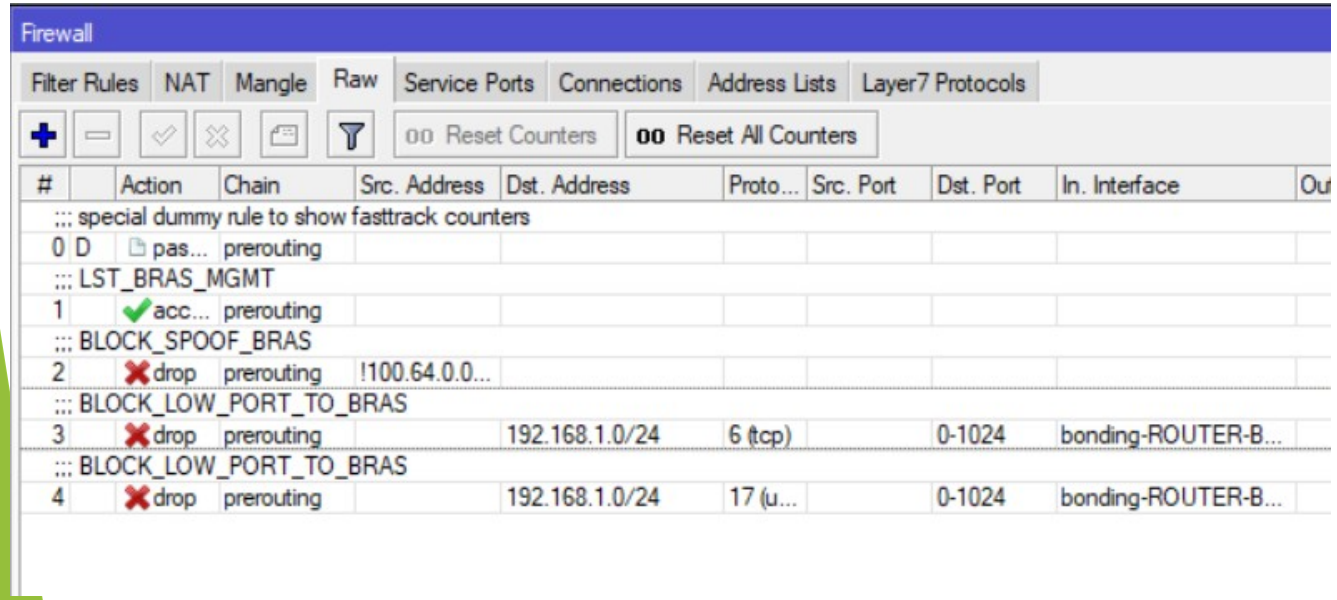
- Configurado iBGP com todos os BRAS enviando rota default, iBGP com a router de borda para receber a rota default e enviar as rotas do Pool BRAS
- Selecionado ip e ipv6 for para dual-stack

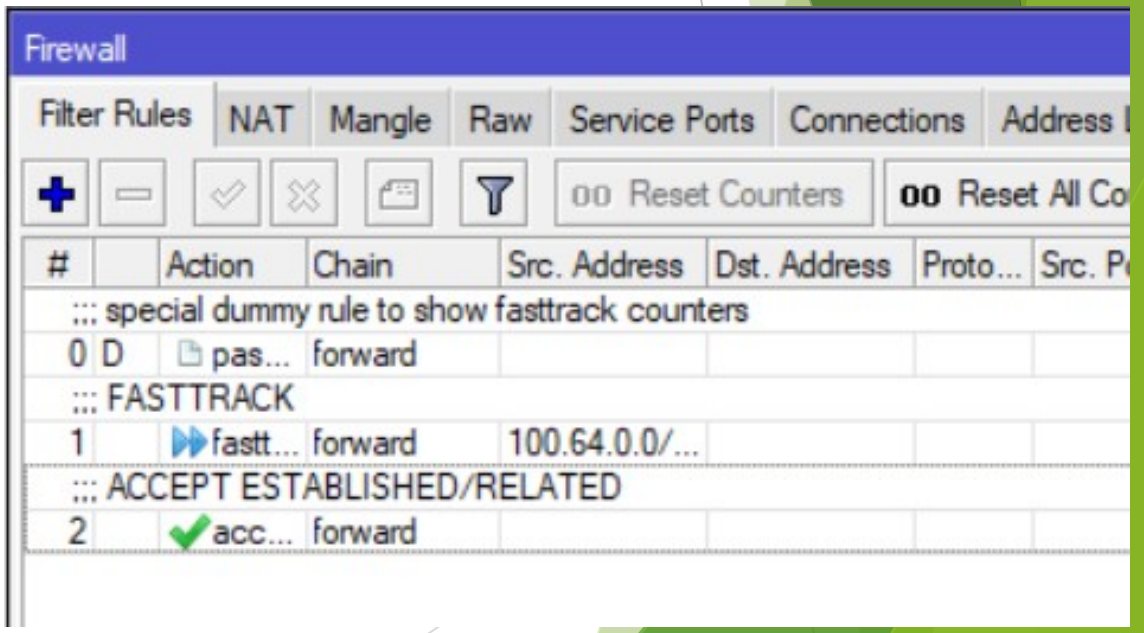


Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID	Uptime	Prefix Co...	State
peer-BORDER_ROUTER	default	10.0.0.13	65530	no	no	d...	192.168.0.1	11d 05:0...	1	established
peer-BRAS01	default	10.0.0.18	65530	no	no	d...	10.0.0.18	11d 05:0...	1	established
peer-BRAS02	default	10.0.0.22	65530	no	no	d...	10.0.0.22	11d 03:3...	1	established
peer-BRAS03	default	10.0.0.26	65530	no	no	d...	10.0.0.26	11d 05:0...	1	established
peer-BRAS04	default	10.0.0.30	65530	no	no	d...	10.0.0.30	11d 05:0...	1	established
peer-BRAS05	default	10.0.0.34	65530	no	no	d...	10.0.0.34	11d 05:0...	1	established
peer-BRAS06	default	10.0.0.38	65530	no	no	d...	10.0.0.38	11d 05:0...	1	established

CGNAT - Cenário Logico

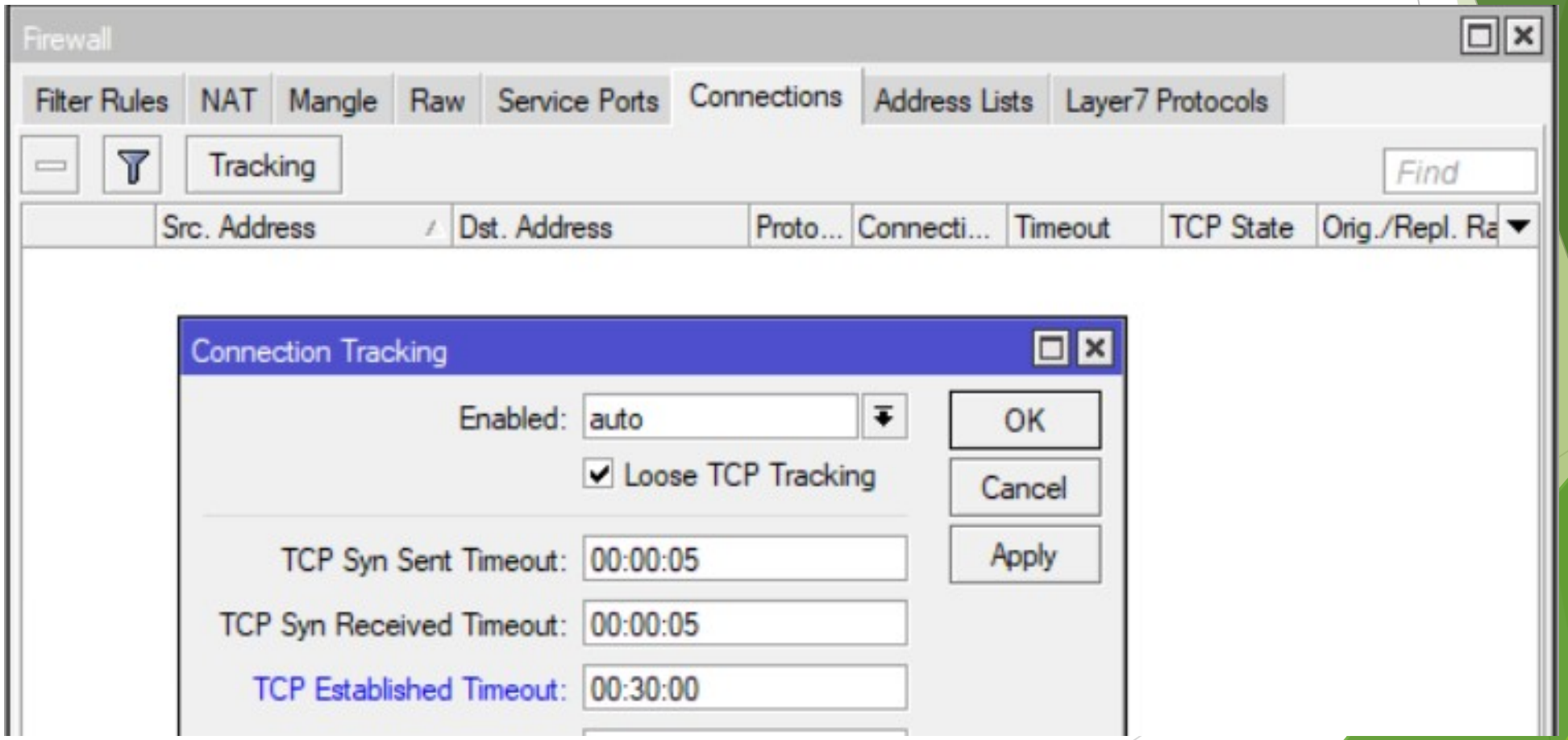
- Configurado Firewall RAW para proteger clientes e a internet, na table Filter configurado FASTTRACK para otimizar o CGNat





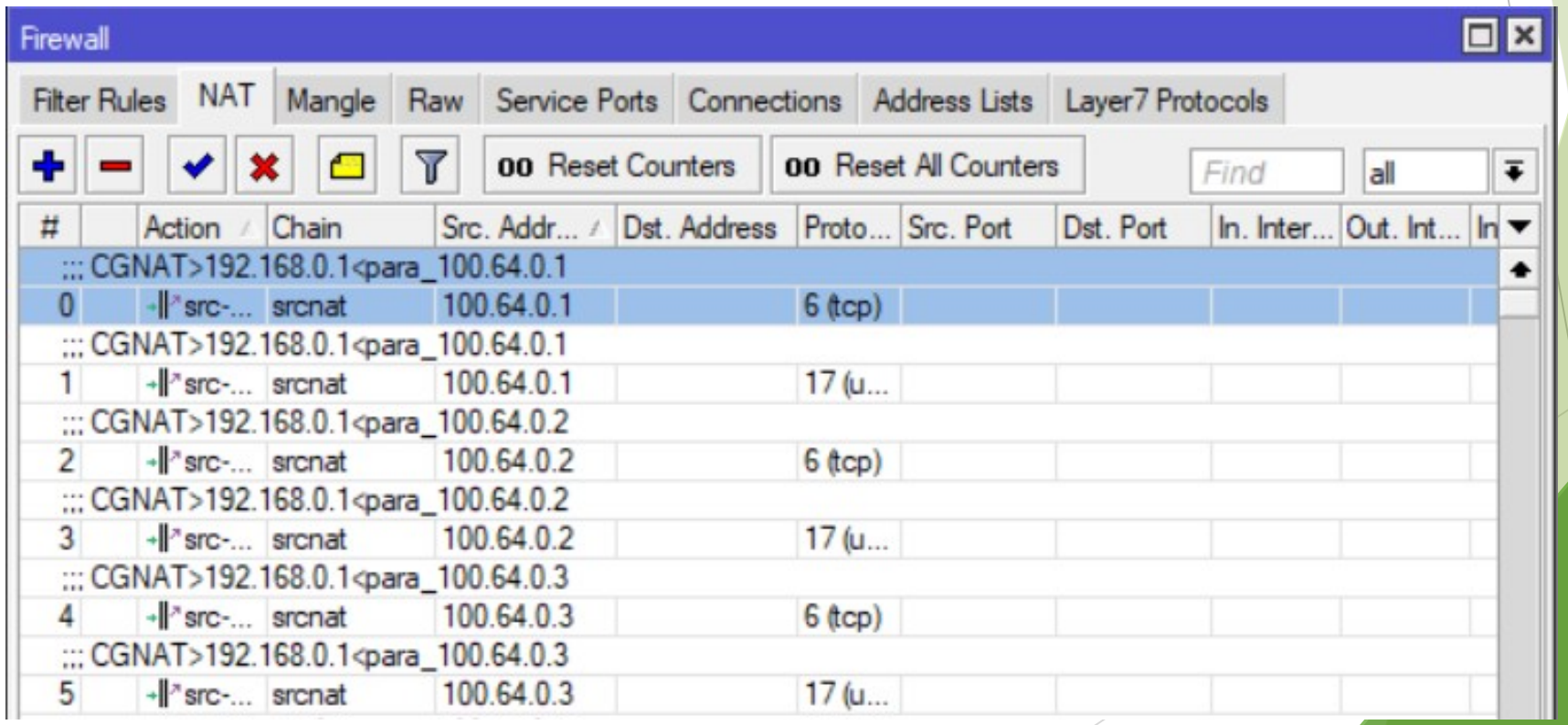
CGNAT - Cenário Logico

- Alterar o “TCP Established Timeout” para 30 minutos



CGNAT - Cenário Logico

- Ajustando a tabela NAT para o CGNat distribuindo as portas para os clientes.
- https://github.com/helysonoliveira/cgnat-mikrotik

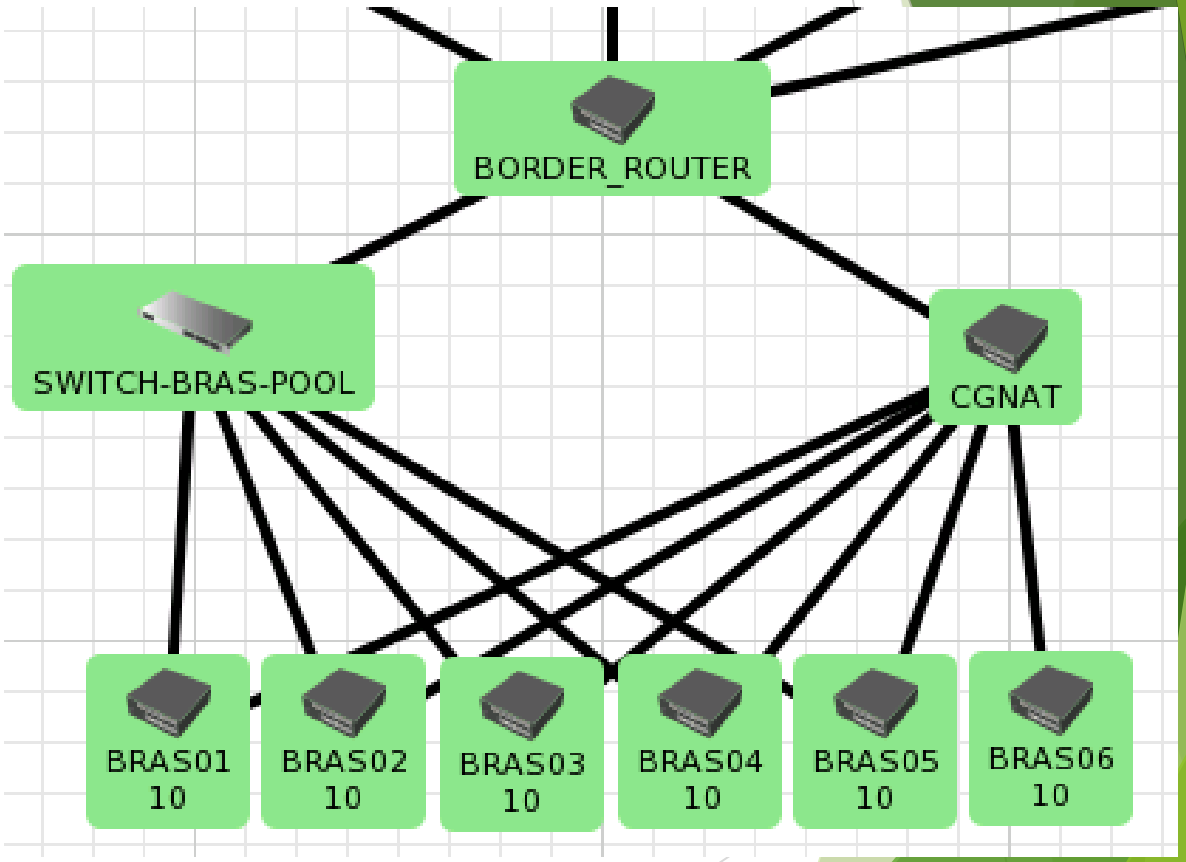


RFC 6269

RFC 6598

Tudo Pronto!

- IPv6 e CGNAT configurados.
- Simulado 60 clientes distribuídos no pool em 6 BRAS.
- Realizado testes de resiliência com sucesso.
- Firewall de proteção mantendo a rede segura.



Obrigado!

Flavio Gomes Figueira Camacho Junior

E-mail: flaviocamacho95@gmail.com

Telefone: +55 21 96978-467

Skype: flaviocamacho95_1