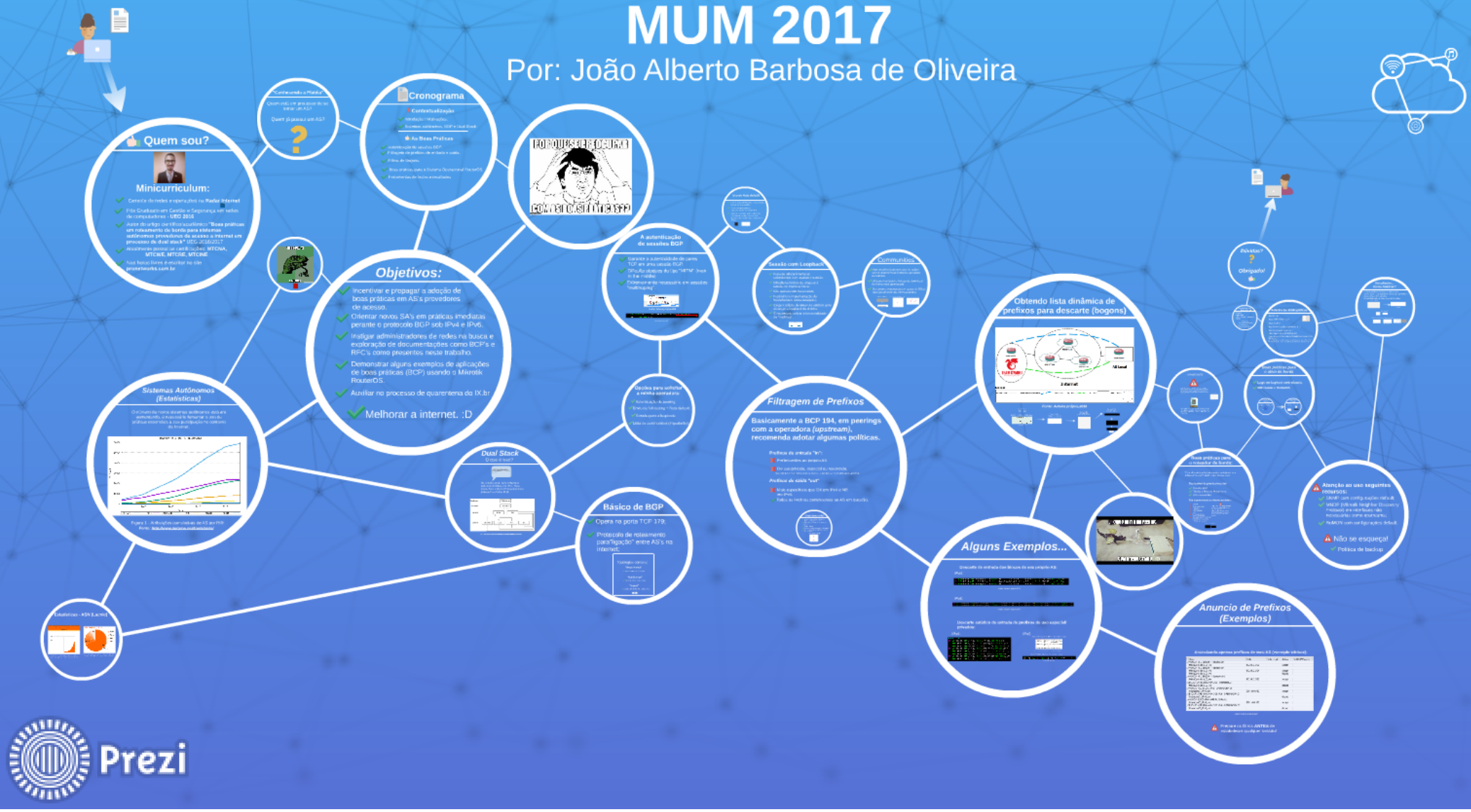
"BOAS PRÁTICAS EM ROTEAMENTO DE BORDA PARA NOVOS SISTEMAS AUTONOMOS PROVEDORES DE ACESSO À INTERNET"

MUM 2017

Por: João Alberto Barbosa de Oliveira



Prezi

MUM MIKROTIK USER MEETING

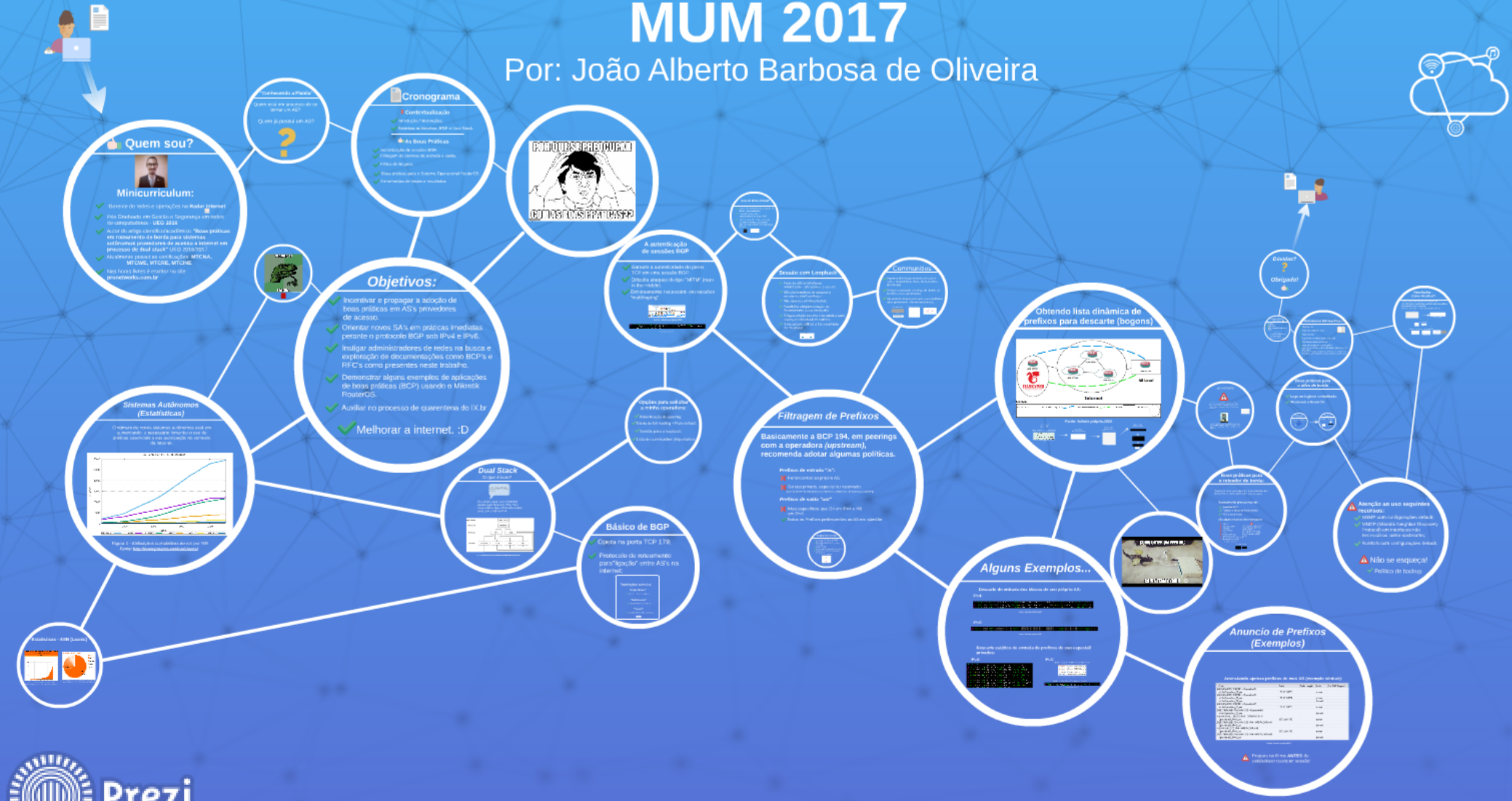
Radar INTERNET BANDA LARGA

MUM MIKROTIK USER MEETING

"BOAS PRÁTICAS EM ROTEAMENTO DE BORDA PARA NOVOS SISTEMAS AUTONOMOS PROVEDORES DE ACESSO À INTERNET"

MUM 2017

Por: João Alberto Barbosa de Oliveira



Prezi

Quem sou?

Minicurriculum:

- Gerente de redes e operações na **Radar Internet**
- Pós Graduado em Gestão e Segurança em redes de computadores - **UEG 2016**
- Autor do artigo científico/acadêmico **"Boas práticas em roteamento de borda para sistemas autônomos provedores de acesso a internet em processo de dual stack"** UEG 2016/2017
- Atualmente possui as certificações: **MTCNA, MTCWE, MTCRE, MTCINE**
- Nas horas livres é escritor no site **pronetworks.com.br**


Mapa de Cobertura
26 cidades em Goiás
Nova América
Itapaci
Rubiataba
Cirilândia
Santa Isabel
Ceres
Rialma
São Patrício
Carmo
Uruana
Uruaçu
Heitoraí
Itapuranga
São Francisco
Santa Rosa
Petrolina
Jaraguá
Radiolândia
Pirenópolis
Jaranápolis
Interlândia
Povoado do Índio
Sousânia
Caxambu
Anápolis
Radar

"Conhecendo a Platéia"

Quem está em processo de se tornar um AS?

Quem já possui um AS?

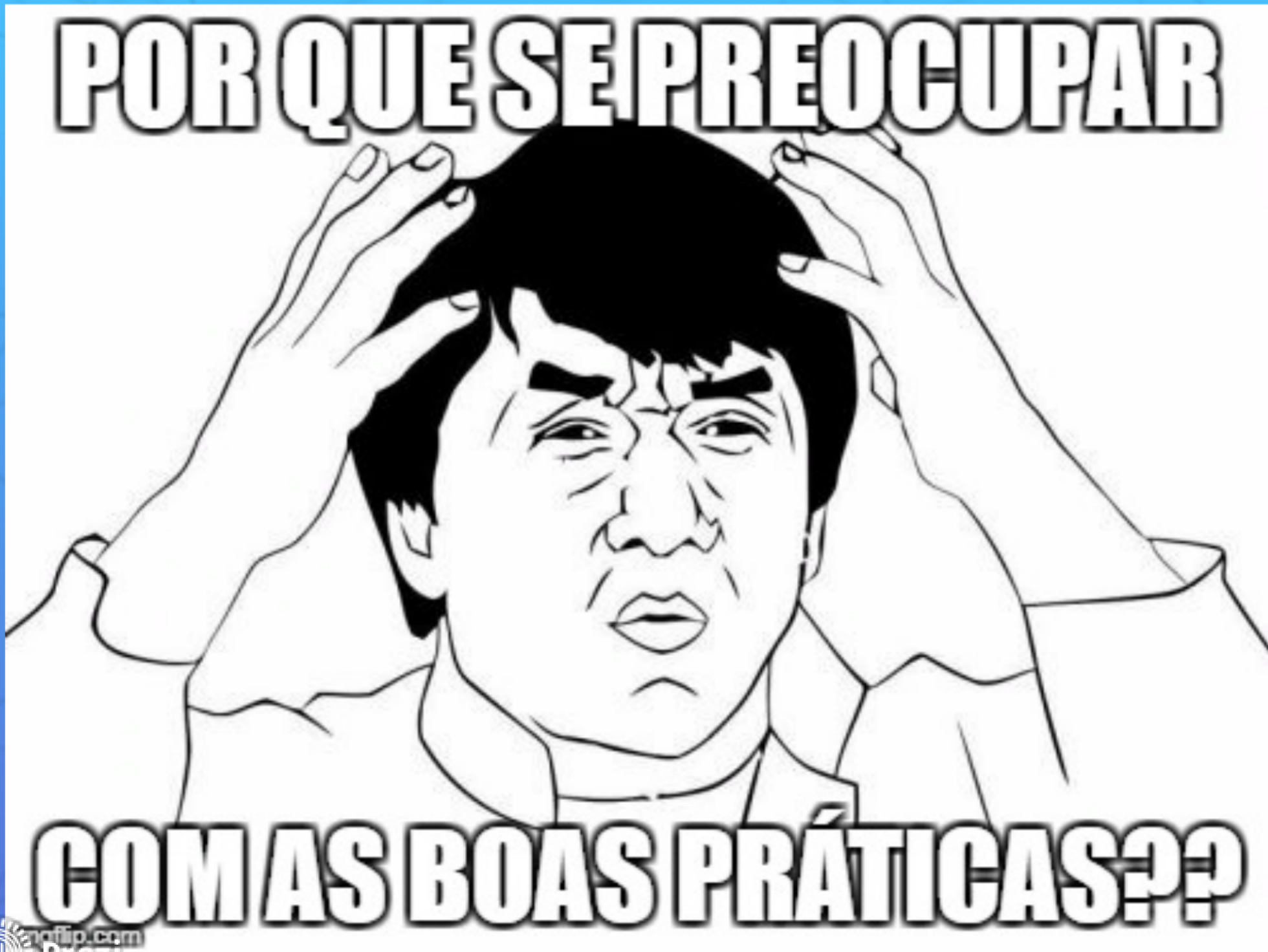
Cronograma

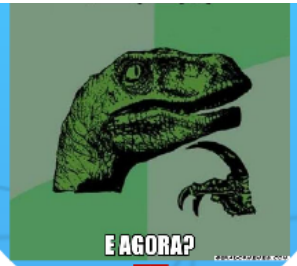
Contextualização

- Introdução / Motivações.
- Sistemas autônomos, BGP e Dual Stack.

As Boas Práticas

- Autenticação de sessões BGP.
- Filtragem de prefixos de entrada e saída.
- Filtros de Bogons.
- Boas práticas para o Sistema Operacional RouterOS.
- Ferramentas de testes e resultados

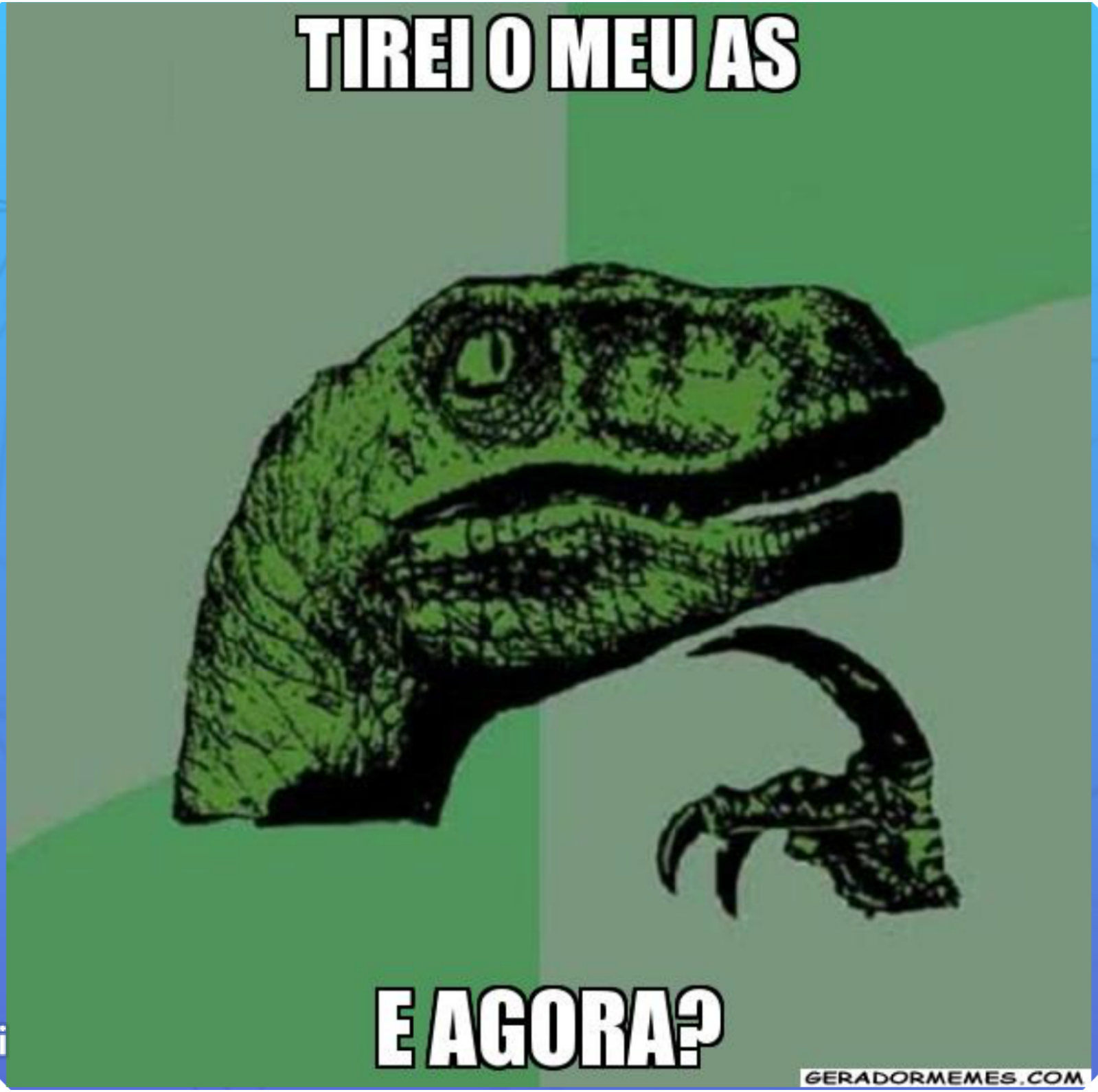

POR QUE SE PREOCUPAR
COM AS BOAS PRÁTICAS??



Objetivos:

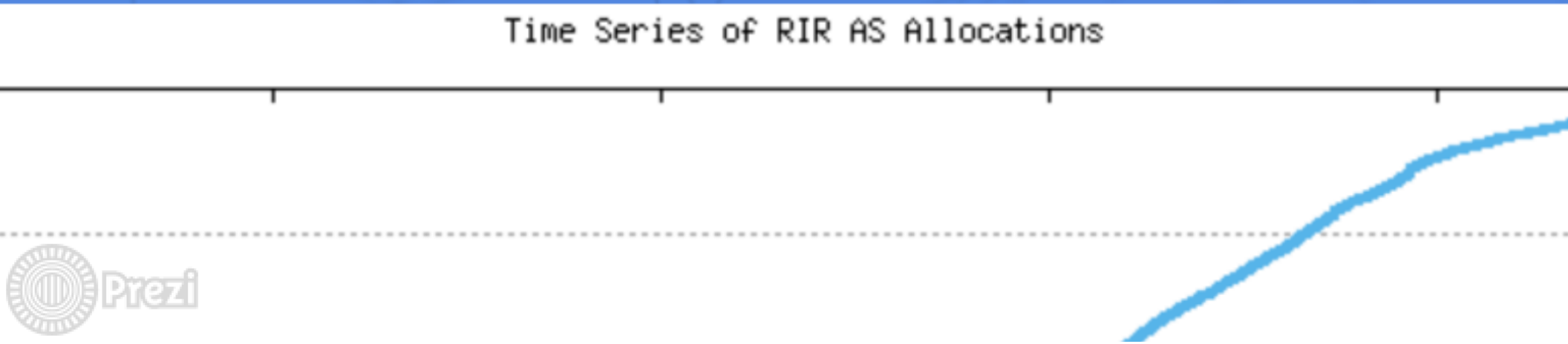
- Incentivar e propagar a adoção de boas práticas em AS's provedores de acesso.
- Orientar novos SA's em práticas imediatas perante o protocolo BGP sob IPv4 e IPv6.
- Instigar administradores de redes na busca e exploração de documentações como BCP's e RFC's como presentes neste trabalho.
- Demonstrar alguns exemplos de aplicações de boas práticas (BCP) usando o Mikrotik RouterOS.
- Auxiliar no processo de quarentena do IX.br
- Melhorar a internet. :D

Dual Stack


TIREI O MEU AS
E AGORA?
GERADORMEMES.COM

Sistemas Autônomos (Estatísticas)

O número de novos sistemas autônomos está em aumentando, é necessário fomentar o uso de práticas essenciais à sua paticipação no contexto da Internet.



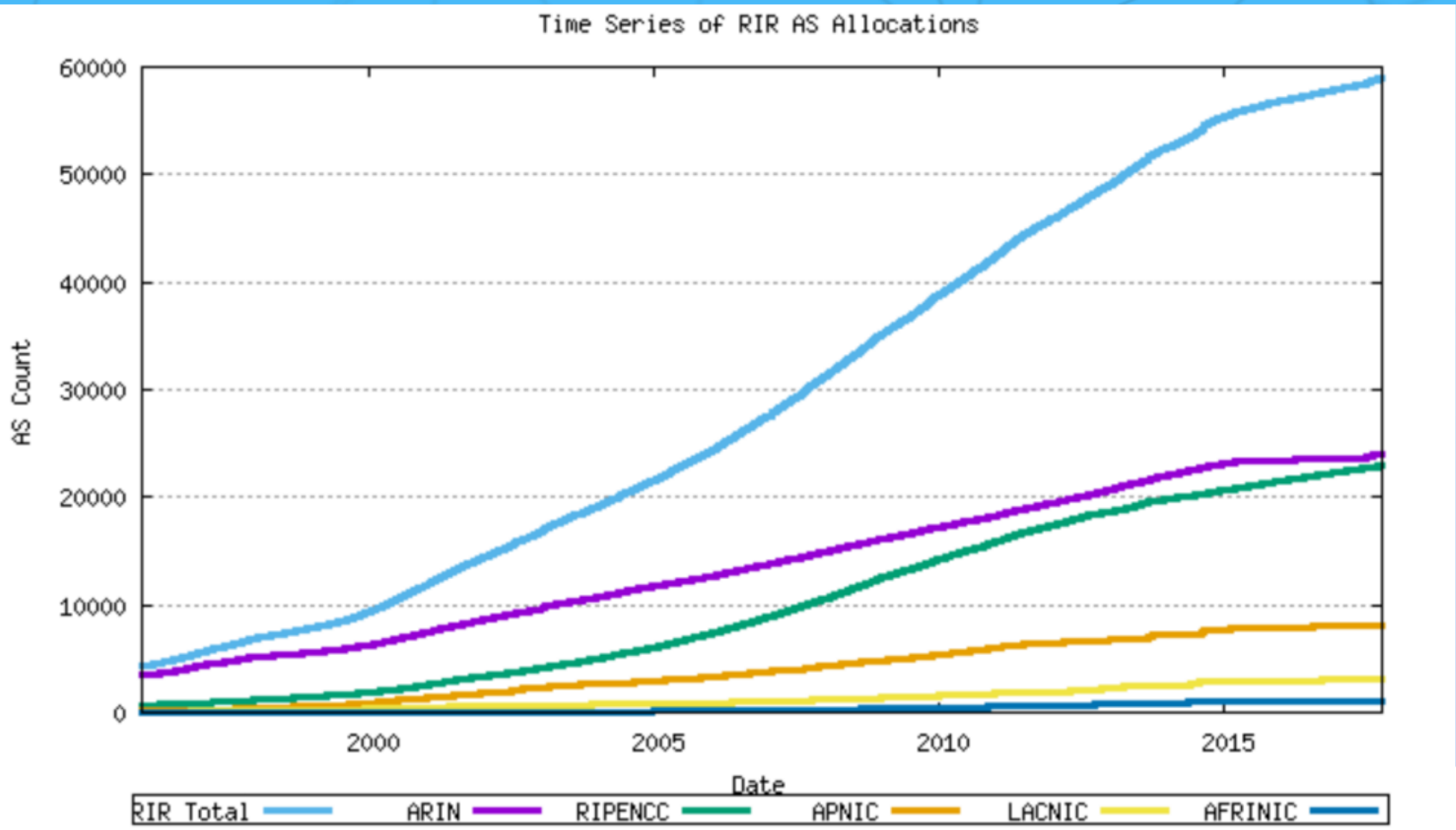


Figura 1 - Atribuições cumulativas de AS por RIR

Fonte: http://www.potaroo.net/tools/asns/

Estatísticas - ASN (Lacnic)

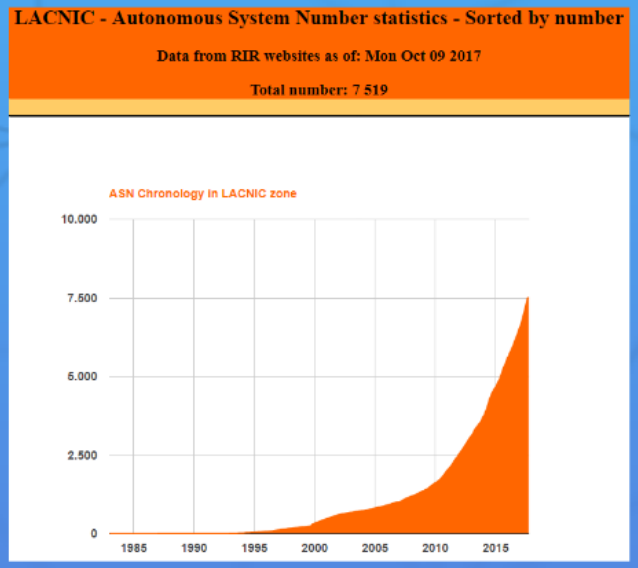


Figura 2 - Histórico de atribuições de ASN's - LACNIC

Fonte: https://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

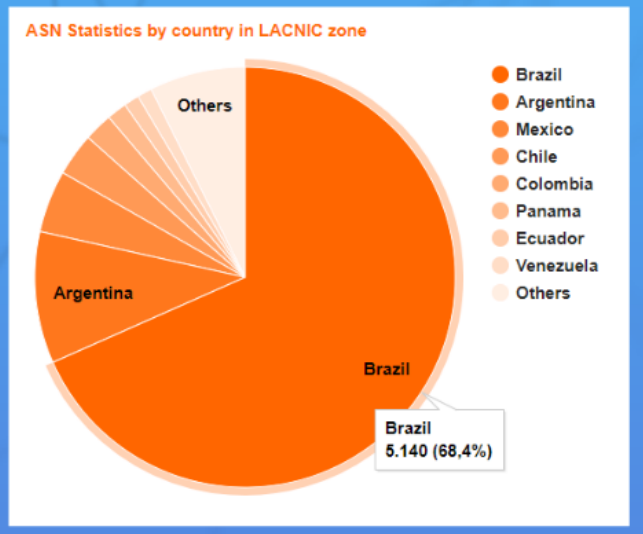


Figura 3 - Ranking de países com ASN's atribuidos (contexto LACNIC)

Fonte: https://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

LACNIC - Autonomous System Number statistics - Sorted by number

Data from RIR websites as of: Mon Oct 09 2017

Total number: 7 519

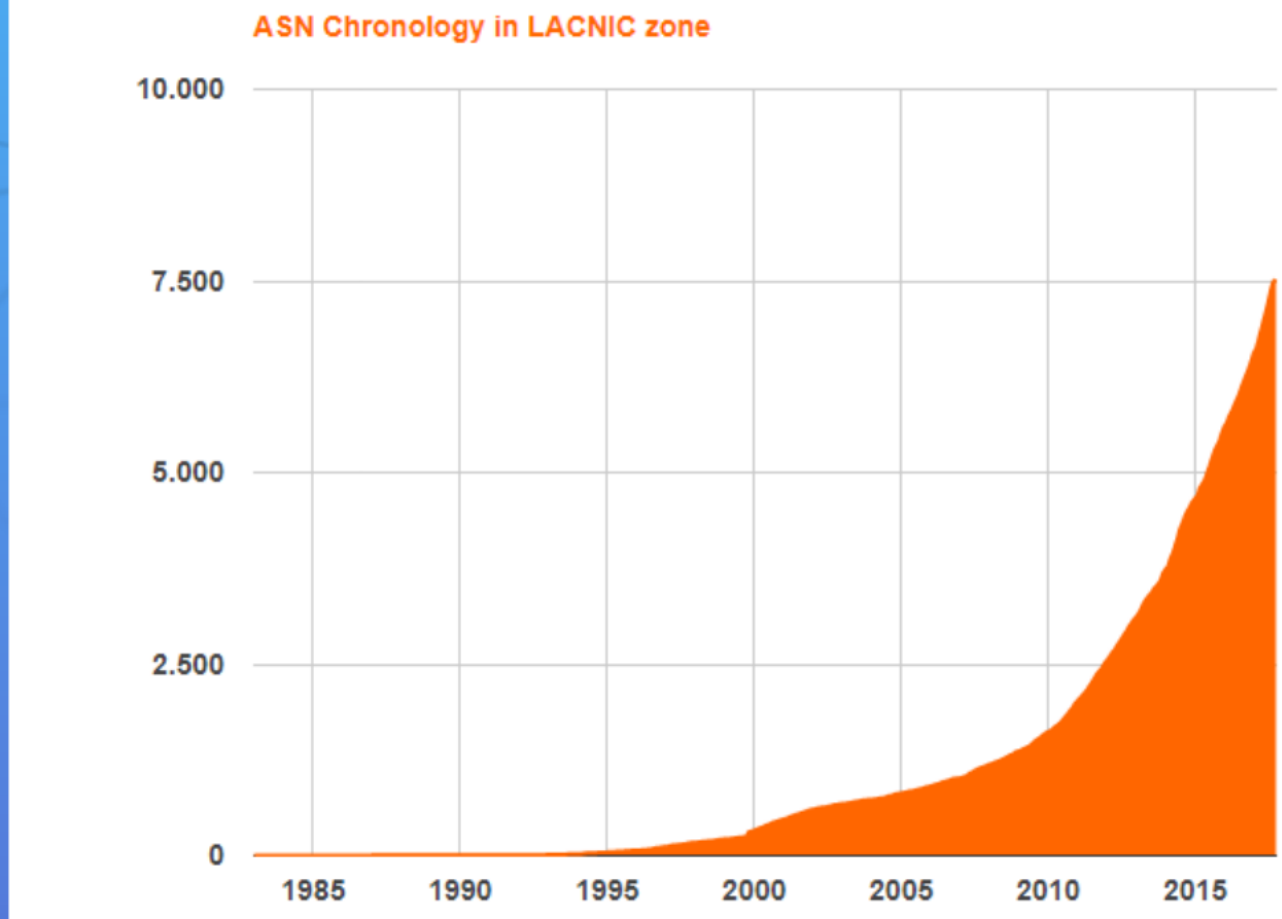


Figura 2 - Histórico de atribuições de ASN's - LACNIC

Fonte: https://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

Figura 3

Fonte

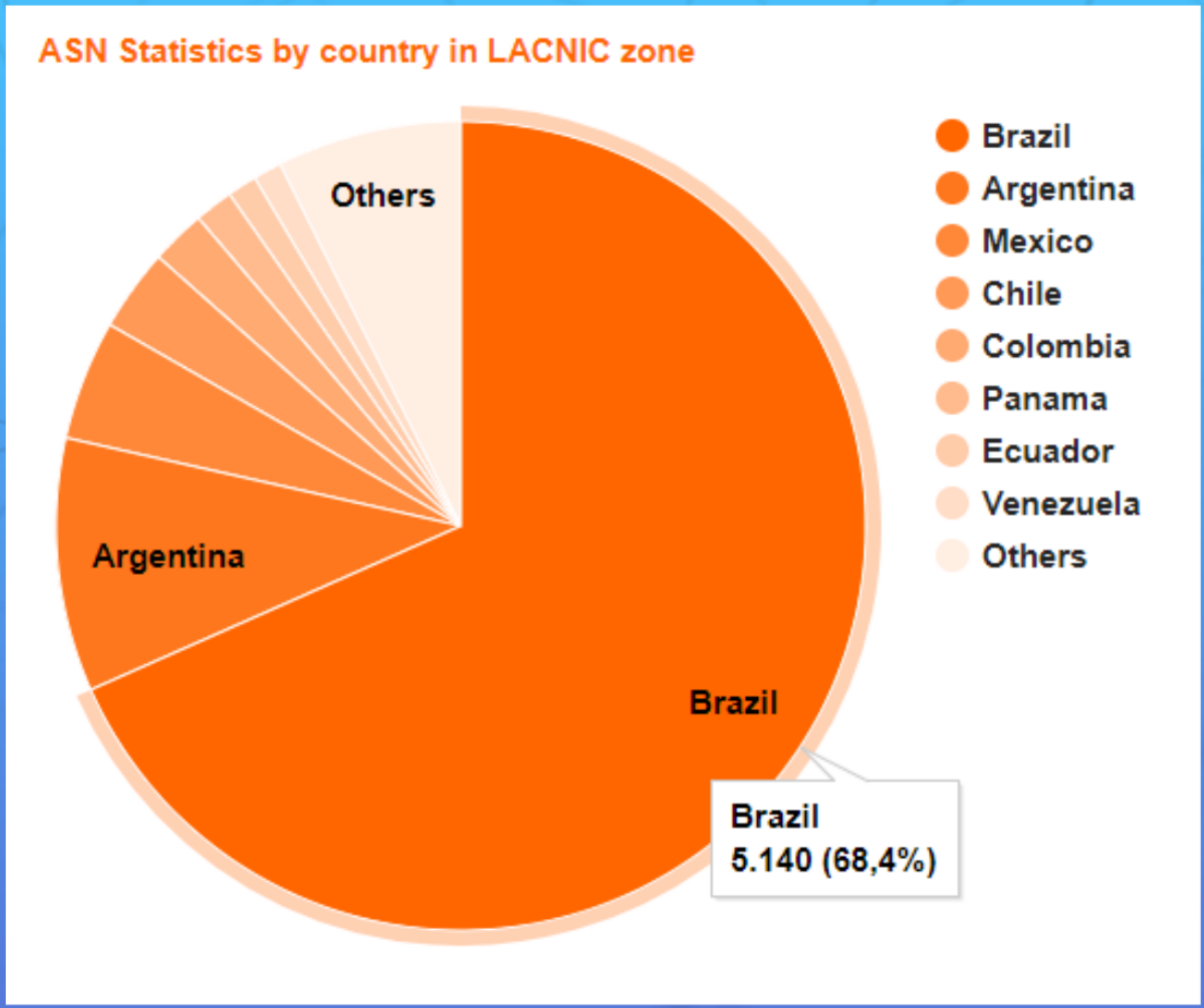


Figura 3 - Ranking de países com ASN's atribuidos (contexto LACNIC)

Fonte: https://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

Básico de BGP

- Opera na porta TCP 179;
- Protocolo de roteamento para"ligação" entre AS's na internet;

Topologias comuns:

"Single Homed"

Apenas 1 upstream (operadora)

"Multihomed"

2 ou mais upstreans (operadoras)

"Transit"

AS que provem trânsito a outros AS's

Topologias comuns:

"Single Homed"

- Apenas 1 upstream (operadora)

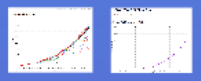
"Multihomed"

- 2 ou mais upstreans (operadoras)

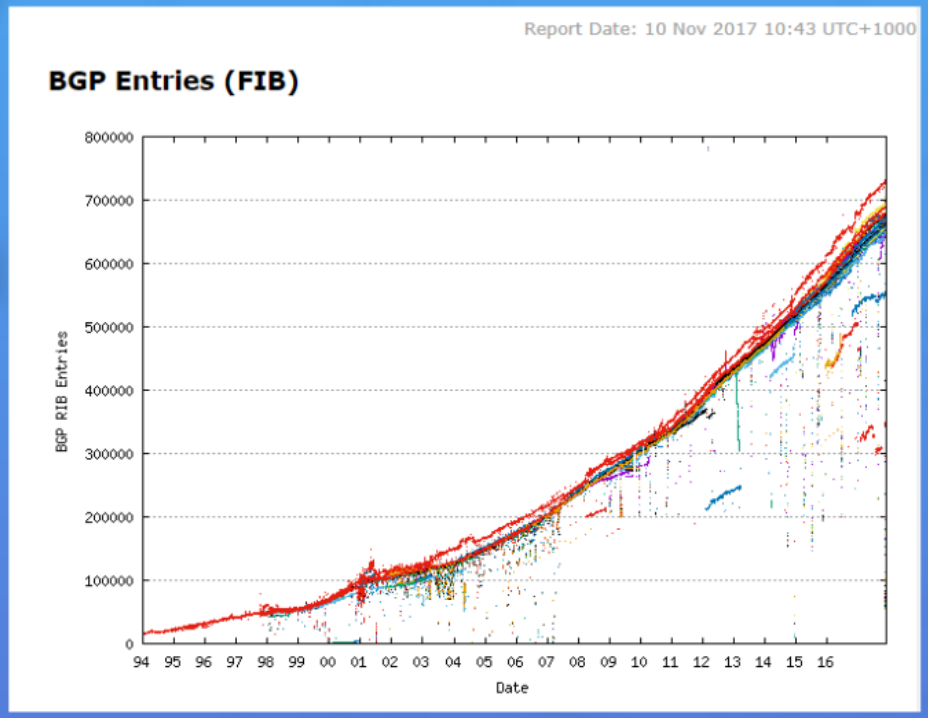
"Transit"

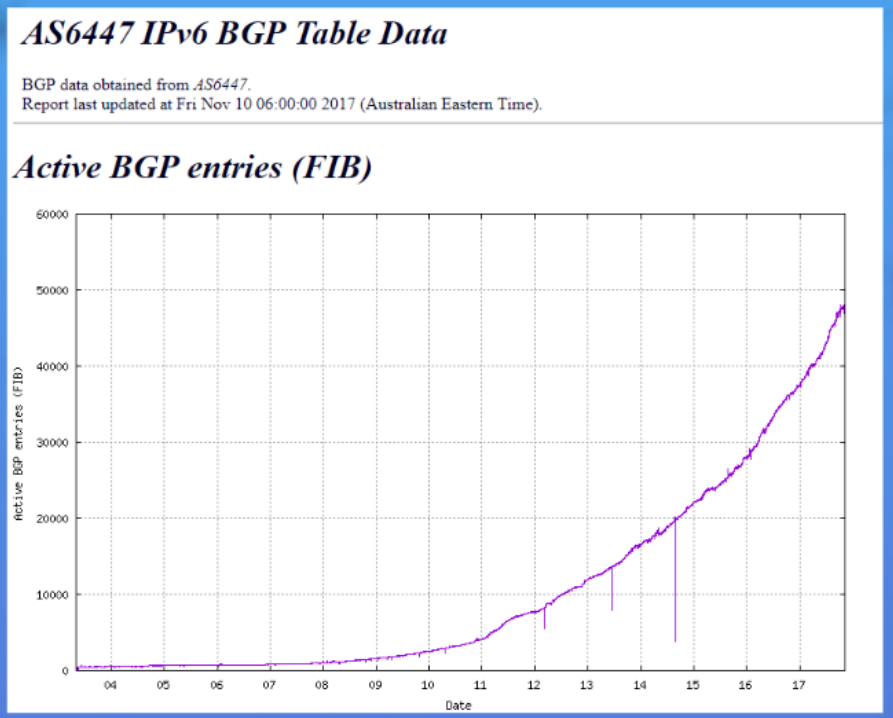
- AS que provem trânsito a outros AS's

Full Routing



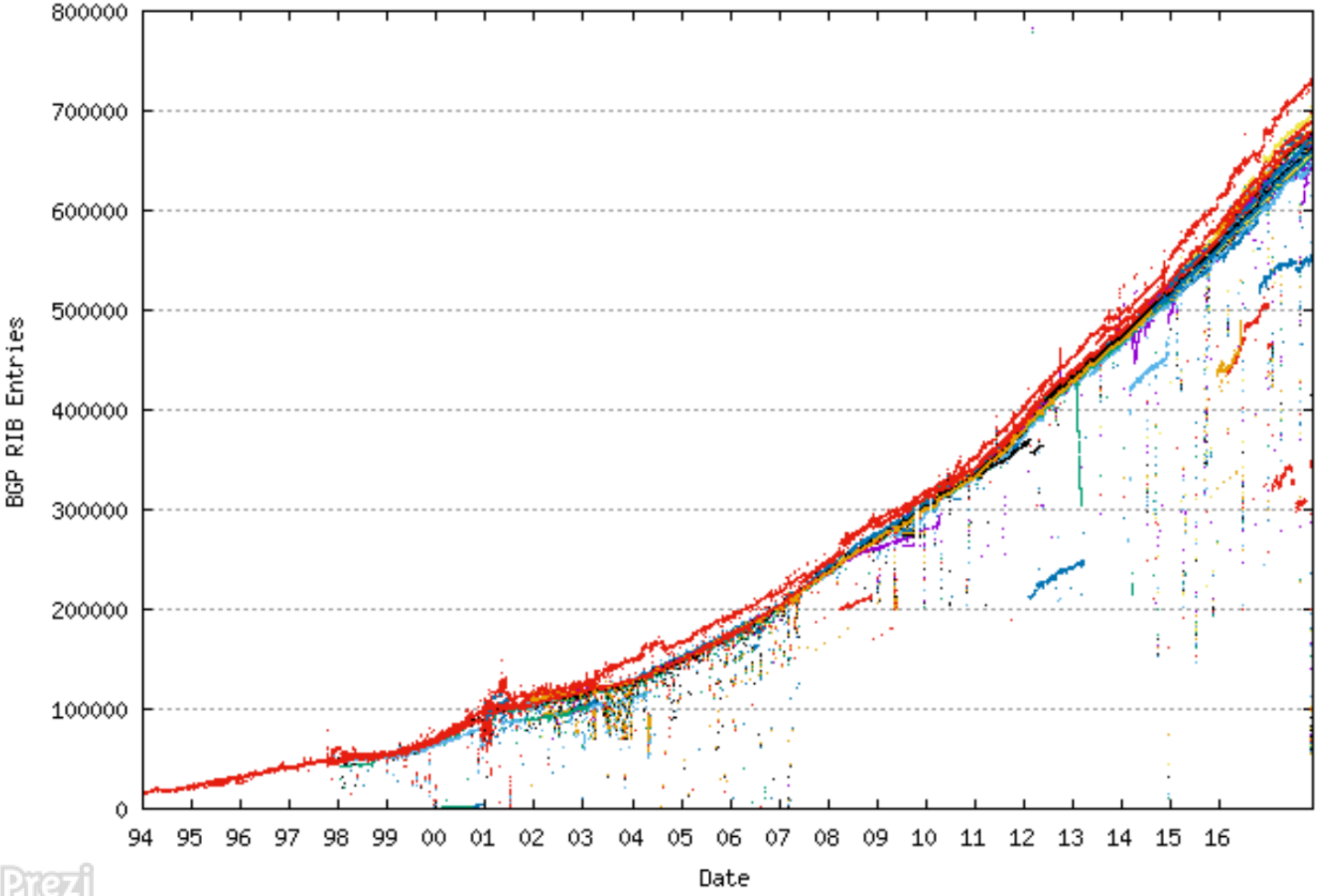
Full Routing





Report Date: 10 Nov 2017 10:43 UTC+1000

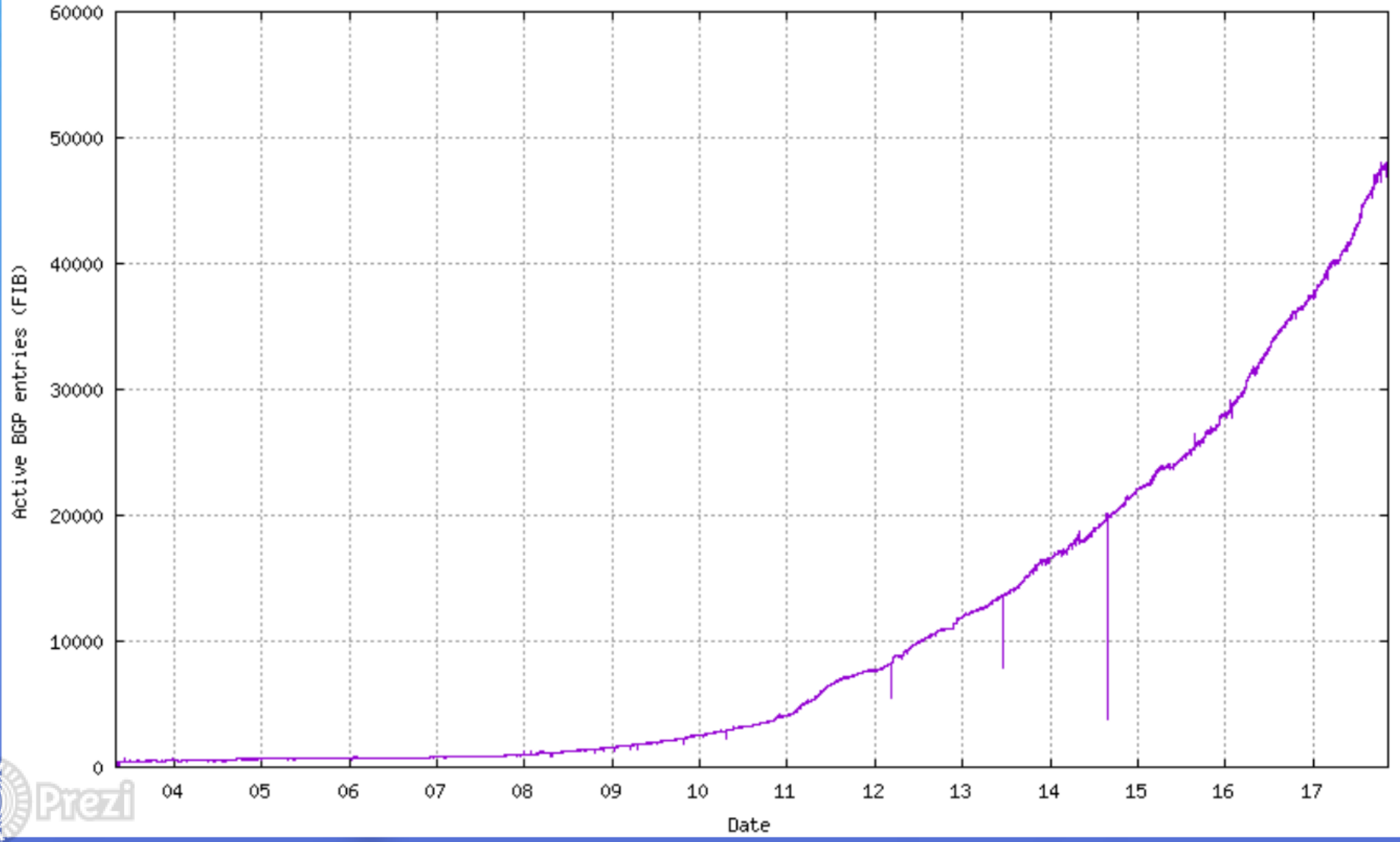
BGP Entries (FIB)



AS6447 IPv6 BGP Table Data

BGP data obtained from *AS6447*.
Report last updated at Fri Nov 10 06:00:00 2017 (Australian Eastern Time).

Active BGP entries (FIB)



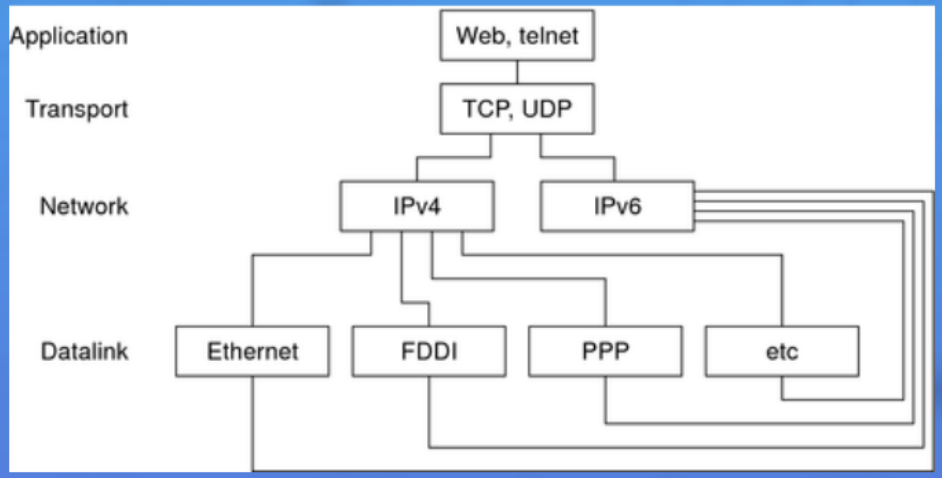
Dual Stack

O que é isso?

"Recomenda-se que todos os hosts, antes de migrarem completamente para a versão 6, implementem a pilha dupla de protocolos. Em outras palavras, uma estação deve rodar o IPv4 e o IPv6 simultaneamente até que toda a Internet passe a usar o IPv6".

Furouzan (2008, p.604).

No cenário atual, SA's existentes podem pedir bloco em IPv6. Para novos SA's o bloco IPv6 está incluso junto com o ASN e IPv4.



Fonte: https://docs.oracle.com/cd/E23823_01/html/816-4554/figures/dual.png

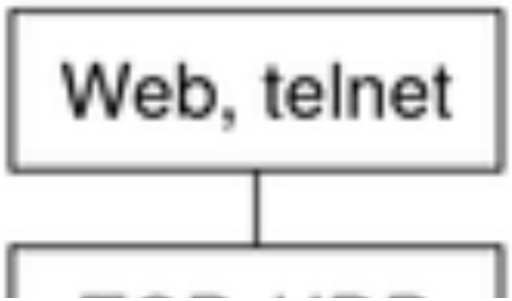
“Recomenda-se que todos os hosts, antes de migrarem completamente para a versão 6, implementem a pilha dupla de protocolos. Em outras palavras, uma estação deve rodar o IPv4 e o IPv6 simultaneamente até que toda a Internet passe a usar o IPv6”.

Furouzan (2008, p.604).

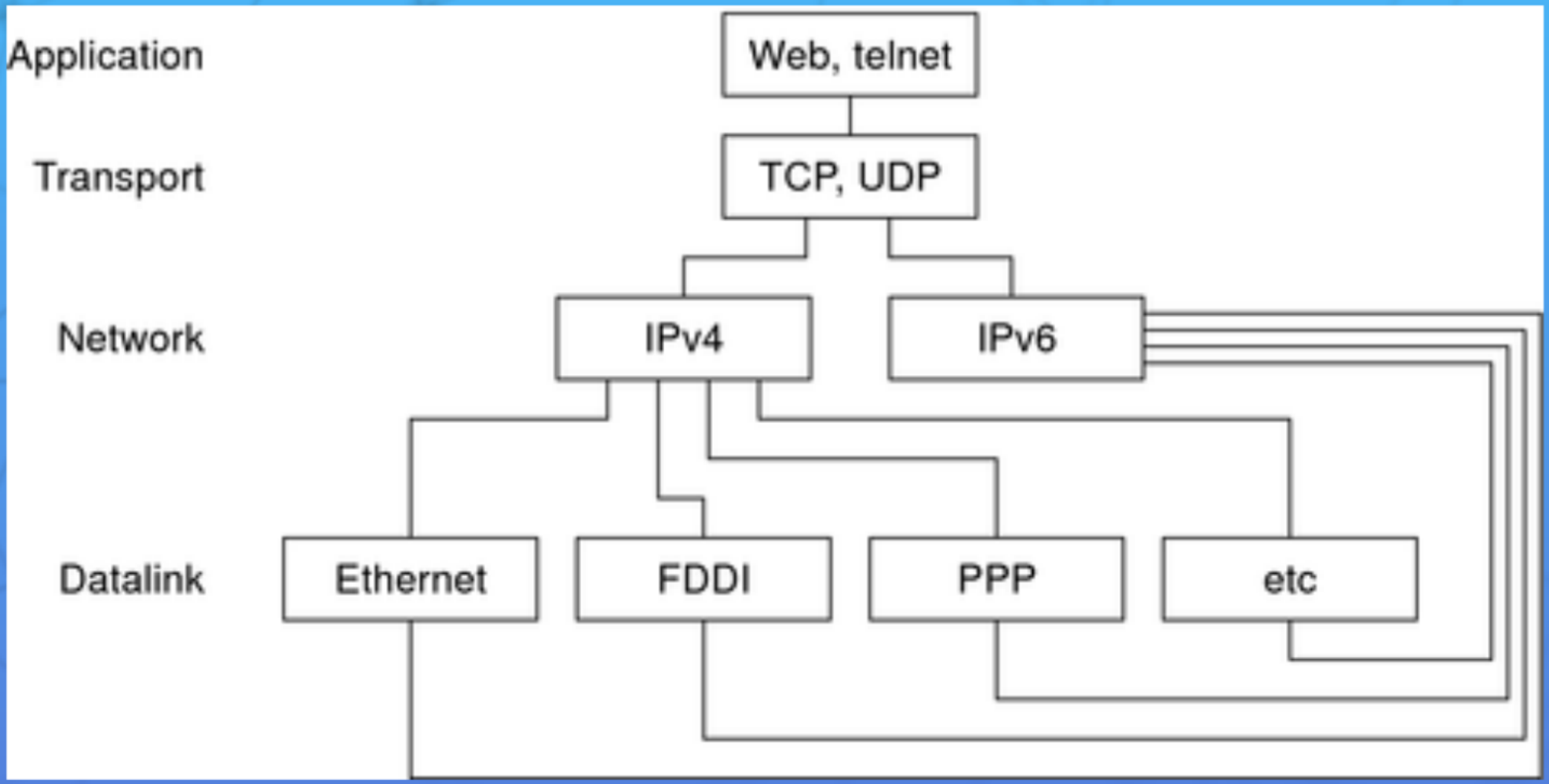
toda a Internet passe a usar o IPv6".

Furouzan (2008, p.604).

No cenário atual, SA's existentes podem pedir bloco em IPv6. Para novos SA's o bloco IPv6 está incluso junto com o ASN e IPv4.



junto com o ASN e IPv4.



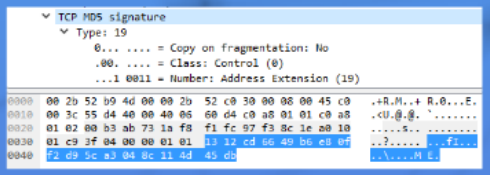
Fonte: https://docs.oracle.com/cd/E23823_01/html/816-4554/figures/dual.png

Opções para solicitar a minha operadora:

- Autenticação do peering;
- Envio de full routing + Rota default;
- Sessão para a loopback;
- Lista de communities (importante);

A autenticação de sessões BGP

- Garante a autenticidade de pares TCP em uma sessão BGP.
- Dificulta ataques do tipo "MITM" (man in the middle)
- Extremamente necessário em sessões "multihoping".

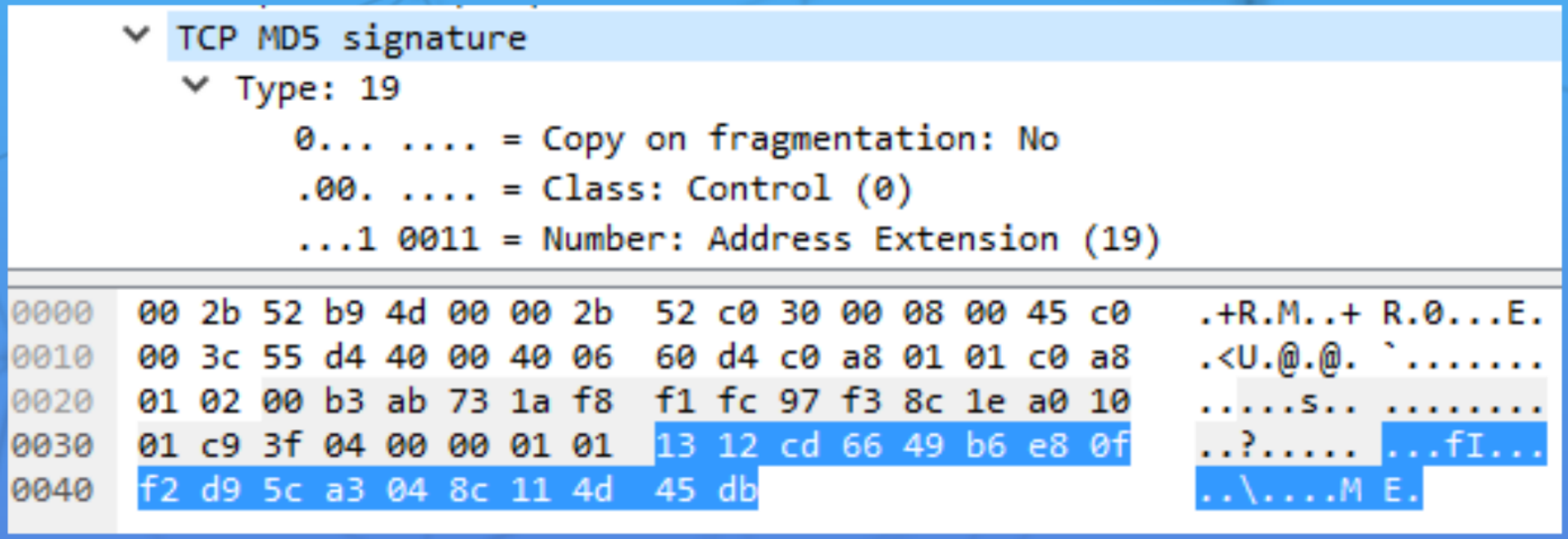


Fonte: Autoria própria,2016

```
add address-families=ipv6 in-filter=Operadora01_IPv6_in name=Operadora01_IPv6 out-filter=\
    Operadora02_IPv6_out remote-address=2001:db8::f0ca remote-as=28329 tcp-md5-key=M1kr0tik-MUM@2017 \
    ttl=default update-source=sfp-sfpplus3
```

Fonte: Autoria própria,2017

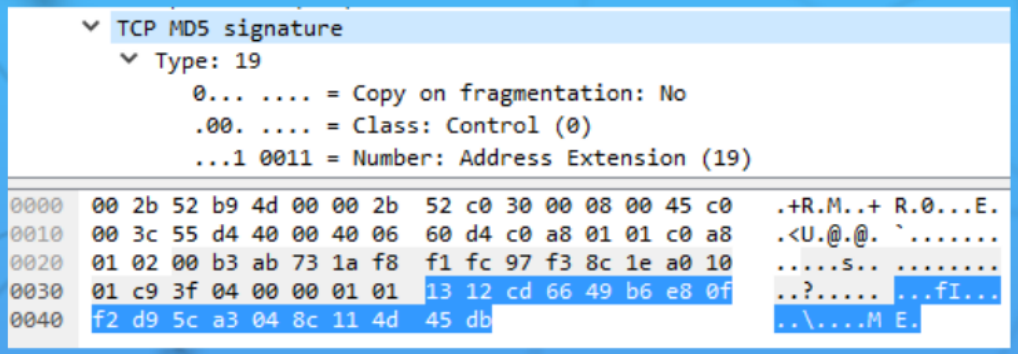
oping".



Fonte: Autoria própria,2016

in-filter=Operadora01_IPv6_in name=Operadora01_IPv6
remote-address=2001:db8::f0ca remote-as=28329 tcp-md5-

multihoping".



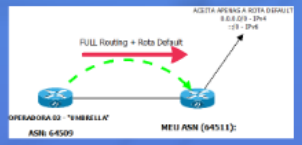
Fonte: Autoria própria,2016

```
add address-families=ipv6 in-filter=Operadora01_IPv6_in name=Operadora01_IPv6 out-filter=\
    Operadora02_IPv6_out remote-address=2001:db8::f0ca remote-as=28329 tcp-md5-key=M1krOtik-MUM@2017 \
    ttl=default update-source=sfp-sfpplus3
```

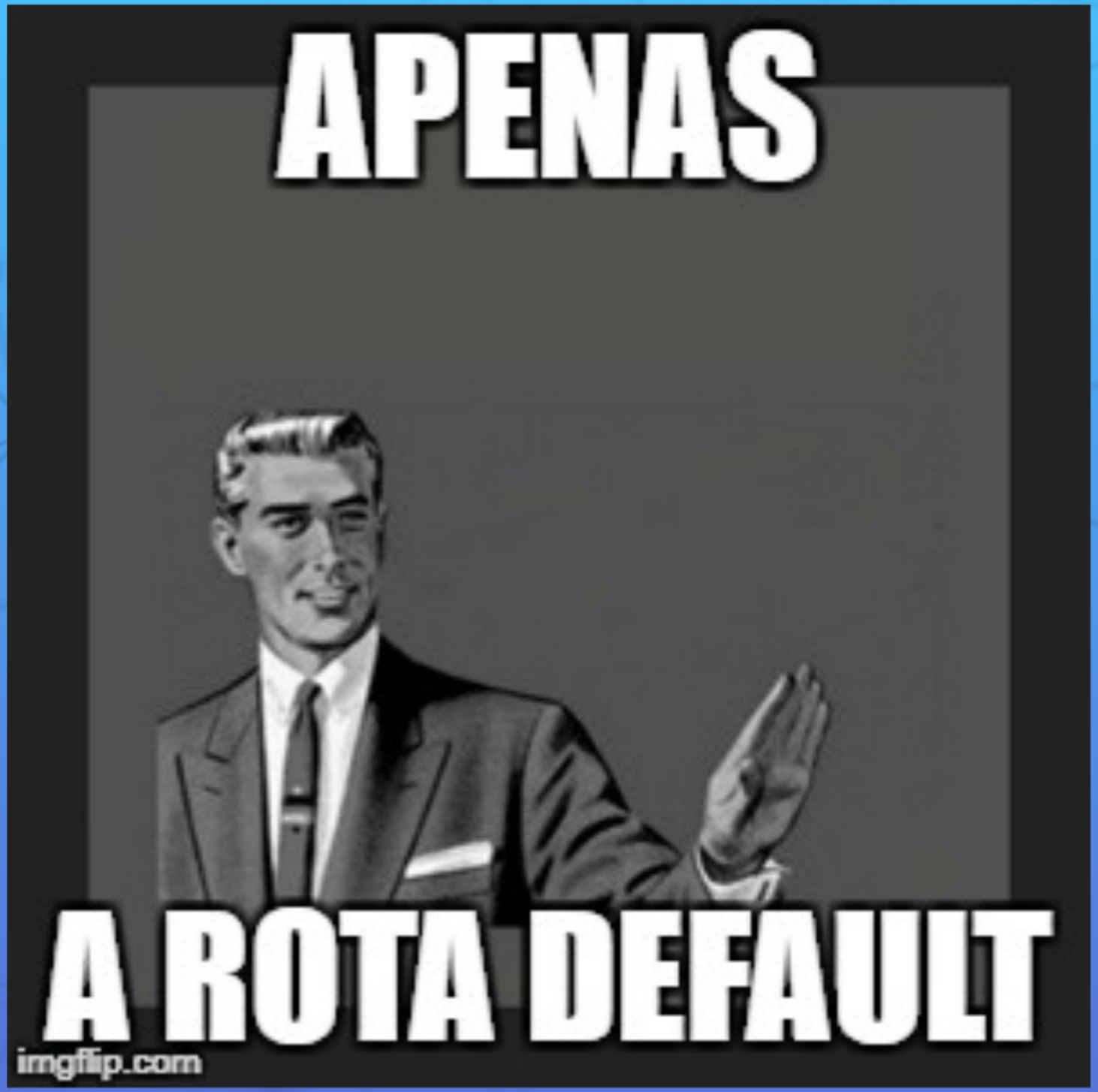
Fonte: Autoria própria,2017

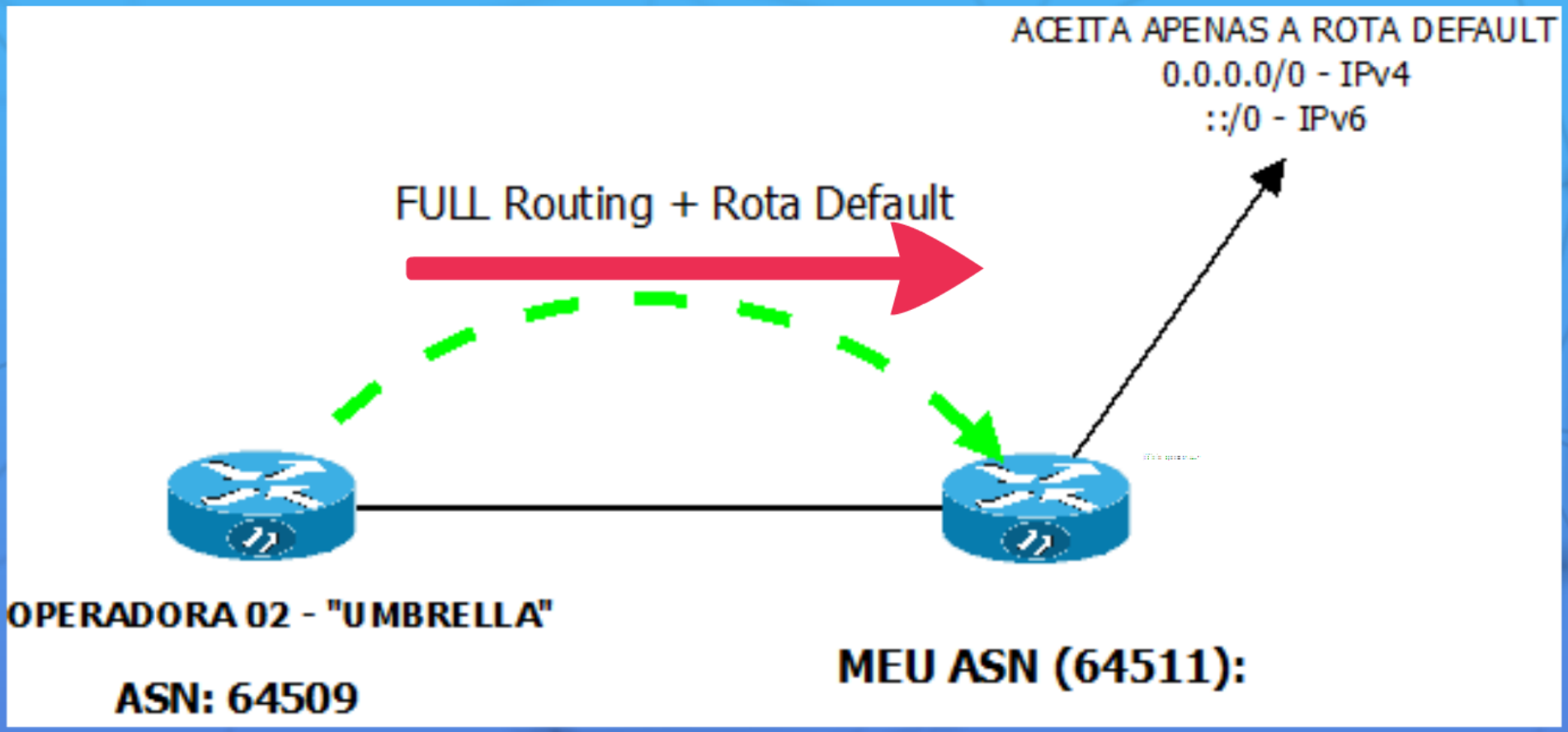
Uso de Rota default

- A BCP 194 também indica o uso da rota default, **se necessário;**
- Vantajoso para poupar processamento da tabela "full";
- Pode-se descartar tudo e criar uma rota default estatica, ou receber apenas a rota default (se a operadora enviar).



Fonte: Autoria propria, 2017





Fonte: Autoria propria, 2017

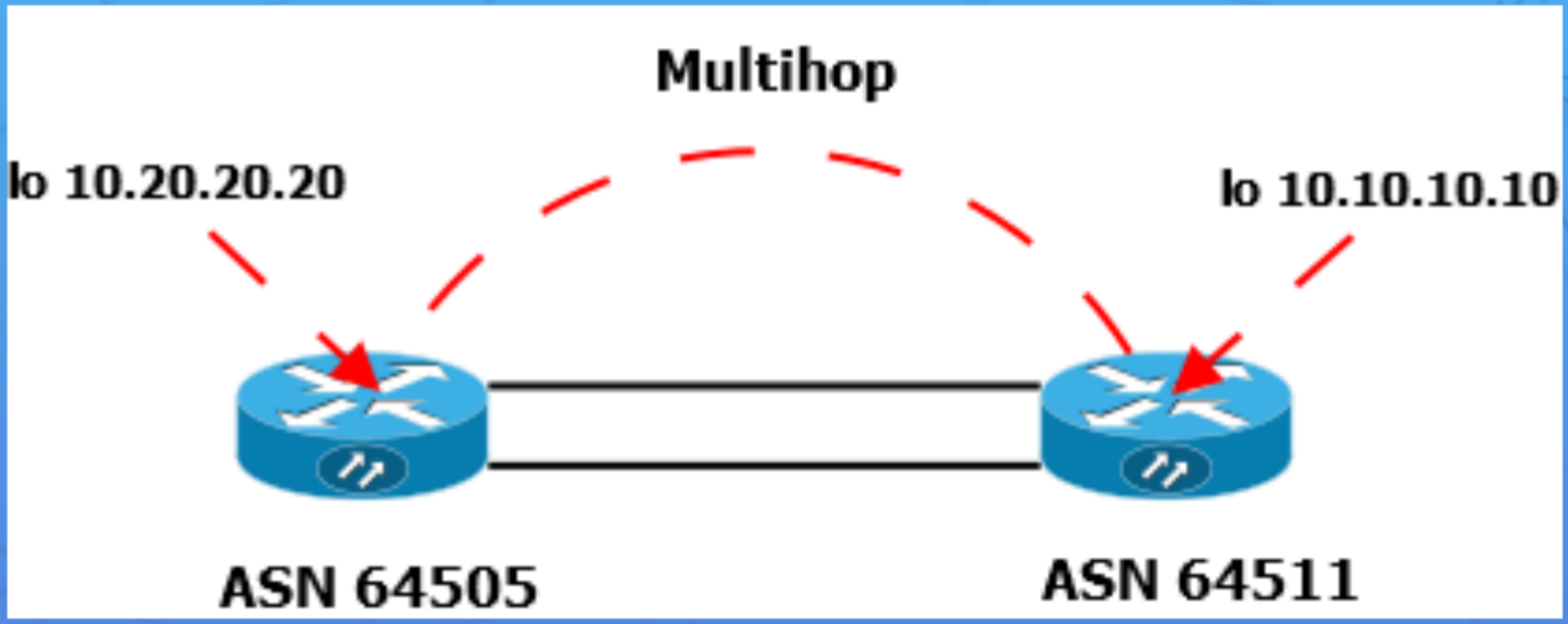
```
/routing filter
add action=discard chain=Operadoral_in prefix=!0.0.0.0/0
add action=discard chain=Operadoral_IPv6_in prefix=!::/0
```

Sessão com Loopback

- Pode-se utilizar interfaces redundantes com apenas 1 sessão;
- Dificulta tentativas de ataques à sessão na interface fisica ;
- Não aparece em traceroutes;
- Possibilita a implementação de RouteServers (caso desejado).
- Exige a adição de uma rota estática para alcançar a loopback do vizinho;
- É necessario utilizar a funcionalidade de "multihop".

Fonte: Autoria própria, 2017

- Pode-se utilizar interfaces redundantes com apenas 1 sessão;
- Dificulta tentativas de ataques à sessão na interface fisica ;
- Não aparece em traceroutes;
- Possibilita a implementação de RouteServers (caso desejado).
- Exige a adição de uma rota estática para alcançar a loopback do vizinho;
- É necessario utilizar a funcionalidade de "multihop".



Fonte: Autoria própria, 2017

Communities

- Impresncidível para tomadas de ações sem a dependência direta da operadora de trânsito;
- Util para manipular o trafego de download de forma mais aprimorada;
- De extrema importancia em casos de DDoS (que geralmente são internacionais);

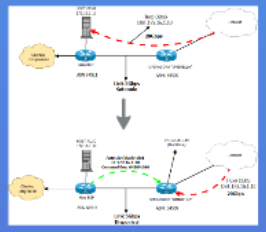
lista (alguns exemplos)

Level3

28329:666	BLACKHOLE

G8

Exemplo básico de uso em ataque DDoS



lista (alguns exemplos)

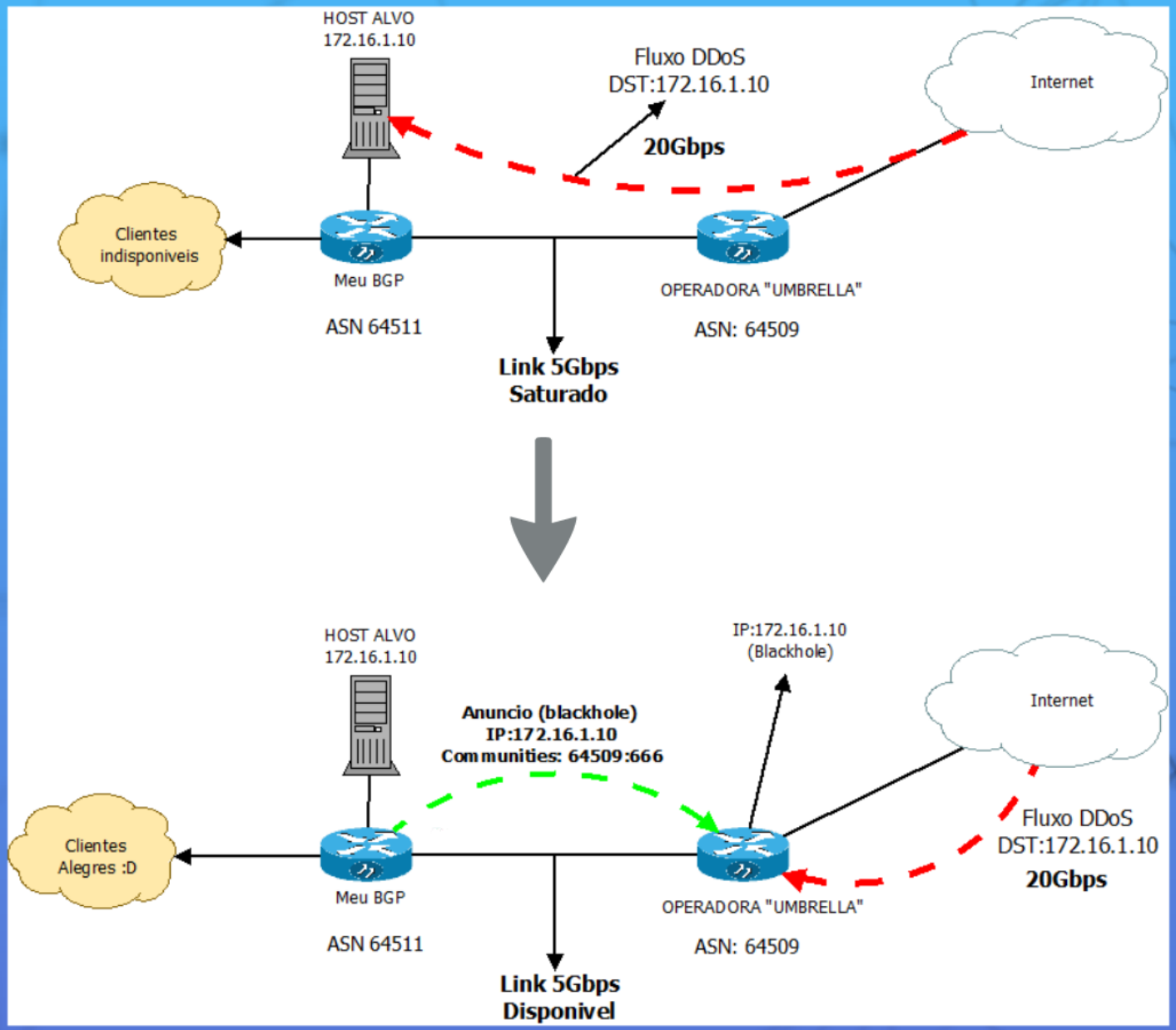
Controlling Route Propagation		
Community	Action	Region Enabled
3549:600	Deny inter-continental export of tagged prefix [iBGP].	EU/SA
3549:601	Deny inter-cluster export of tagged prefix [iBGP].	SA
3549:602	Deny inter-country export of tagged prefix [iBGP].	SA
3549:603	Deny inter-metro export of tagged prefix [iBGP].	TBD
3549:604	Deny inter-Hub export of tagged prefix [iBGP].	TBD
3549:605	Deny inter-router export of tagged prefix [iBGP].	TBD
3549:666	Deny inter-as export of tagged prefix (deny to peers, send to customers) [eBGP].	NA/SA/EU/AS
3549:695	Deny in country peers but export globally	SA

Level3

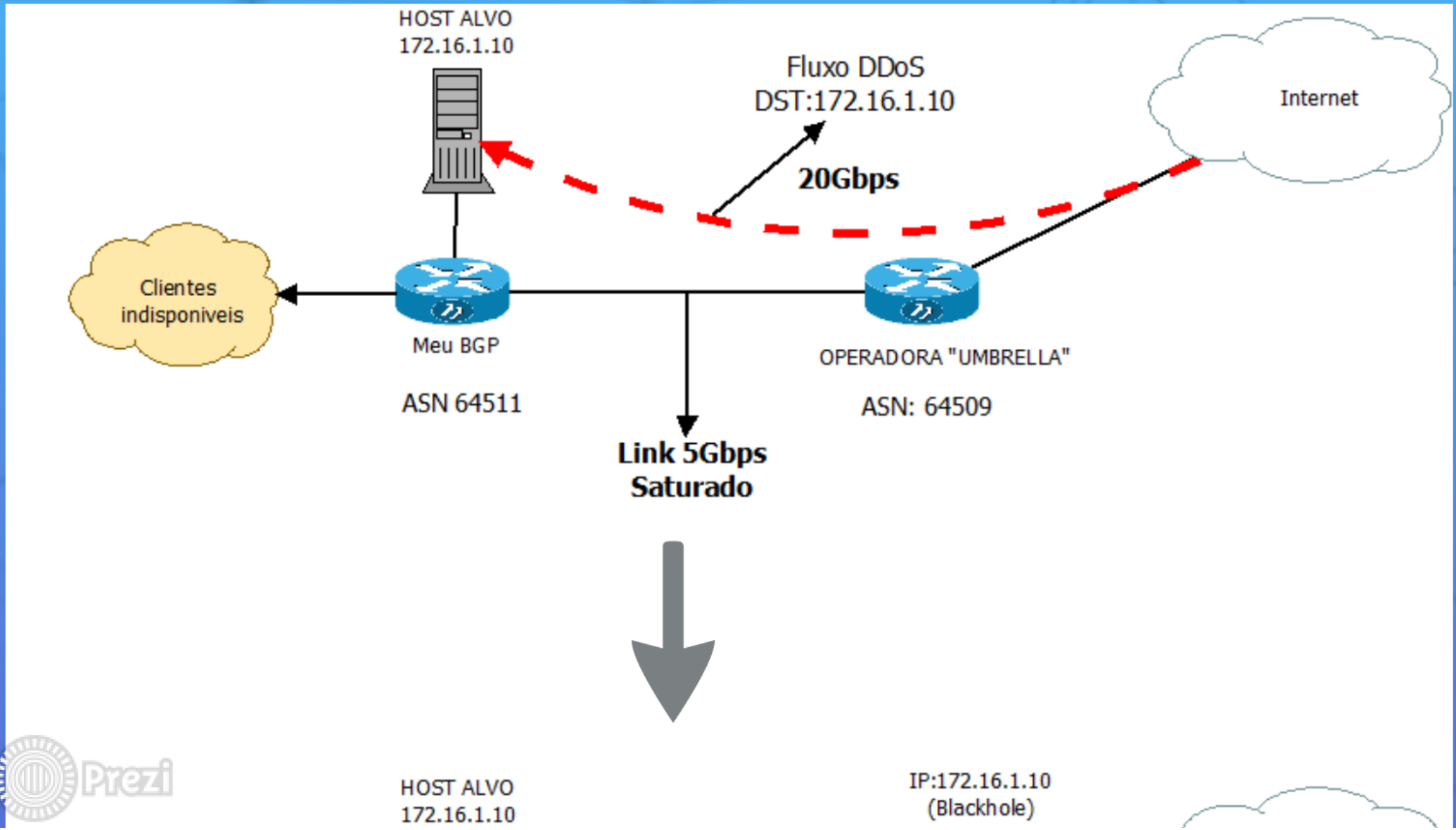
28329:666	BLACKHOLE

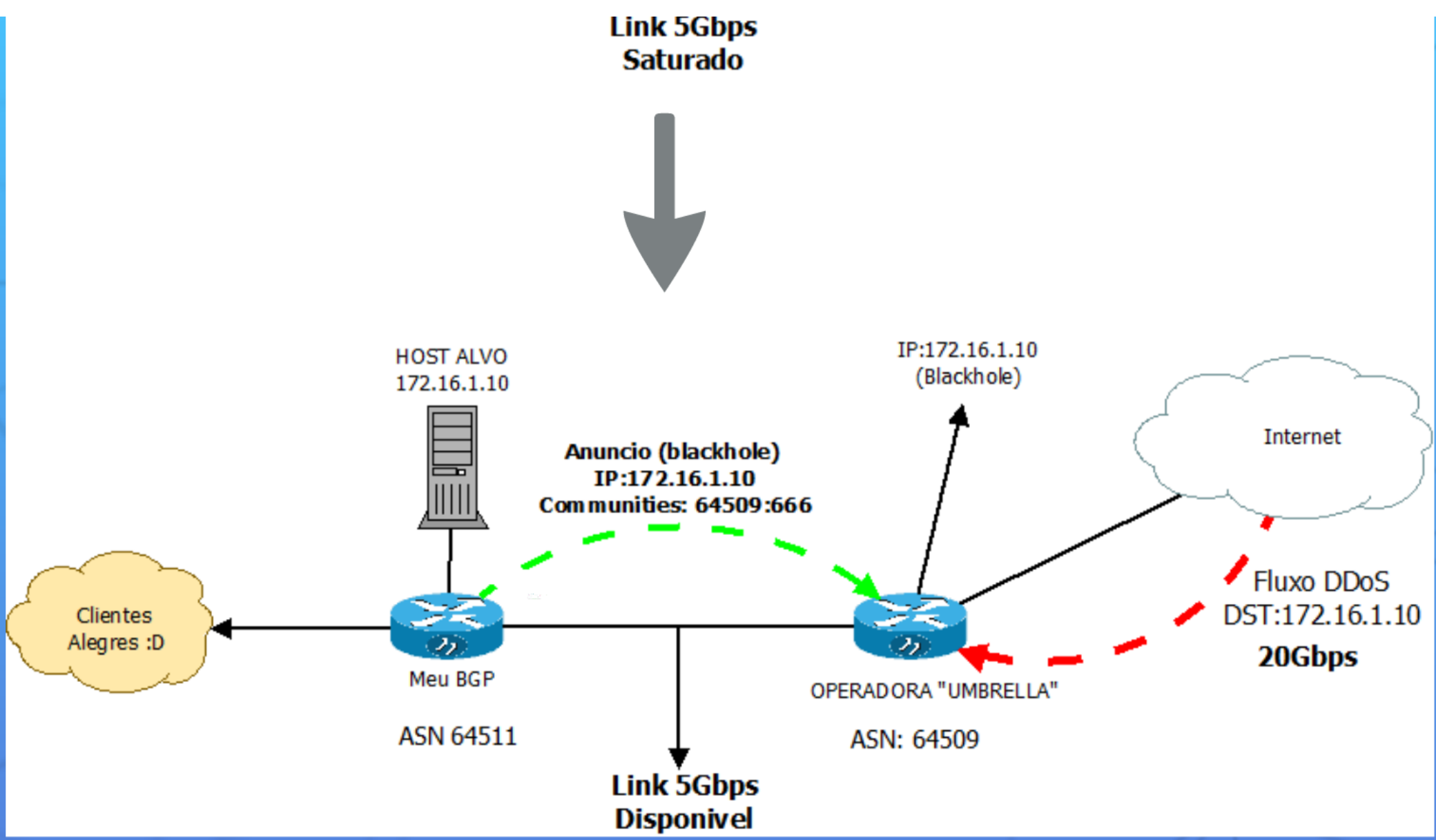
G8

Exemplo básico de uso em ataque DDoS



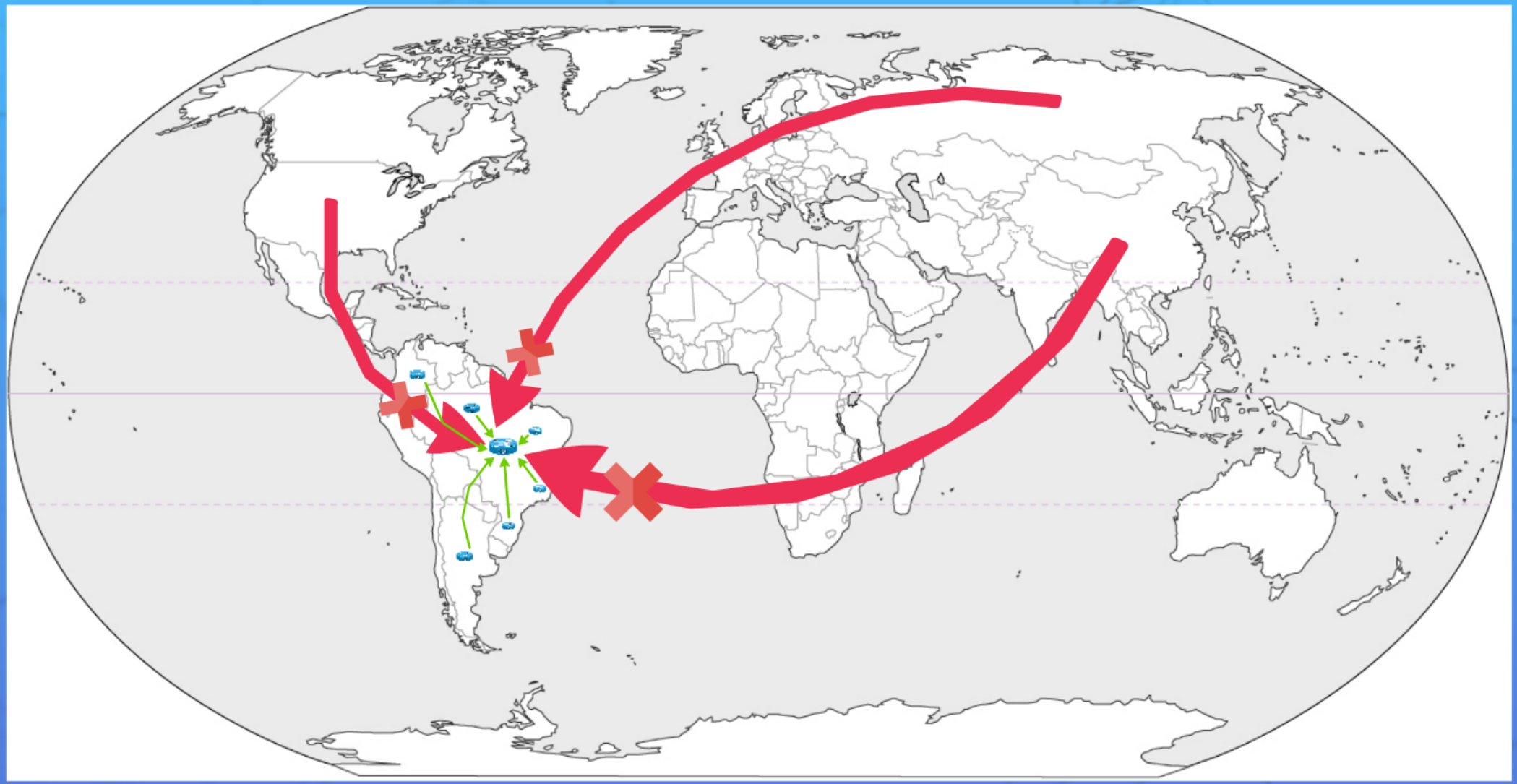
plo básico de uso em ataque D

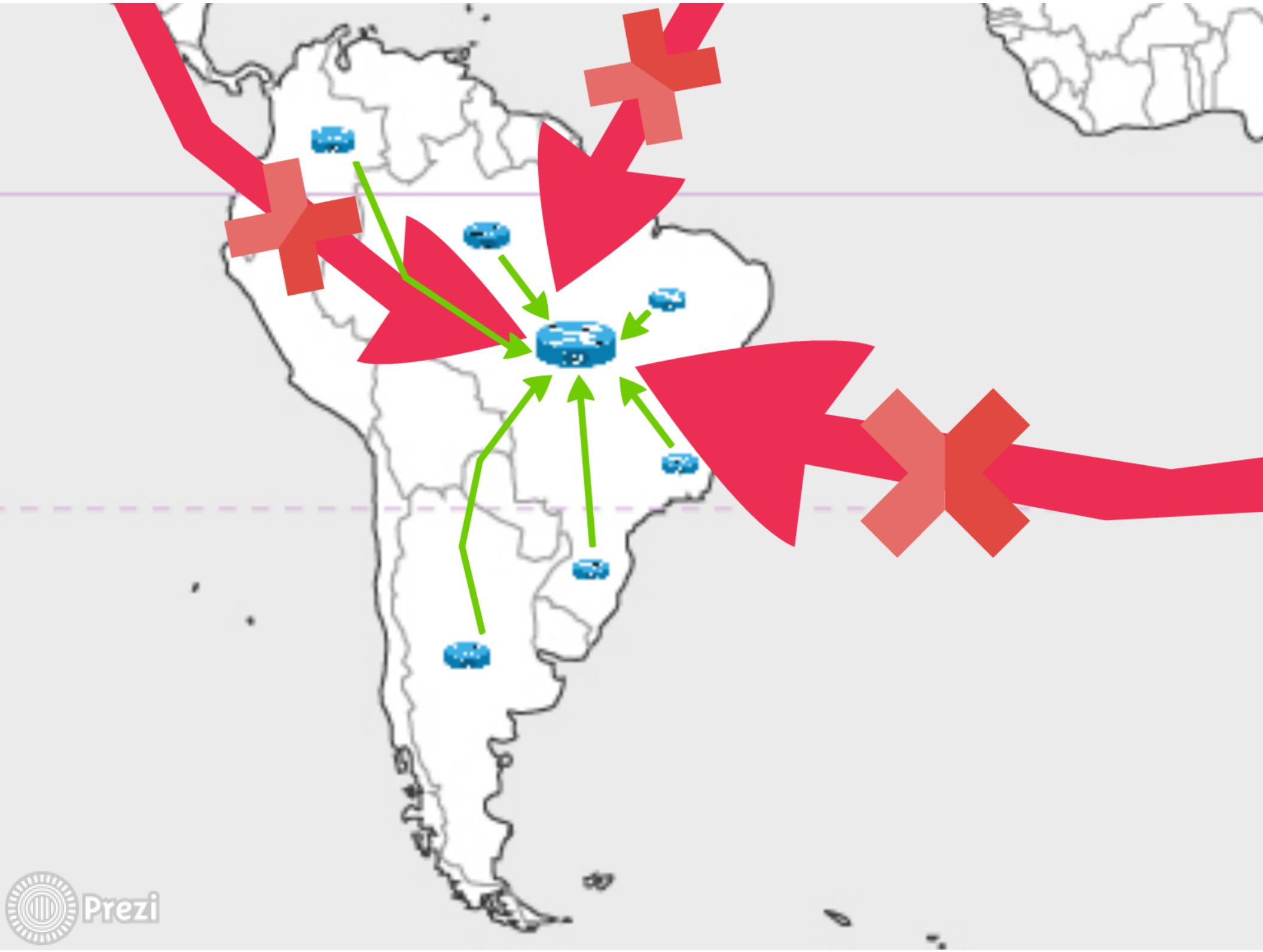



Link 5Gbps
Saturado
HOST ALVO
172.16.1.10
IP:172.16.1.10
(Blackhole)
Internet
Anuncio (blackhole)
IP:172.16.1.10
Communities: 64509:666
Clientes
Alegres :D
Fluxo DDoS
DST:172.16.1.10
20Gbps
Meu BGP
OPERADORA "UMBRELLA"
ASN 64511
ASN: 64509
Link 5Gbps
Disponivel

```
/routing bgp network
add network=172.16.1.10/32 synchronize=no
```

```
/routing filter
add action=accept chain=Operadora1_out comment="ANUNCIO PARA BLACKHOLE" prefix=\
    172.16.1.10 set-bgp-communities=64509:666
```




Prezi

Filtragem de Prefixos

Basicamente a BCP 194, em peerings com a operadora *(upstream)*, recomenda adotar algumas políticas.

Prefixos de entrada "in":

- ✗ Pertencentes ao próprio AS.
- ✗ De uso privado, especial ou reservado.
  (que não devem ter roteamento na internet, e também ser utilizados para spoofing)

Prefixos de saída "out"

- ✗ Mais específicos que /24 em IPv4 e /48 em IPv6.
- ✓ Todos os Prefixos pertencentes ao AS em questão.

O que isso evita?

- ✓ Qualquer possibilidade de receber prefixos de meu próprio AS;
- ✓ Virar trânsito para terceiros, de forma indesejada;
- ✓ "Route Leaking";
- ✓ Encaminhamento de pacotes "Marcianos";
- ✓ "Flood" descontrolado da tabela global de roteamento;

Exemplo (tuncito indesejável):

...menda adotar algumas polít...

Prefixos de entrada "in":

- ✗ Pertencentes ao próprio AS.
- ✗ De uso privado, especial ou reservado.

(que não devem ter roteamento na internet, e também ser utilizados para spoofing)

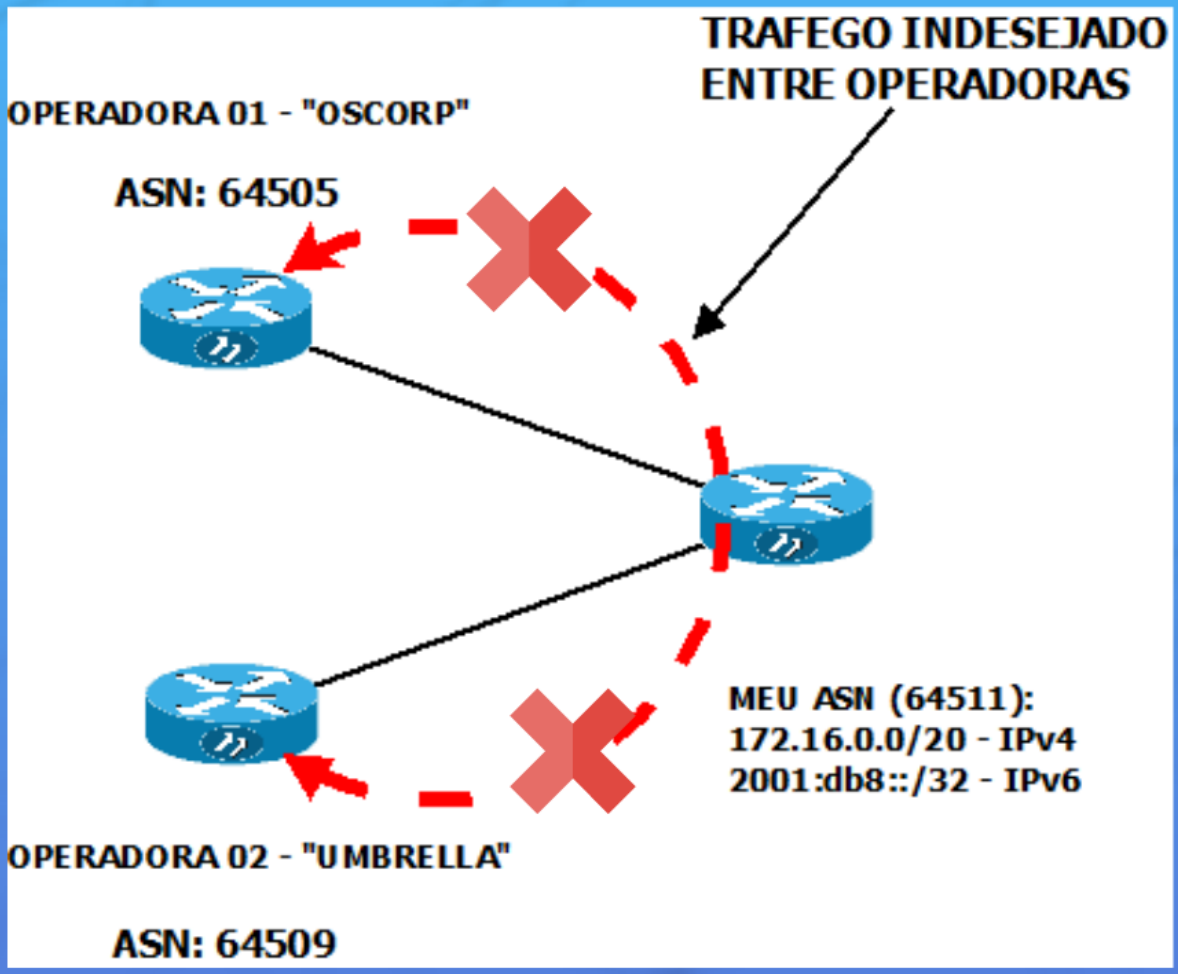
Prefixos de saída "out"

- ✗ Mais específicos que /24 em IPv4 e /48 em IPv6.
- ✓ Todos os Prefixos pertencentes ao AS em questão

O que isso evita?

- Quaisquer possibilidade de receber prefixos de meu próprio AS;
- Virar trânsito para terceiros, de forma indesejada;
- "Route Leaking";
- Encaminhamento de pacotes "Marcianos";
- "Flood" descontrolado da tabela global de roteamento;

Exemplo (transito indesejavel):



Fonte: Autoria própria, 2017

Alguns Exemplos...

Descarte de entrada dos blocos de seu próprio AS:

IPv4:

```
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora01" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 2  - Operadora01" prefix=172.16.16.0/21 prefix-length=21-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora02" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 2 - Operadora02" prefix=172.16.16.0/21 prefix-length=21-32
```

Fonte: Autoria própria,2017

IPv6:

```
add action=discard chain=OperadoraO1_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 01" prefix=2001:db8::/32 prefix-length=32-128
add action=discard chain=OperadoraO2_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 02" prefix=2001:db8::/32 prefix-length=32-128
```

Fonte: Autoria própria,2017

Descarte estático de entrada de prefixos de uso especial/ privados:

IPv4:

```
/routing filter
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
add action=discard chain=BGP-IN-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=198.18.0.0/15 prefix-length=15-32
add action=discard chain=BGP-IN-IPV4 prefix=198.51.100.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=203.0.113.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=224.0.0.0/4 prefix-length=4-32
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/0
```

IPv6:

Aceitar alocaçoes de RIR's e descartar o resto

Aceitar "Global Unicast" e descartar o resto

Fonte: Autoria propria, 2017

Prezi

Alguns Exemplos...

Descarte de entrada dos blocos de seu próprio AS:

IPv4:

```
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora01" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 2  - Operadora01" prefix=172.16.16.0/21 prefix-length=21-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora02" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 2 - Operadora02" prefix=172.16.16.0/21 prefix-length=21-32
```

Fonte: Autoria própria,2017

IPv6:

```
add action=discard chain=Operadora01_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 01" prefix=2001:db8::/32 prefix-length=32-12
add action=discard chain=Operadora02_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 02" prefix=2001:db8::/32 prefix-length=32-12
```

Fonte: Autoria própria,2017

Descarte estático de entrada de prefixos de uso especial/ privados:

Descarte de entrada dos blocos de seu próprio AS:

IPv4:

```
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora01" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 2  - Operadora01" prefix=172.16.16.0/21 prefix-length=21-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora02" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 2 - Operadora02" prefix=172.16.16.0/21 prefix-length=21-32
```

Fonte: Autoria própria,2017

IPv6:

```
add action=discard chain=Operadora01_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 01" prefix=2001:db8::/32 prefix-length=32-128
add action=discard chain=Operadora02_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 02" prefix=2001:db8::/32 prefix-length=32-128
```

Fonte: Autoria própria,2017

Descarte estático de entrada de prefixos de uso especial/ privados:

IPv4:

```
uting filter
 action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
 action=discard chain=BGP-IN-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
 action=discard chain=BGP-IN-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
 action=discard chain=BGP-IN-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
 action=discard chain=BGP-IN-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
 action=discard chain=BGP-IN-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
 action=discard chain=BGP-IN-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
 action=discard chain=BGP-IN-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
```

IPv6:

Aceitar alocaçoes de RIR's e descartar o resto

2600:0000::/12	ARIN	2006-10-03	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2610:0000::/23	ARIN	2006-11-17	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2620:0000::/23	ARIN	2006-09-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
2a00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2c00:0000::/12	AFRINIC	2006-10-03	whois.afrinic.net	https://rdap.afrinic.net/rdap/ http://rdap.afrinic.net/rdap/	ALLOCATED

lista completa em: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

IPv6:

```
add action=discard chain=Operadora01_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 01" prefix=2001:db8::/32 prefix-length=32-128
add action=discard chain=Operadora02_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 02" prefix=2001:db8::/32 prefix-length=32-128
```

Fonte: Autoria própria,2017

Descarte estático de entrada de prefixos de uso especial/ privados:

IPv4:

```
/routing filter
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
add action=discard chain=BGP-IN-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=198.18.0.0/15 prefix-length=15-32
add action=discard chain=BGP-IN-IPV4 prefix=198.51.100.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=203.0.113.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=224.0.0.0/4 prefix-length=4-32
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/0
```

IPv6:

Aceitar alocaçoes de RIR's e descartar o resto

2600:0000::/12	ARIN	2006-10-03	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2610:0000::/23	ARIN	2005-11-17	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2620:0000::/23	ARIN	2006-09-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
2a00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2c00:0000::/12	AFRINIC	2006-10-03	whois.afrinic.net	https://rdap.afrinic.net/rdap/ http://rdap.afrinic.net/rdap/	ALLOCATED

lista completa em: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

Aceitar "Global Unicast" e descartar o resto

```
/routing filter
add action=accept chain=BGP-IN-IPV6 comment="ACEITA - GLOBAL - IPv6" prefix=2000::/3 prefix-length=3-48
add action=discard chain=BGP-IN-IPV6 comment="DESCARTA - RESTO - IPv6"
```

Fonte: Autoria propria, 2017

Descarte estático de entrada privados:

IPv4:

```
/routing filter
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
add action=discard chain=BGP-IN-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=198.18.0.0/15 prefix-length=15-32
add action=discard chain=BGP-IN-IPV4 prefix=198.51.100.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=203.0.113.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=224.0.0.0/4 prefix-length=4-32
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/0
```

IPv6:

Aceitar alocaçoes de RIR's e descartar o resto

2600:0000::/12	ARIN	2006-10-03	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2610:0000::/23	ARIN	2005-11-17	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2620:0000::/23	ARIN	2006-09-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
2a00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2c00:0000::/12	AFRINIC	2006-10-03	whois.afrinic.net	https://rdap.afrinic.net/rdap/ http://rdap.afrinic.net/rdap/	ALLOCATED

lista completa em: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

Aceitar "Global Unicast" e descartar o resto

```
/routing filter
add action=accept chain=BGP-IN-IPV6 comment="ACEITA - GLOBAL - IPv6" prefix=2000::/3 prefix-length=3-48
add action=discard chain=BGP-IN-IPV6 comment="DESCARTA - RESTO - IPv6"
```

Fonte: Autoria propria, 2017

Aceitar alocaçoes de RIR's e descartar o resto

2600:0000::/12	ARIN	2006-10-03	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2610:0000::/23	ARIN	2005-11-17	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2620:0000::/23	ARIN	2006-09-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
2a00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2c00:0000::/12	AFRINIC	2006-10-03	whois.afrinic.net	https://rdap.afrinic.net/rdap/ http://rdap.afrinic.net/rdap/	ALLOCATED

lista completa em: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

ceitar "Global Unicast" e descartar o resto

2600:0000::/12	ARIN	2006-10-03	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2610:0000::/23	ARIN	2005-11-17	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2620:0000::/23	ARIN	2006-09-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	ALLOCATED
2800:0000::/12	LACNIC	2006-10-03	whois.lacnic.net	https://rdap.lacnic.net/rdap/	ALLOCATED
2a00:0000::/12	RIPE NCC	2006-10-03	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED
2c00:0000::/12	AFRINIC	2006-10-03	whois.afrinic.net	https://rdap.afrinic.net/rdap/ http://rdap.afrinic.net/rdap/	ALLOCATED

lista completa em: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

Aceitar "Global Unicast" e descartar o resto

```
/routing filter
add action=accept chain=BGP-IN-IPV6 comment="ACEITA - GLOBAL - IPv6" prefix=2000::/3 prefix-length=3-48
add action=discard chain=BGP-IN-IPV6 comment="DESCARTA - RESTO - IPv6"
```

Fonte: Autoria propria, 2017

Anuncio de Prefixos (Exemplos)

Anunciando apenas prefixos de meu AS (exemplo winbox):

	Chain	Prefix	Prefix Length	Action	Set BGP Prepend
;	ANUNCIA MEU BLOCO 1 - Operadora01				
	MinhaOperadora_01_out	172.16.0.0/20		accept	
;	ANUNCIA MEU BLOCO 1 - Operadora01				
	MinhaOperadora_01_out	172.16.0.0/24		accept	
	MinhaOperadora_01_out			discard	
;	ANUNCIA MEU BLOCO 1 - Operadora02				
	MinhaOperadora_02_out	172.16.0.0/20		accept	
;	DESCARTA RESTO ANUNCIOS - Operadora02				
	MinhaOperadora_02_out			discard	
;	ANUNCIO MEU BLOCO IPv6 - OPERADORA 01				
	Operadora01_IPv6_out	2001:db8::/32		accept	
;	DESCARTA RESTO ANUNCIOS IPv6 - OPERADORA 01				
	Operadora01_IPv6_out			discard	
;	ANUNCIA BLOCO IPv6 - OPERADORA 02				
	Operadora02_IPv6_out	2001:db8::/32		accept	
;	DESCARTA RESTO ANUNCIOS IPv6 - OPERADORA 02				
	Operadora02_IPv6_out			discard	

Fonte: Autoria própria,2017

Prepare os filtros **ANTES** de estabelecer qualquer sessão!

Anunciando apenas prefixos de meu AS (exemplo winbox):

Chain	Prefix	Prefix Length	Action	Set BGP Prepend
;;; ANUNCIA MEU BLOCO 1 - Operadora01				
MinhaOperadora_01_out	172.16.0.0/20		accept	
;;; ANUNCIA MEU BLOCO 1 - Operadora01				
MinhaOperadora_01_out	172.16.0.0/24		accept	
MinhaOperadora_01_out			discard	
;;; ANUNCIA MEU BLOCO 1 - Operadora02				
MinhaOperadora_02_out	172.16.0.0/20		accept	
;;; DESCARTA RESTO ANUNCIOS - Operadora02				
MinhaOperadora_02_out			discard	
;;; ANUNCIO MEU BLOCO IPv6 - OPERADORA 01				
Operadora01_IPv6_out	2001:db8::/32		accept	
;;; DESCARTA RESTO ANUNCIOS IPv6 - OPERADORA 01				
Operadora01_IPv6_out			discard	
;;; ANUNCIA BLOCO IPv6 - OPERADORA 02				
Operadora02_IPv6_out	2001:db8::/32		accept	
;;; DESCARTA RESTO ANUNCIOS IPv6 - OPERADORA 02				
Operadora02_IPv6_out			discard	

Fonte: Autoria própria,2017

Prezi

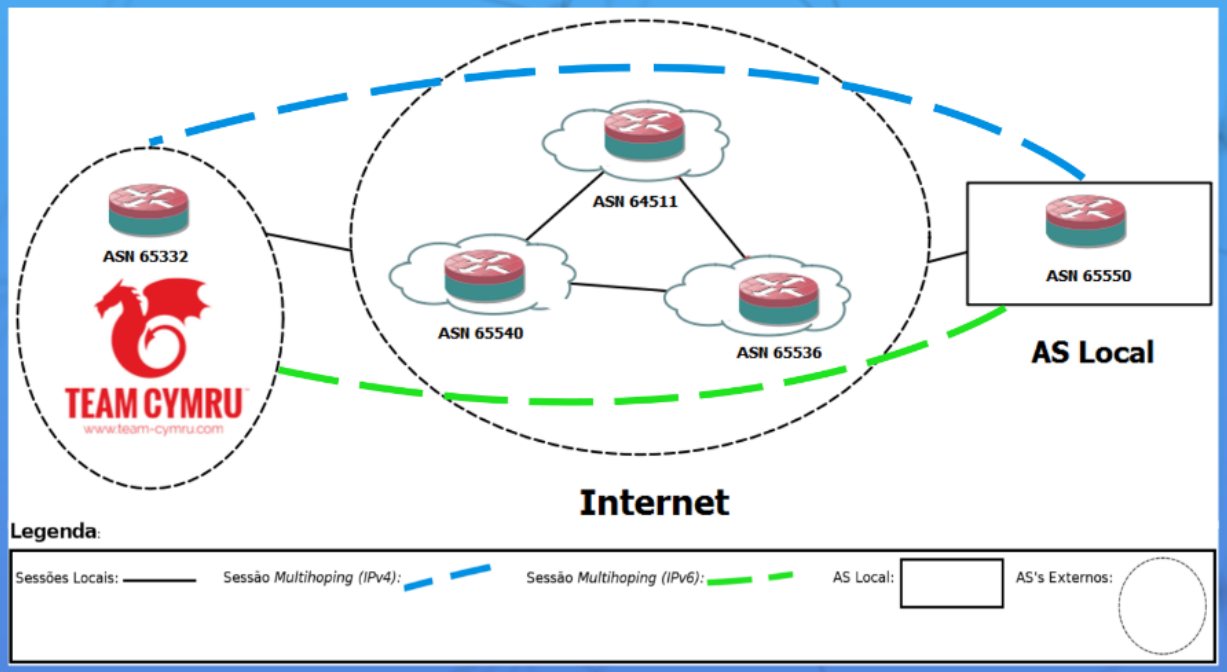
Prepare os filtros **ANTES** de estabelecer qualquer sessão!

ut	2001:db8::/32	
NUNCIOS IPv6 - OPERADORA 02		
ut		

Fonte: Autoria própria,2017

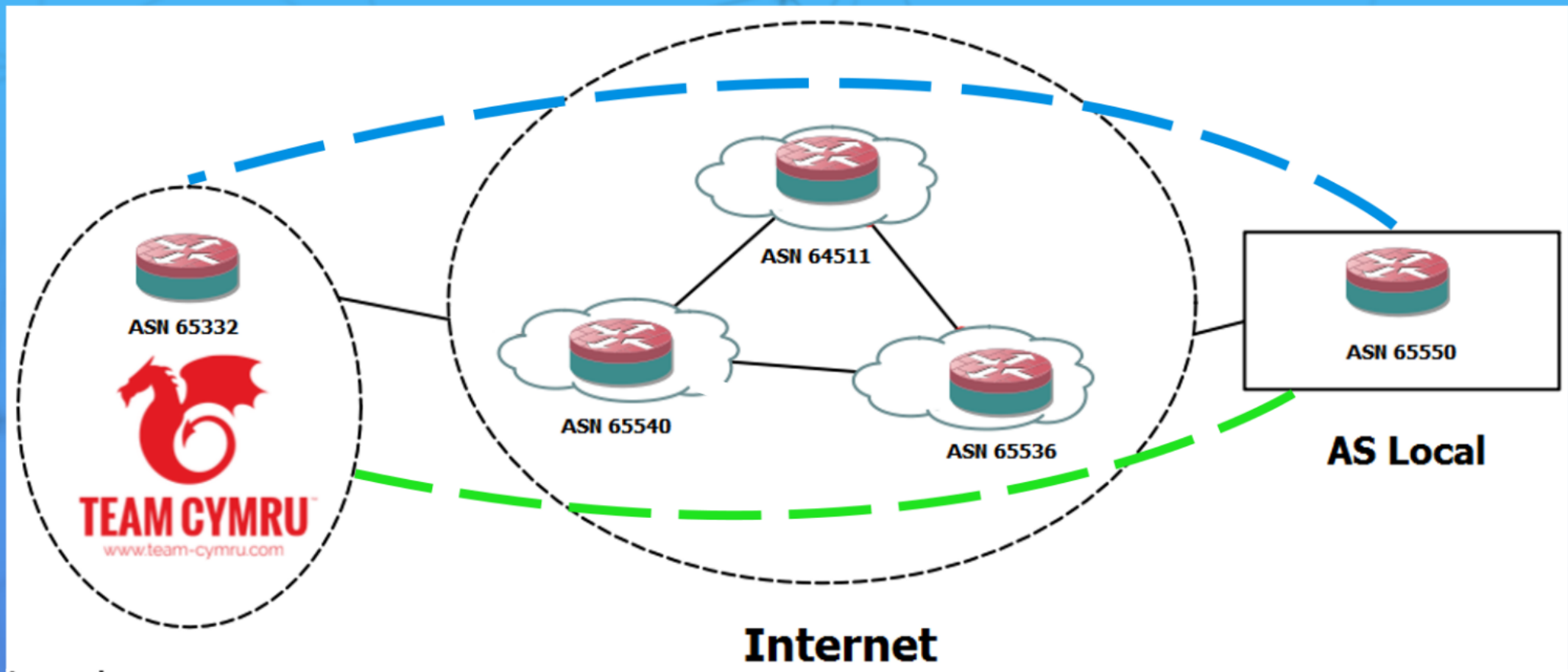
Prepare os filtros **ANTES** de estabelecer qualquer sessão!

Obtendo lista dinâmica de prefixos para descarte (bogons)



Fonte: Autoria própria,2016

Prezi



Legenda:

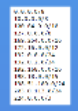
Sessões Locais: ——— Sessão *Multihoping (IPv4):* - - - Sessão *Multihoping (IPv6):* - - - AS Local: ▭ AS's Externos: ◯

Fonte: Autoria própria,2016

"Taditional Bogons vs FULL Bogons":

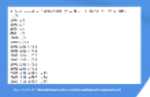
"Traditional Bogons"

- Lista atual de 13 prefixos
- De uso reservado para uso especial ou privado pela IANA.
- Pode ser utilizado para compor ACL's que analisam a origem de pacotes como o antispoofing.



"FULL Bogons"

- Inclui todos os prefixos do modo "traditional" com acrécimo de prefixos não alocados pelos RIR's.
- Lista constantemente atualizada



CYMRU - (Estatís

"Traditional Bogons"

- Lista atual de 13 prefixos
- De uso reservado para uso especial ou privado pela IANA.
- Pode ser utilizado para compor ACL's que analisam a origem de pacotes como o antispoofing.

```
0.0.0.0/8
10.0.0.0/8
100.64.0.0/10
127.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.0.0.0/24
192.0.2.0/24
192.168.0.0/16
198.18.0.0/15
198.51.100.0/24
203.0.113.0/24
224.0.0.0/3
```

...sível em: http://www.team-cymru.org/Services/Bogons/bogon-b... ...xt

0.0.0.0/8
10.0.0.0/8
100.64.0.0/10
127.0.0.0/8
169.254.0.0/16
172.16.0.0/12
192.0.0.0/24
192.0.2.0/24
192.168.0.0/16
198.18.0.0/15
198.51.100.0/24
203.0.113.0/24
224.0.0.0/3

"FULL Bogons"

- Inclui todos os prefixos do modo "traditional" com acrécimo de prefixos não alocados pelos RIR's.
- Lista constantemente atualizada

```
# last updated 1509655801 (Thu Nov  2 20:50:01 2017 GMT)
0.0.0.0/8
2.56.0.0/14
5.8.248.0/21
5.39.200.0/21
5.45.32.0/20
5.100.240.0/21
5.104.72.0/21
5.133.64.0/18
5.172.176.0/21
5.180.0.0/14
5.199.184.0/21
5.252.0.0/15
10.0.0.0/8
31.12.72.0/21
31.13.184.0/21
31.22.8.0/21
31.40.192.0/18
31.132.8.0/21
31.132.32.0/19
31.133.96.0/21
31.169.120.0/21
```

lista completa em: http://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

```
# last updated 1509655801 (Thu Nov  2 20:50:01 2017 GMT)
::/8
100::/8
200::/7
400::/6
800::/5
1000::/4
2000::/16
2001:201::/32
2001:202::/31
2001:204::/30
2001:209::/32
2001:20a::/31
2001:20c::/30
2001:210:2000::/35
2001:210:4000::/34
2001:210:8000::/33
```

lista completa em: http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt

```
# last updated 1509655801 (Thu Nov  2 20:50:01 2017 GMT)
0.0.0.0/8
2.56.0.0/14
5.8.248.0/21
5.39.200.0/21
5.45.32.0/20
5.100.240.0/21
5.104.72.0/21
5.133.64.0/18
5.172.176.0/21
5.180.0.0/14
5.199.184.0/21
5.252.0.0/15
10.0.0.0/8
31.12.72.0/21
31.13.184.0/21
31.22.8.0/21
31.40.192.0/18
31.132.8.0/21
31.132.32.0/19
31.133.96.0/21
31.169.120.0/21
```

lista completa em: http://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt

```
# last updated 1509655801 (Thu Nov  2 20:50:01 2017 GMT)
::/8
100::/8
200::/7
400::/6
800::/5
1000::/4
2000::/16
2001:201::/32
2001:202::/31
2001:204::/30
2001:209::/32
2001:20a::/31
2001:20c::/30
2001:210:2000::/35
2001:210:4000::/34
2001:210:8000::/33
```

lista completa em: http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt

Team CYMRU - (Estatísticas):

PREFIX COUNTS LAST UPDATED: **JULY 2017**

The *IPv4 traditional bogons* list is currently **13 prefixes**.

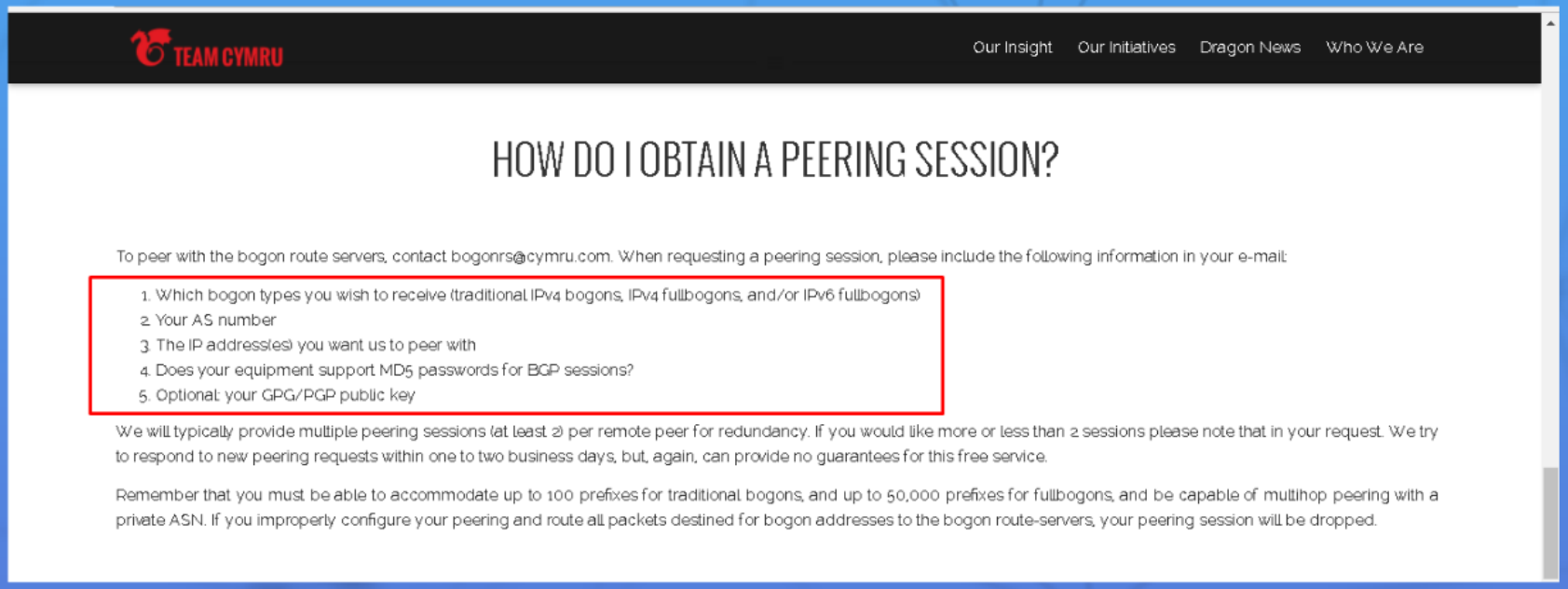
It is not likely to change going forward (IANA allocated the remaining free blocks in 2011.)

The *IPv4 fullbogons* list is approximately **3,827 prefixes**.

The *IPv6 fullbogons* list is approximately **86,836 prefixes**.

fonte: http://www.team-cymru.org/bogon-reference-bgp.html
Em: 07/2017

Team CYMRU
Obtendo sua sessão:



TEAM CYMRU

Our Insight Our Initiatives Dragon News Who We Are

HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact bogonrs@cymru.com. When requesting a peering session, please include the following information in your e-mail:

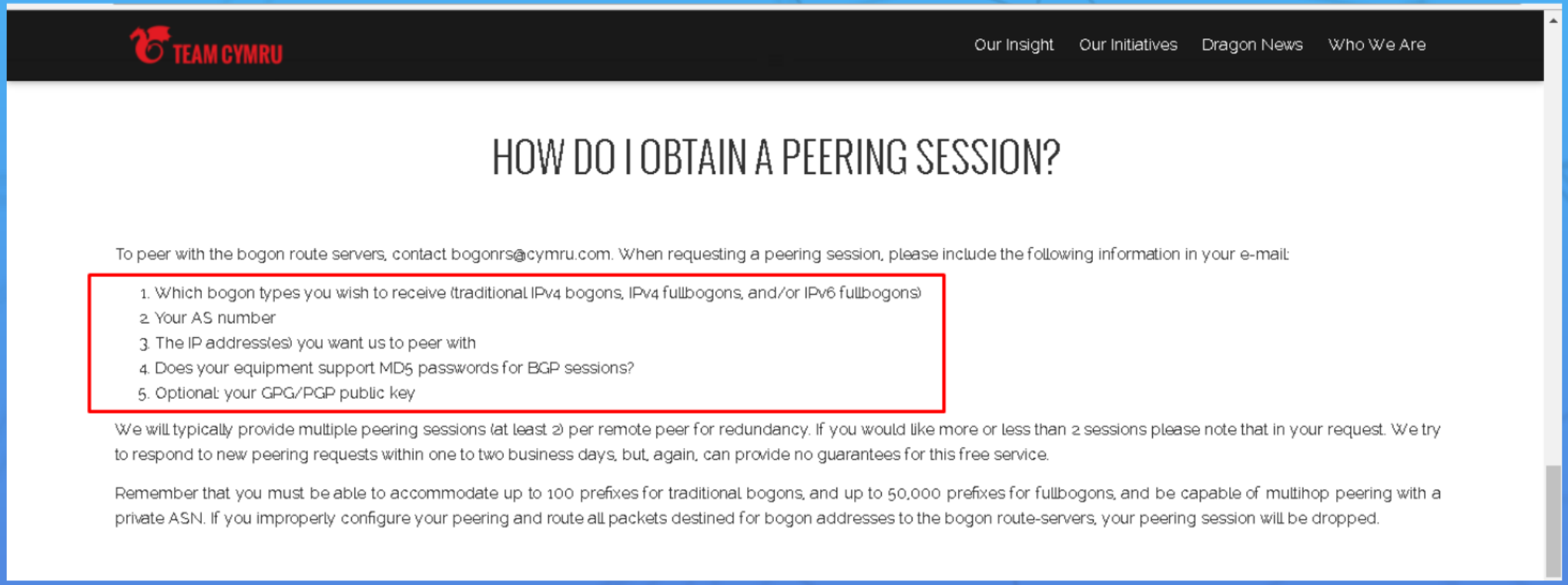
1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this free service.

Remember that you must be able to accommodate up to 100 prefixes for traditional bogons, and up to 50,000 prefixes for fullbogons, and be capable of multihop peering with a private ASN. If you improperly configure your peering and route all packets destined for bogon addresses to the bogon route-servers, your peering session will be dropped.

fonte: www.team-cymru.org/bogon-reference-bgp.html - julho 2017

Obtendo sua sessão:



TEAM CYMRU

Our Insight Our Initiatives Dragon News Who We Are

HOW DO I OBTAIN A PEERING SESSION?

To peer with the bogon route servers, contact bogonrs@cymru.com. When requesting a peering session, please include the following information in your e-mail:

1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4 fullbogons, and/or IPv6 fullbogons)
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

We will typically provide multiple peering sessions (at least 2) per remote peer for redundancy. If you would like more or less than 2 sessions please note that in your request. We try to respond to new peering requests within one to two business days, but, again, can provide no guarantees for this free service.

Remember that you must be able to accommodate up to 100 prefixes for traditional bogons, and up to 50,000 prefixes for fullbogons, and be capable of multihop peering with a private ASN. If you improperly configure your peering and route all packets destined for bogon addresses to the bogon route-servers, your peering session will be dropped.

fonte: www.team-cymru.org/bogon-reference-bgp.html - julho 2017

Team CYMRU Implementação

(exemplo de full bogons no RouterOS)

```
# Full Bogons Mikrotik Template
# Work on RouterOS 4.X
# 2010-11-01 by Ricardo Ozelo

# BGP instance setup

/routing bgp instance set default as=<YOUR_ASN> \
 router-id=<WAN_IP_ADDRESS>

# ROUTING FILTERS - Install these routes as blackholes,
# does NOT receive or announce anything else

/routing filter add action=accept bgp-communities=65332:888 \
 chain=cymru-in comment="" disabled=no invert-match=no \
 set-type=blackhole
/routing filter add action=discard chain=cymru-in comment="" \
 disabled=no invert-match=no
/routing filter add action=discard chain=cymru-out comment="" \
 disabled=no invert-match=no

# Peering #1

/routing bgp peer add address-families=ip,ipv6 disabled=no in-filter=cymru-in \
 instance=default multihop=yes name=FULLBOGONS-CYMRU-1 out-filter=cymru-out \
 remote-address=<CYMRU_IP_ADDRESS_1> remote-as=65332 tcp-md5-key=<CYMRU_MD5_PASSWORD>

# Peering #2

/routing bgp peer add address-families=ip,ipv6 disabled=no in-filter=cymru-in \
 instance=default multihop=yes name=FULLBOGONS-CYMRU-2 out-filter=cymru-out \
 remote-address=<CYMRU_IP_ADDRESS_2> remote-as=65332 tcp-md5-key=<CYMRU_MD5_PASSWORD>
```

fonte: http://www.team-cymru.org/bgp-examples.html#mikrotik-full
em 10/2017

```
# Full Bogons Mikrotik Template
# Work on RouterOS 4.X
# 2010-11-01 by Ricardo Ozelo

# BGP instance setup

/routing bgp instance set default as=<YOUR_ASN> \
 router-id=<WAN_IP_ADDRESS>

# ROUTING FILTERS - Install these routes as blackholes,
# does NOT receive or announce anything else

/routing filter add action=accept bgp-communities=65332:888 \
 chain=cymru-in comment="" disabled=no invert-match=no \
 set-type=blackhole
/routing filter add action=discard chain=cymru-in comment="" \
 disabled=no invert-match=no
/routing filter add action=discard chain=cymru-out comment="" \
 disabled=no invert-match=no

# Peering #1

/routing bgp peer add address-families=ip,ipv6 disabled=no in-filter=cymru-in \
 instance=default multihop=yes name=FULLBOGONS-CYMRU-1 out-filter=cymru-out \
 remote-address=<CYMRU_IP_ADDRESS_1> remote-as=65332 tcp-md5-key=<CYMRU_MD5_PASSWORD>

# Peering #2

/routing bgp peer add address-families=ip,ipv6 disabled=no in-filter=cymru-in \
 instance=default multihop=yes name=FULLBOGONS-CYMRU-2 out-filter=cymru-out \
 remote-address=<CYMRU_IP_ADDRESS_2> remote-as=65332 tcp-md5-key=<CYMRU_MD5_PASSWORD>
```

fonte: http://www.team-cymru.org/bgp-examples.html#mikrotik-full
em 10/2017

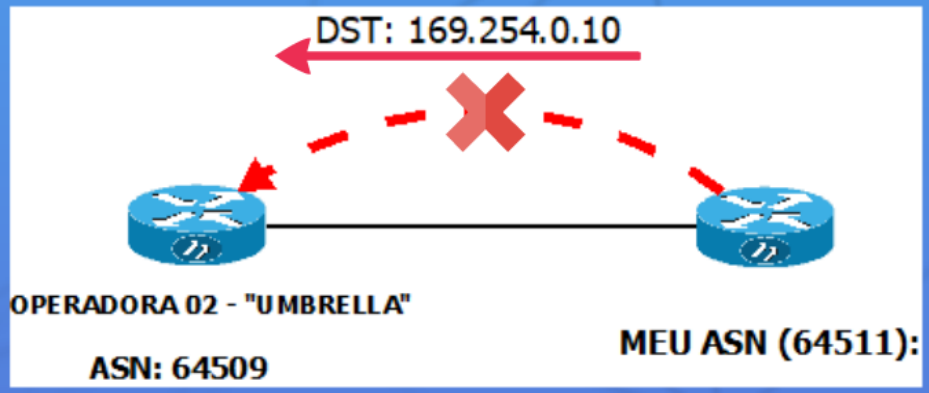
Team CYMRU

(sessão ativa - exemplo)

```
E name="TeamCYMRU_Bogons_IPv4" instance=default remote-address=193.[redacted] remote-as=65332
  tcp-md5-key="[redacted]" nexthop-choice=default multihop=yes route-reflect=no hold-time=3m
  ttl=default max-prefix-limit=10000 max-prefix-restart-time=30m in-filter=Cymru_in
  out-filter=Cymru_out address-families=ip default-originate=never remove-private-as=no
  as-override=no passive=no use-bfd=no
```

```
[                                        ] > ip route print where type=blackhole
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r
 #      DST-ADDRESS        PREF-SRC        GATEWAY                DISTANCE
 0 ADbB 0.0.0.0/8                                                      20
 1 ADbB 2.56.0.0/14                                                    20
 2 ADbB 5.8.248.0/21                                                   20
 3 ADbB 5.39.200.0/21                                                  20
 4 ADbB 5.45.32.0/20                                                   20
 5 ADbB 5.100.240.0/21                                                 20
 6 ADbB 5.104.72.0/21                                                  20
 7 ADbB 5.133.64.0/18                                                  20
 8 ADbB 5.172.176.0/21                                                 20
 9 ADbB 5.180.0.0/14                                                   20
10 ADbB 5.199.184.0/21                                                 20
```

```
[                                                    ] > tool traceroute 169.254.0.10
 # ADDRESS                                          LOSS SENT    LAST      AVG
 1                                                  100%    2 timeout
 2                                                  100%    2 timeout
 3                                                  100%    1 timeout
 4                                                  100%    1 timeout
 5                                                  100%    1 timeout
```



IMPORTANTE!

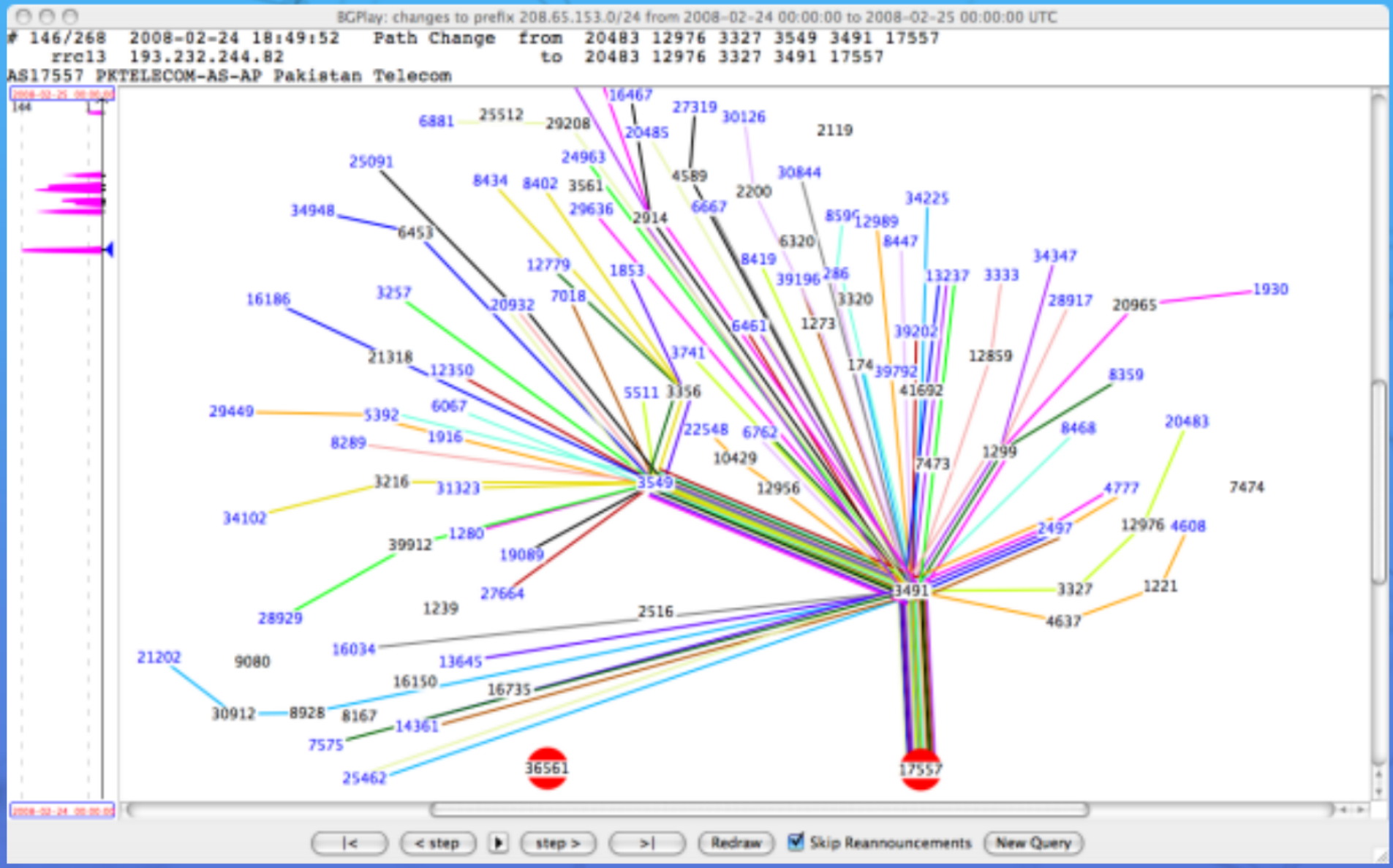
SEMPRE anunciar os prefixos originados a partir de seu AS apenas com recursos pertencentes ao mesmo, caso contrário, podemos cometer um erro chamado de "Route Leaking" que pode atrapalhar o funcionamento da Internet.

O anúncio de prefixos não pertencentes ao AS em questão também pode ser utilizado com principios maliciosos, como tentativas de "Hijacking".

SEMPRE anunciar os prefixos originados a partir de seu AS apenas com recursos pertencentes ao mesmo, caso contrário, podemos cometer um erro chamado de "Route Leaking" que pode atrapalhar o funcionamento da Internet.

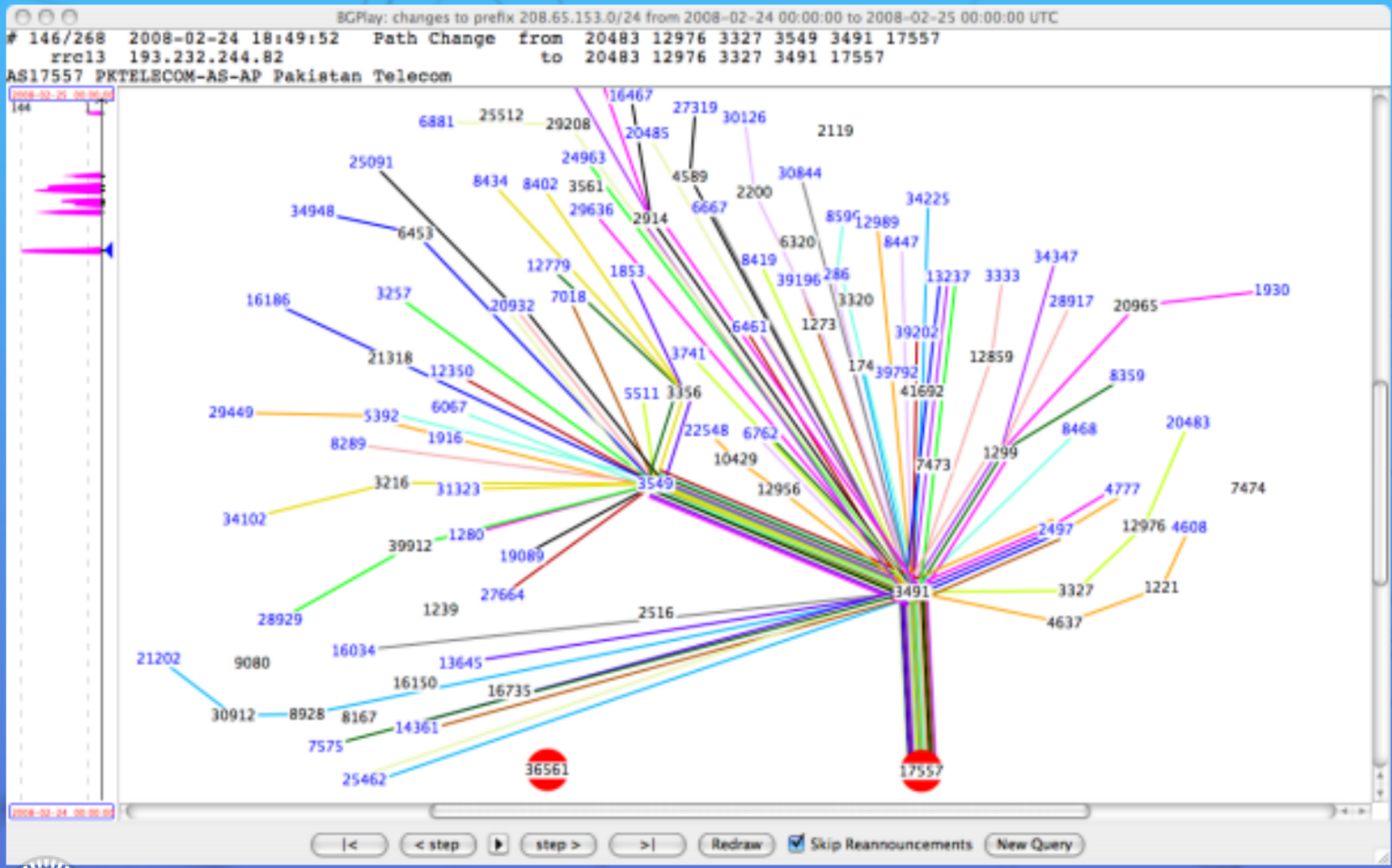
O anúncio de prefixos não pertencentes ao AS em questão também pode ser utilizado com principios maliciosos, como tentativas de "Hijacking".

Caso conhecido entre Youtube e Pakistan Telecom (24 de fevereiro de 2008)



http://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

(24 de fevereiro de 2008)



Boas práticas para o roteador de borda:

"Este ativo deve estar plenamente configurado com ênfase em sua principal função" *(Oliveira, 2016).*

Basicamente precisamos ter:

- Sessões BGP;
- Tabelas e filtros de Roteamento;
- ACL's essenciais;

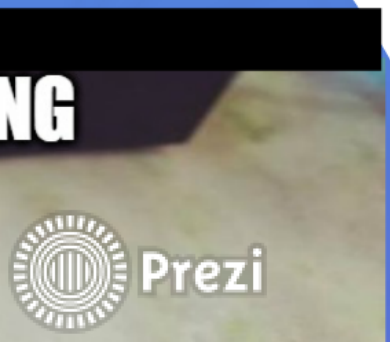
São alguns recursos desnecessários:

- DHCP;
- DNS recursivo;
- Hotspot;
- NTP Server;
- FTP;
- IGP nas interfaces de sessões como o OSPF.
- IPv6 RA (Router Advertisement) nas interfaces de sessões.

Alguns serviços desnecessários mal configurados, podem ser tornar potenciais vulnerabilidades exploradas para amplificação de trafego (muito usado para ataques DDoS).

E outras "coisas"...

Simples exemplo em cenário real:



Boas práticas para o roteador de borda:

"Este ativo deve estar plenamente configurado com ênfase em sua principal função" *(Oliveira, 2016).*

Basicamente precisamos ter:

- ✓ Sessões BGP;
- ✓ Tabelas e filtros de Roteamento;

Basicamente precisamos ter:

- Sessões BGP;
- Tabelas e filtros de Roteamento;
- ACL's essenciais;

São alguns recursos desnecessários:

- DHCP;
- DNS recursivo;
- Hotspot;
- NTP Server;
- FTP;
- IGP nas interfaces de sessões como o OSPF.
- IPv6 RA (Router Advertisement) nas interfaces de sessões.

Alguns serviços desnecessários mal configurados, podem ser tornar potenciais vulnerabilidades exploradas para amplificação de trafego (muito usado para ataques DDoS).

E outras "coisas"...

Simples exemplo em cenário real:

- DHCP;
- DNS recursivo;
- Hotspot;
- NTP Server;
- FTP;
- IGP nas interfaces de sessões como o OSPF.
- IPv6 RA (Router Advertisement) nas interfaces de sessões.

Algu
mal
torn
vuln
para
(mu
DDo

E outras "coisas"...

Alguns serviços desnecessários mal configurados, podem ser tornar potenciais vulnerabilidades exploradas para amplificação de trafego (muito usado para ataques DDoS).

Simples exemplo em cenário real:

(Lembre-se: Adeque-os de acordo com a função e necessidade)

```
[                                ] > /system package print
Flags: X - disabled
 #    NAME                                VERSION
 0    routeros-tile                       6.34.6
 1    system                              6.34.6
 2  X wireless-cm2                        6.34.6
 3    ipv6                                6.34.6
 4  X wireless-fp                         6.34.6
 5  X hotspot                             6.34.6
 6  X dhcp                                6.34.6
 7  X mpls                                6.34.6
 8    routing                             6.34.6
 9  X ppp                                 6.34.6
10    security                            6.34.6
11    advanced-tools                      6.34.6
```

Fonte: Autoria própria, 2016.

```
[                                ] > /ip service print
Flags: X - disabled, I - invalid
 #    NAME            PORT ADDRESS
 0 XI telnet            23
 1 XI ftp               21
 2    www
 3    ssh
 4 XI www-ssl          443
 5 XI api             8728
 6    winbox
 7 XI api-ssl         8729
```

Fonte: Autoria própria, 2016.

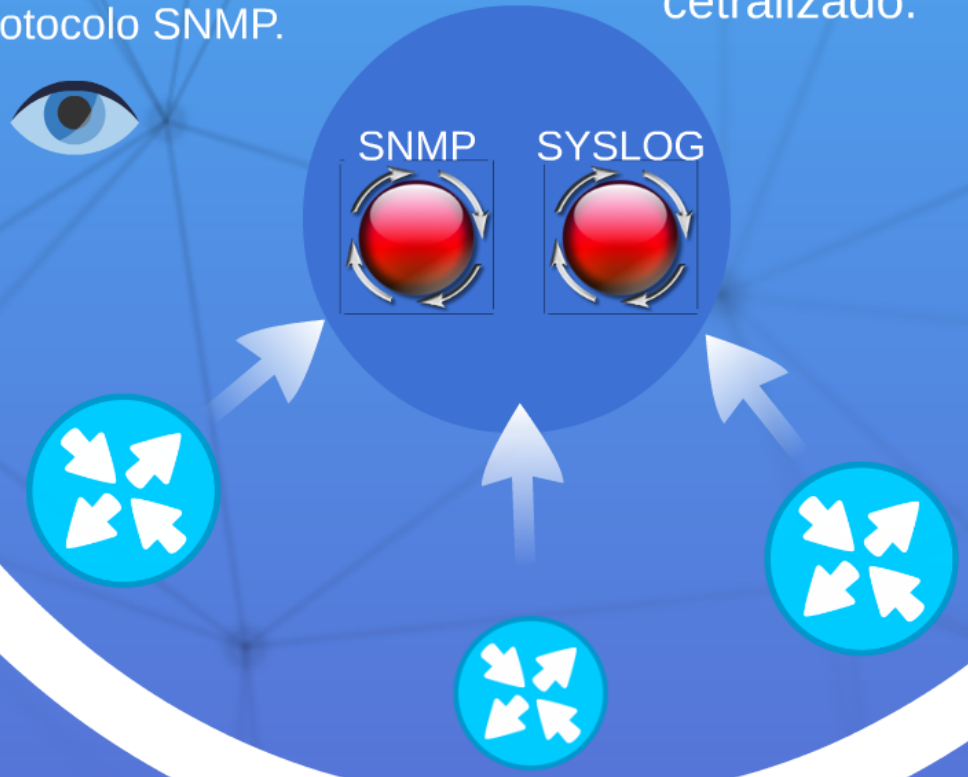
Boas práticas para o ativo de borda

- Logs em loghost centralizado.
- Otimizando o RouterOS.

Monitoramento e Armazenamento de logs:

Para o Monitoramento de CPU, temperatura e tráfego, podemos utilizar o protocolo SNMP.

Uma boa prática é manter os logs em um loghost cetralizado.



Dica básica para Performance no RouterOS:

FastPath:

- ✔ Permite um ganho incrível de uso de CPU no emcaminhamento de pacotes.
- ✔ Útil em cenários de **alto throughput**.

Condições

IPv4 handler

IPv4 fast path is automatically used if following conditions are met:

- firewall rules are not configured;
- firewall address lists are not configured;
- ~~Traffic flow is disabled. /ip traffic-flow enabled=no~~ restriction removed in 6.33;
- Simple and queue trees with parent=global are not configured;
- no mesh, metarouter interface configuration;
- sniffer, torch and traffic generator is not running;
- connection tracking is not active;
- ip accounting is disabled (/ip accounting enabled=no);
- VRFs are not set (/ip route vrf is empty);
- Hotspot is not used (/ip hotspot has no interfaces);
- IpSec policies are not configured (ROS v6.6);
- ~~no active mac-ping, mac-telnet or mac-winbox sessions~~ restriction removed in 6.33;
- /tool mac-scan is not actively used;
- /tool ip-scan is not actively used;
- route cache must be enabled

fonte:https://wiki.mikrotik.com/wiki/Manual:Fast_Path

Fasttrack:

FastTrack	
Without	With
360Mbps	890Mbps
CPU 100%	CPU 86%
41% CPU on firewall	6% CPU on firewall

* tested on RX1100 with single TCP stream

Fonte: https://wiki.mikrotik.com/wiki/Manual:Fasttrack

```
/ip firewall filter
add action=fasttrack-connection chain=forward comment=\
    "RouterOS Guide - FastTrack" connection-state=\
    established,related
add action=accept chain=forward comment="Aceita Estabelecidas / Relacionadas" \
    connection-state=established,related
```

Fonte: Autoria própria, 2017.

Observação: O FastTrack até o momento está disponível para IPv4.

Prezi

FastPath:

- Permite um ganho incrível de uso de CPU no emcaminhamento de pacotes.
- Útil em cenários de **alto throughput**.

Condições

IPv4 handler

IPv4 fast path is automatically used if following conditions are met:

- firewal rules are not configured;
- firewall address lists are not configured;
- ~~Traffic flow is disabled~~ `~~/ip traffic flow enabled=no~~` ~~restriction removed in 6.33~~;
- Simple and queue trees with parent=global are not configured;
- no mesh, metarouter interface configuration;
- sniffer, torch and traffic generator is not running;
- connection tracking is not active;
- ip accounting is disabled (/ip accounting enabled=no);
- VRFs are not set (/ip route vrf is empty);
- Hotspot is not used (/ip hostspot has no interfaces);
- IpSec policies are not configured (ROS v6.8);
- ~~no active mac ping, mac telnet or mac winbox sessions~~ restriction removed in 6.33;
- /tool mac-scan is not actively used;
- /tool ip-scan is not actively used;
- route cache must be enabled

fonte:https://wiki.mikrotik.com/wiki/Manual:Fast_Path

FastTrack

Without	With
360Mbps	**890Mbps**
CPU 100%	**CPU 86%**
44% CPU on firewall	6% CPU on firewall

* tested on RB2011 with single TCP stream

Fonte: https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack

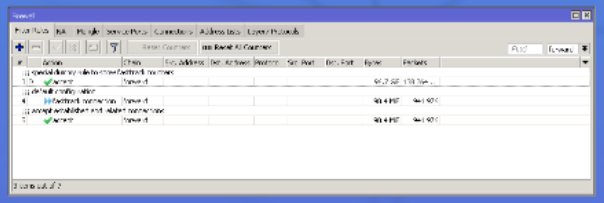
44% CPU on firewall	6% CPU on firewall

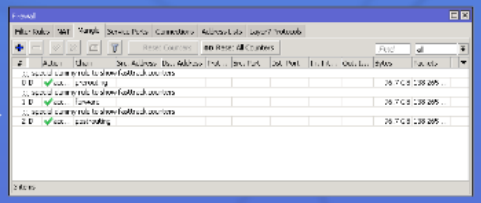
* tested on RB2011 with single TCP stream

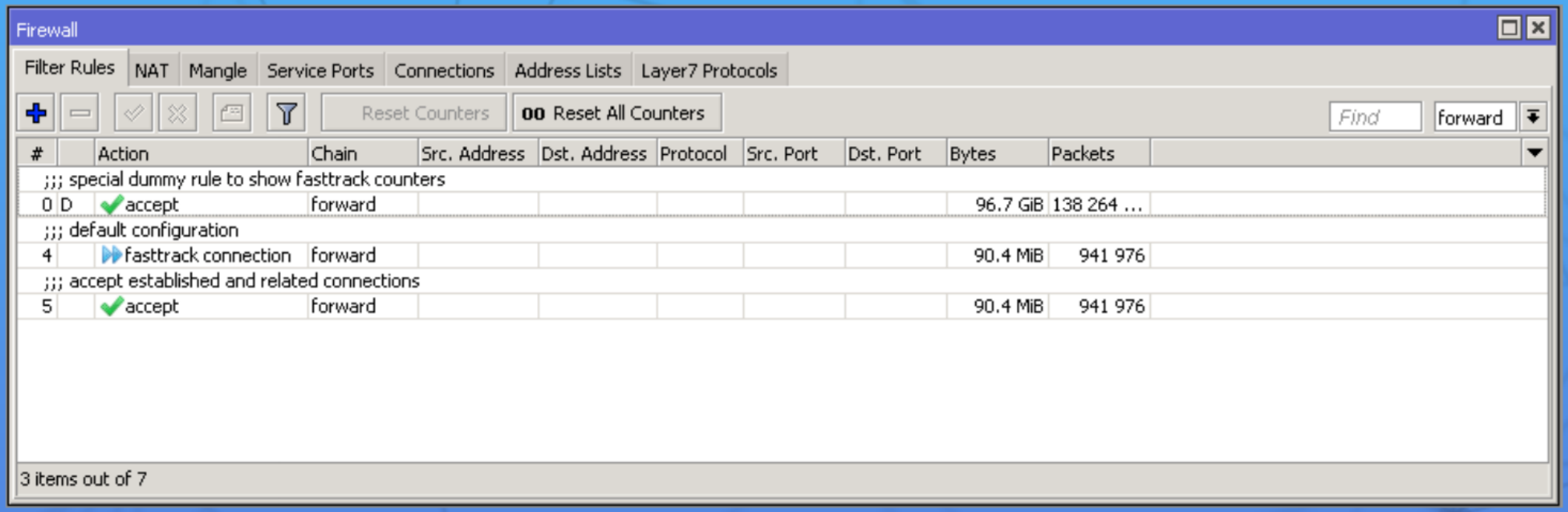
Fonte: https://wiki.mikrotik.com/wiki/Manual:IP/Fasttrack

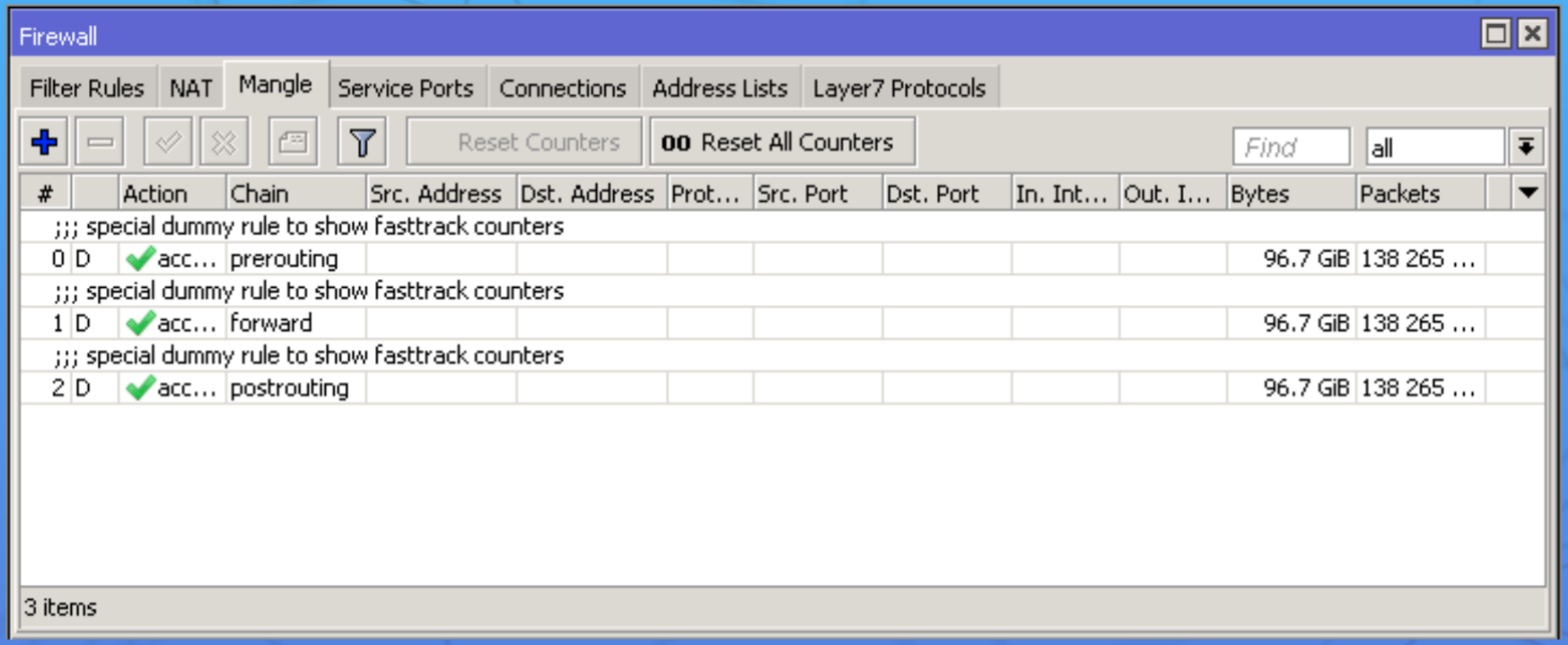
```
/ip firewall filter
add action=fasttrack-connection chain=forward comment=\
    "Estabelecidas / Relacionadas - Fasttrack" connection-state=\
    established,related
add action=accept chain=forward comment="Aceita Estabelecidas / Relacionadas" \
    connection-state=established,related
```

Fonte: Autoria própria, 2017.






Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
forward
Action Chain Src. Address Dst. Address Protocol Src. Port Dst. Port Bytes Packets
;;; special dummy rule to show fasttrack counters
0 D accept forward 96.7 GiB 138 264 ...
;;; default configuration
4 fasttrack connection forward 90.4 MiB 941 976
;;; accept established and related connections
5 accept forward 90.4 MiB 941 976
3 items out of 7


Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Prot... Src. Port Dst. Port In. Int... Out. I... Bytes Packets
;;; special dummy rule to show fasttrack counters
0 D acc... prerouting 96.7 GiB 138 265 ...
;;; special dummy rule to show fasttrack counters
1 D acc... forward 96.7 GiB 138 265 ...
;;; special dummy rule to show fasttrack counters
2 D acc... postrouting 96.7 GiB 138 265 ...
3 items

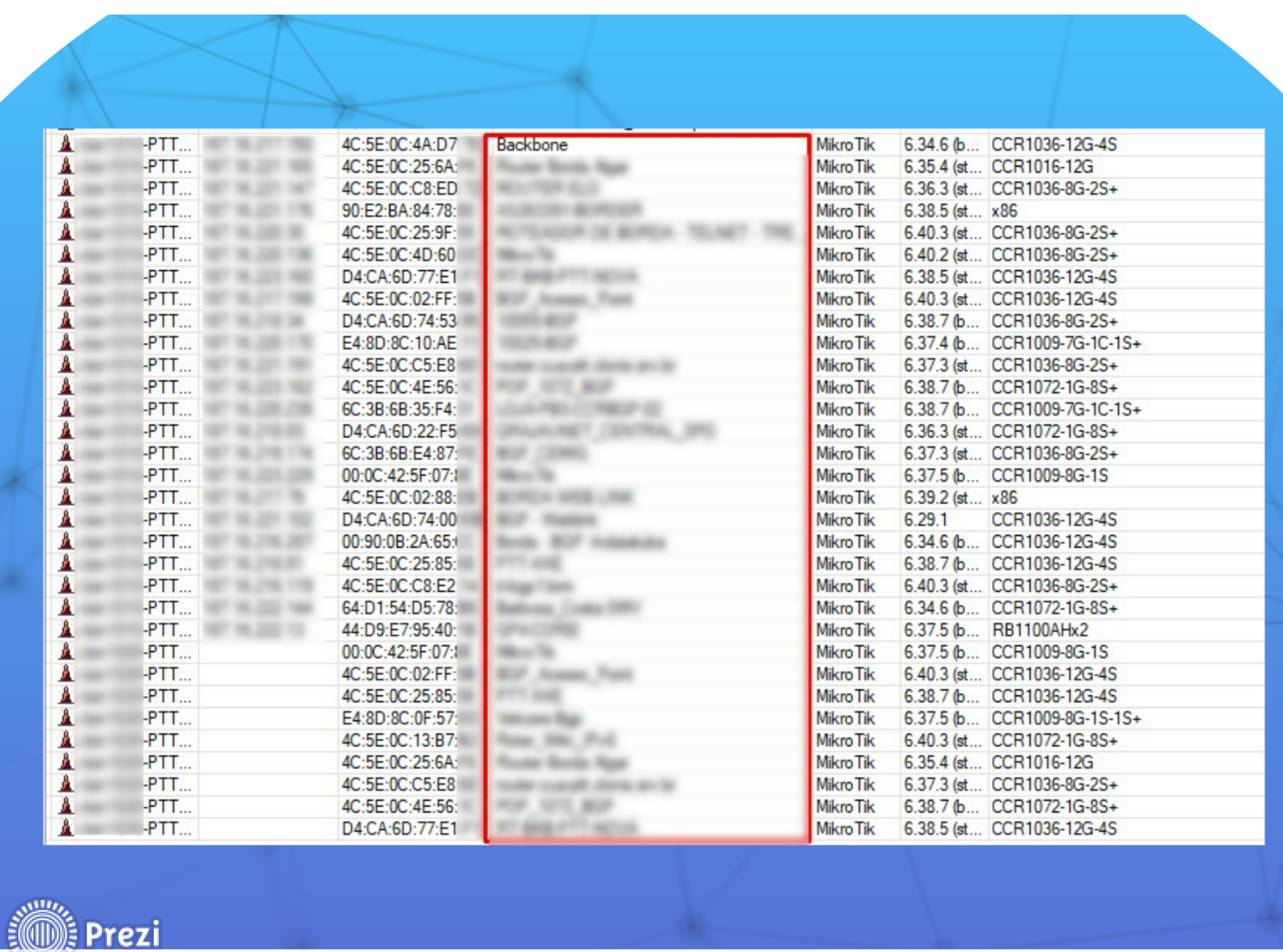
Observação: O FastTrack até o momento está disponível para IPv4.

Atenção ao uso seguintes recursos:

- SNMP com configurações default;
- MNDP (Mikrotik Neighbor Discovery Protocol) em interfaces não necessárias como upstreams;
- RoMON com configurações default.

Não se esqueça!

- Política de backup



-PTT...		4C:5E:0C:4A:D7	Backbone	MikroTik	6.34.6 (b...	CCR1036-12G-4S
-PTT...		4C:5E:0C:25:6A:		MikroTik	6.35.4 (st...	CCR1016-12G
-PTT...		4C:5E:0C:C8:ED		MikroTik	6.36.3 (st...	CCR1036-8G-2S+
-PTT...		90:E2:BA:84:78:		MikroTik	6.38.5 (st...	x86
-PTT...		4C:5E:0C:25:9F:		MikroTik	6.40.3 (st...	CCR1036-8G-2S+
-PTT...		4C:5E:0C:4D:60		MikroTik	6.40.2 (st...	CCR1036-8G-2S+
-PTT...		D4:CA:6D:77:E1		MikroTik	6.38.5 (st...	CCR1036-12G-4S
-PTT...		4C:5E:0C:02:FF:		MikroTik	6.40.3 (st...	CCR1036-12G-4S
-PTT...		D4:CA:6D:74:53		MikroTik	6.38.7 (b...	CCR1036-8G-2S+
-PTT...		E4:8D:8C:10:AE		MikroTik	6.37.4 (b...	CCR1009-7G-1C-1S+
-PTT...		4C:5E:0C:C5:E8		MikroTik	6.37.3 (st...	CCR1036-8G-2S+
-PTT...		4C:5E:0C:4E:56:		MikroTik	6.38.7 (b...	CCR1072-1G-8S+
-PTT...		6C:3B:6B:35:F4:		MikroTik	6.38.7 (b...	CCR1009-7G-1C-1S+
-PTT...		D4:CA:6D:22:F5		MikroTik	6.36.3 (st...	CCR1072-1G-8S+
-PTT...		6C:3B:6B:E4:87:		MikroTik	6.37.3 (st...	CCR1036-8G-2S+
-PTT...		00:0C:42:5F:07:		MikroTik	6.37.5 (b...	CCR1009-8G-1S
-PTT...		4C:5E:0C:02:88:		MikroTik	6.39.2 (st...	x86
-PTT...		D4:CA:6D:74:00		MikroTik	6.29.1	CCR1036-12G-4S
-PTT...		00:90:0B:2A:65:		MikroTik	6.34.6 (b...	CCR1036-12G-4S
-PTT...		4C:5E:0C:25:85:		MikroTik	6.38.7 (b...	CCR1036-12G-4S
-PTT...		4C:5E:0C:C8:E2		MikroTik	6.40.3 (st...	CCR1036-8G-2S+
-PTT...		64:D1:54:D5:78:		MikroTik	6.34.6 (b...	CCR1072-1G-8S+
-PTT...		44:D9:E7:95:40:		MikroTik	6.37.5 (b...	RB1100AHx2
-PTT...		00:0C:42:5F:07:		MikroTik	6.37.5 (b...	CCR1009-8G-1S
-PTT...		4C:5E:0C:02:FF:		MikroTik	6.40.3 (st...	CCR1036-12G-4S
-PTT...		4C:5E:0C:25:85:		MikroTik	6.38.7 (b...	CCR1036-12G-4S
-PTT...		E4:8D:8C:0F:57:		MikroTik	6.37.5 (b...	CCR1009-8G-1S-1S+
-PTT...		4C:5E:0C:13:B7:		MikroTik	6.40.3 (st...	CCR1072-1G-8S+
-PTT...		4C:5E:0C:25:6A:		MikroTik	6.35.4 (st...	CCR1016-12G
-PTT...		4C:5E:0C:C5:E8		MikroTik	6.37.3 (st...	CCR1036-8G-2S+
-PTT...		4C:5E:0C:4E:56:		MikroTik	6.38.7 (b...	CCR1072-1G-8S+
-PTT...		D4:CA:6D:77:E1		MikroTik	6.38.5 (st...	CCR1036-12G-4S

Resultados...
Como Analisar?

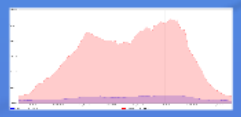
As boas práticas devem ser levadas em consideração e **aplicadas sempre que possivel e de acordo com o cenário.**
O resultado vem através do conjunto delas.

Ferramenta de análise "Radar by qrator"

Resultados de análise do site Radar byQrator
Fonte: https://radar.qrator.net, 2016

Como testar?

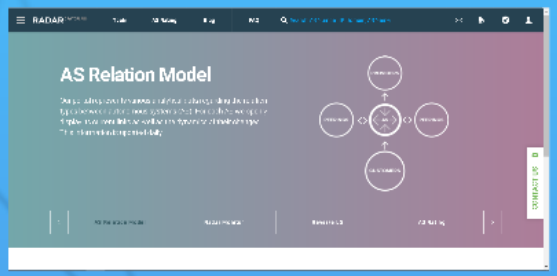
Estatísticas relevantes - Case RadarWISP

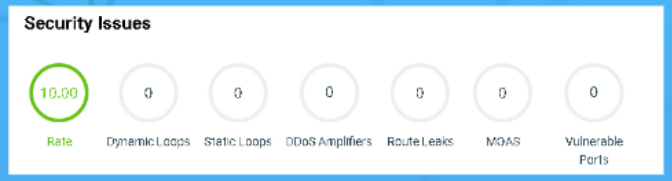


Prezi

O resultado vem através do conjunto delas.

Ferramenta de análise "Radar by qrator"



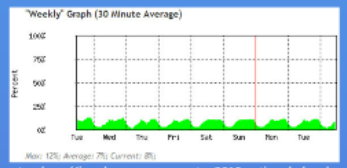


Resultados de análise do site Radar byQrator

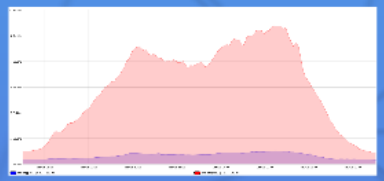
Fonte: https://radar.qrator.net, 2016

Como testar?

Estatísticas relevantes - Case RadarWISP



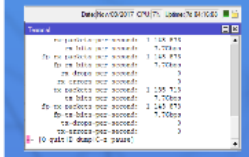
Amostra do gráfico de processamento, 2016 - ativo de borda - Hardware: RouterBoard CCR1072-1G-8S+



Amostra do gráfico em throughput acima de 5Gbps (em uma interface) - Hardware: RouterBoard CCR1072-1G-8S+

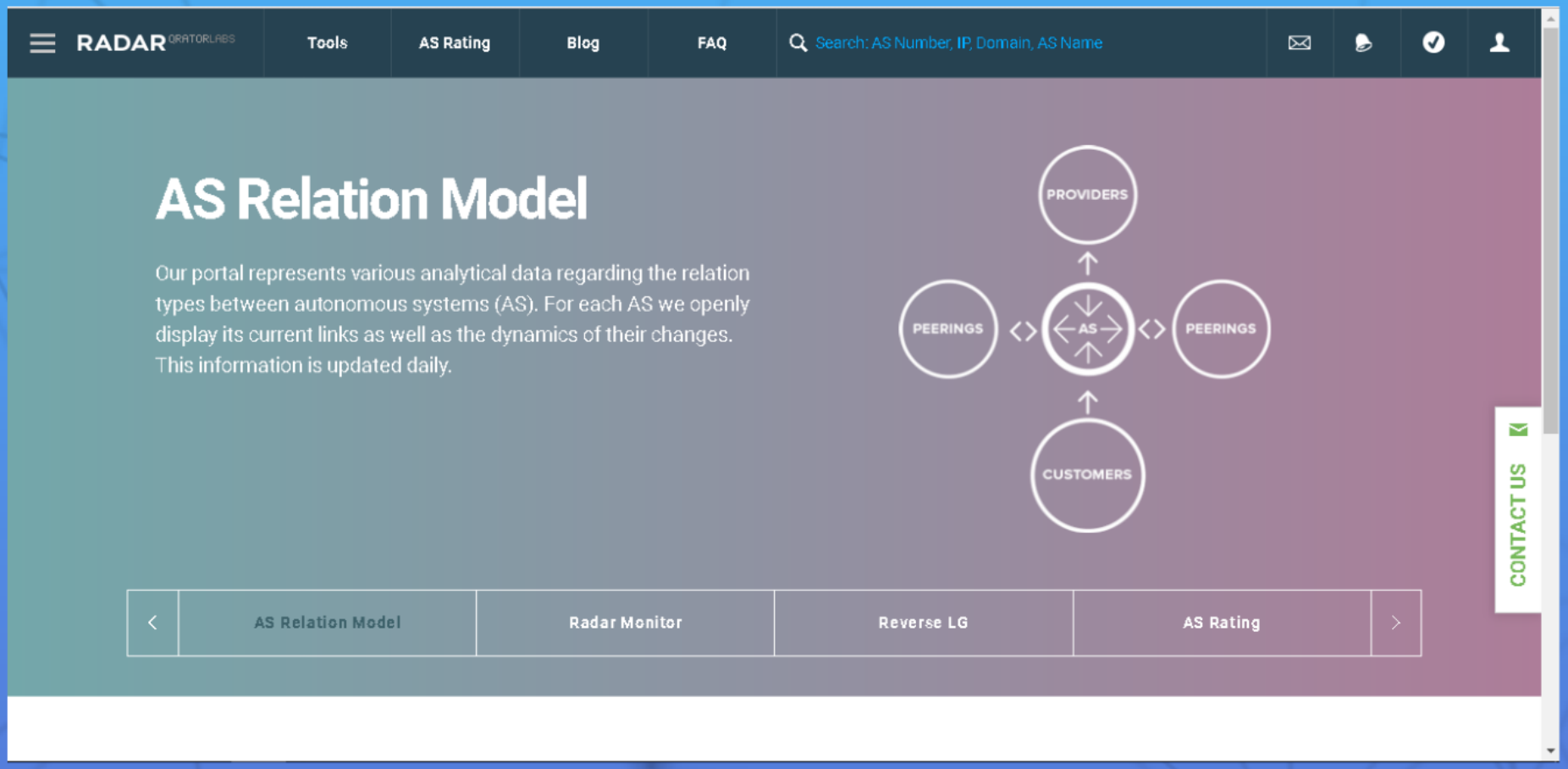
Uso de boas praticas + Route Server

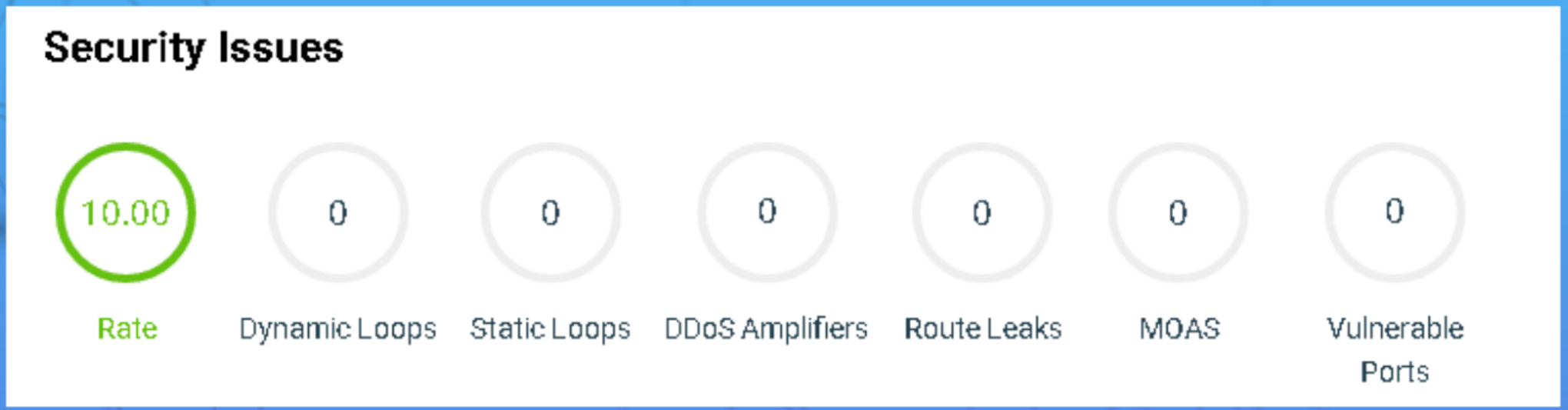
Fonte: Autoria própria, 2017



Prezi

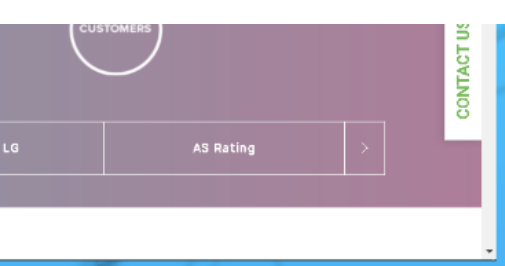
Ferramenta de análise "Radar by qrator"





Resultados de análise do site Radar byQrator

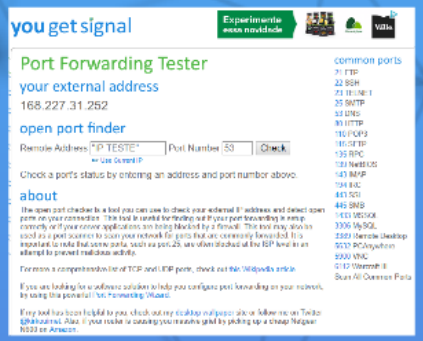
Fonte: https://radar.qrator.net, 2016



Resultado

Fonte

Como testar?

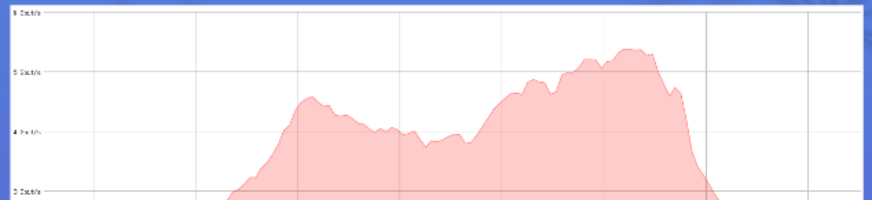


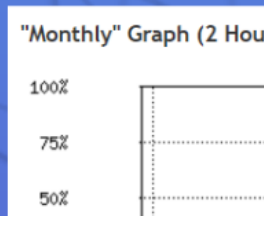
acessível em: https://www.yougetsignal.com/tools/open-ports/

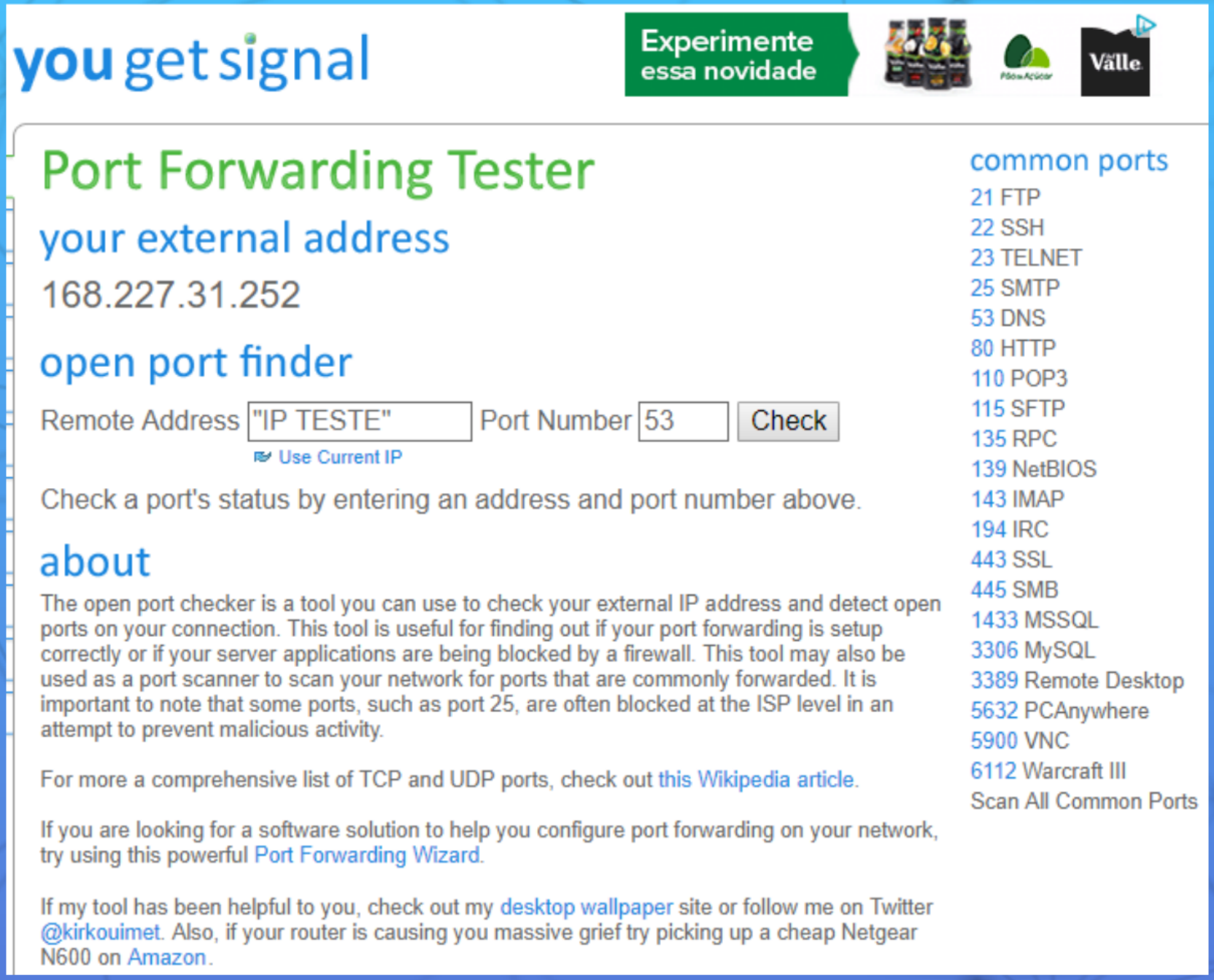
acessível em: http://openresolver.com/

acessível em: https://nmap.org/

ticas relevantes - Case RadarWISP







acessivel em: https://www.yougetsignal.com/tools/open-ports/

To manually test an IP address

```
dig +short test.openresolver.com TXT @1.2.3.4
```

(replace 1.2.3.4 with the IP address or domain name of the DNS server you are testing)

If you get "open-resolver-detected" in response, then you have a problem :)

Or, use a form:

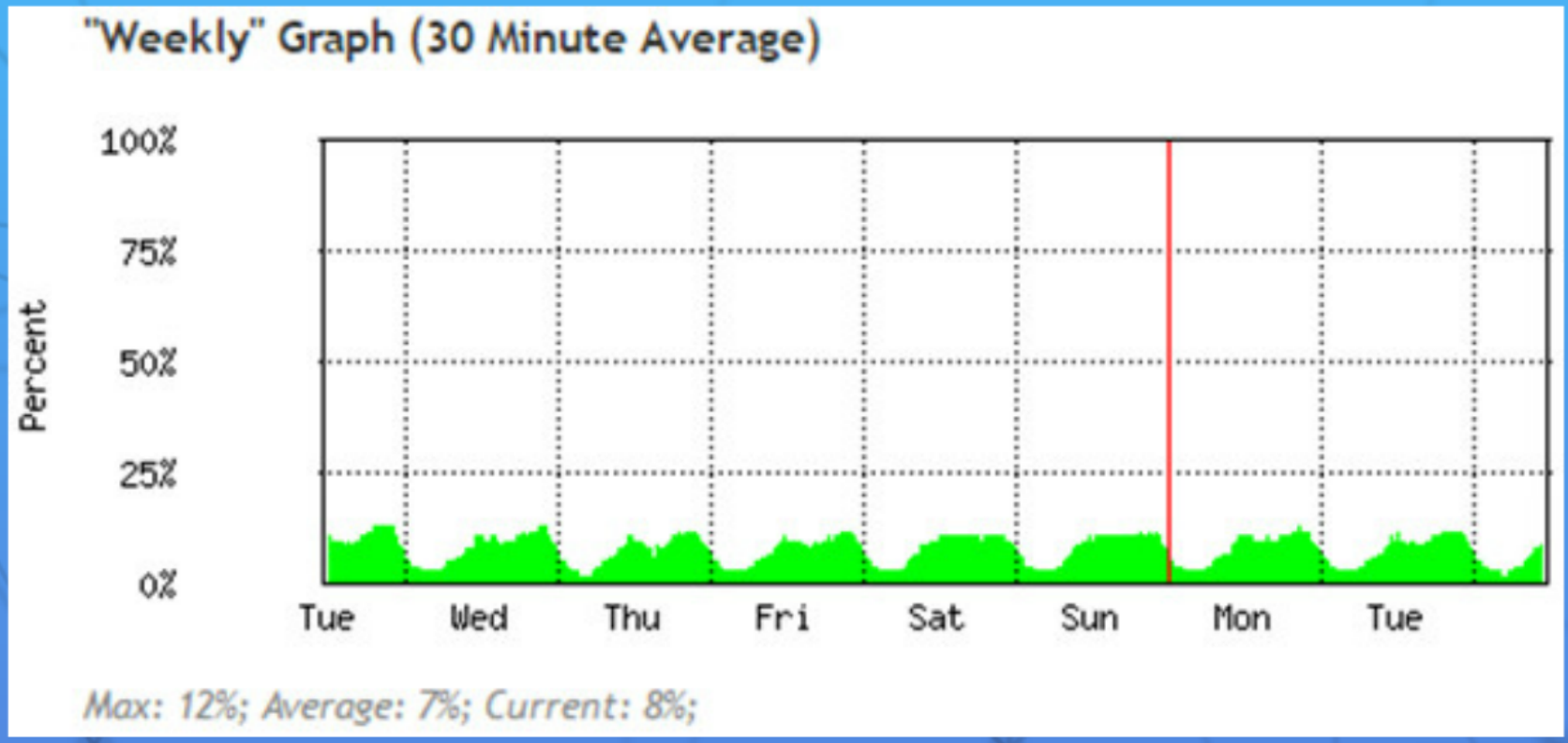
"MEU IP AQUI" Test this IP

acessivel em: http://openresolver.com/

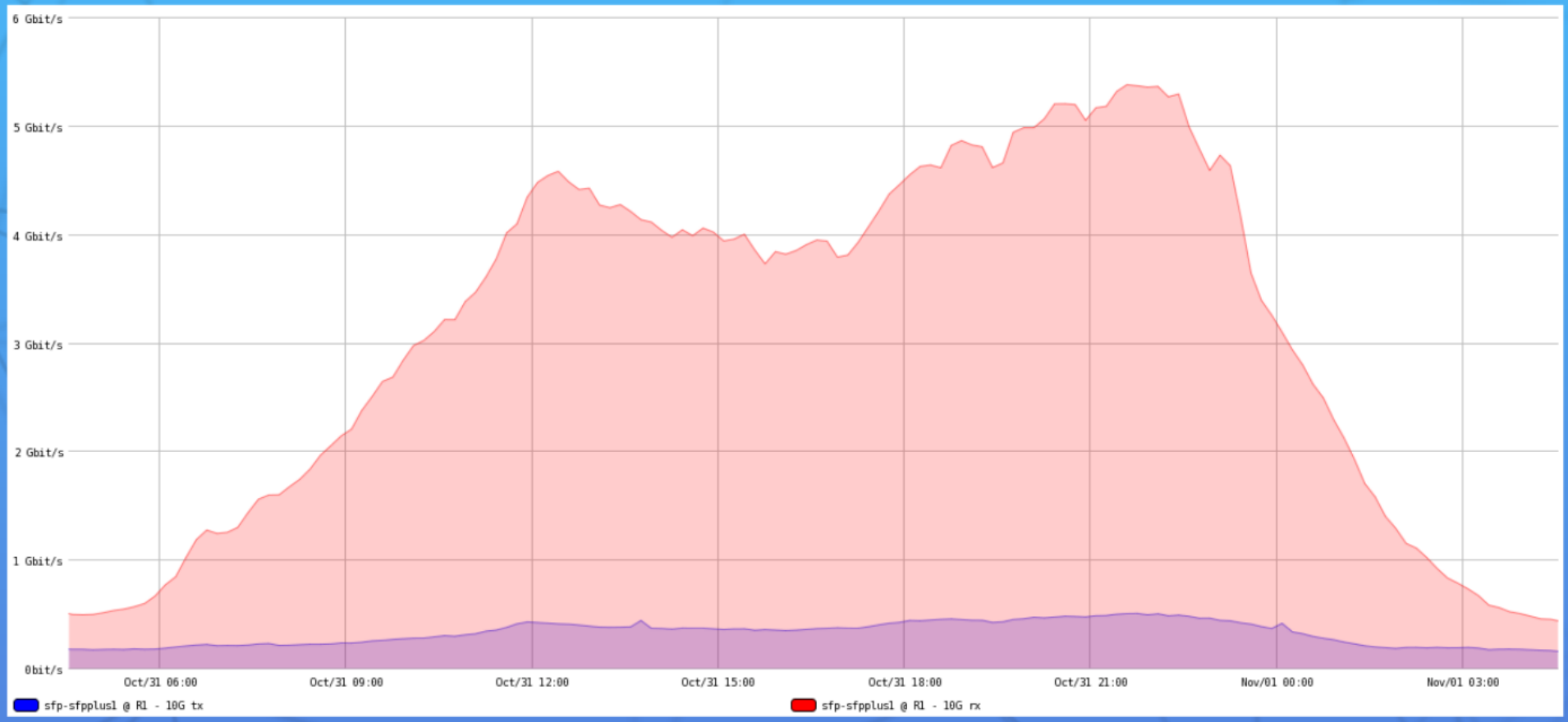
NMAP

acessivel em: https://nmap.org/

Estatísticas relevan

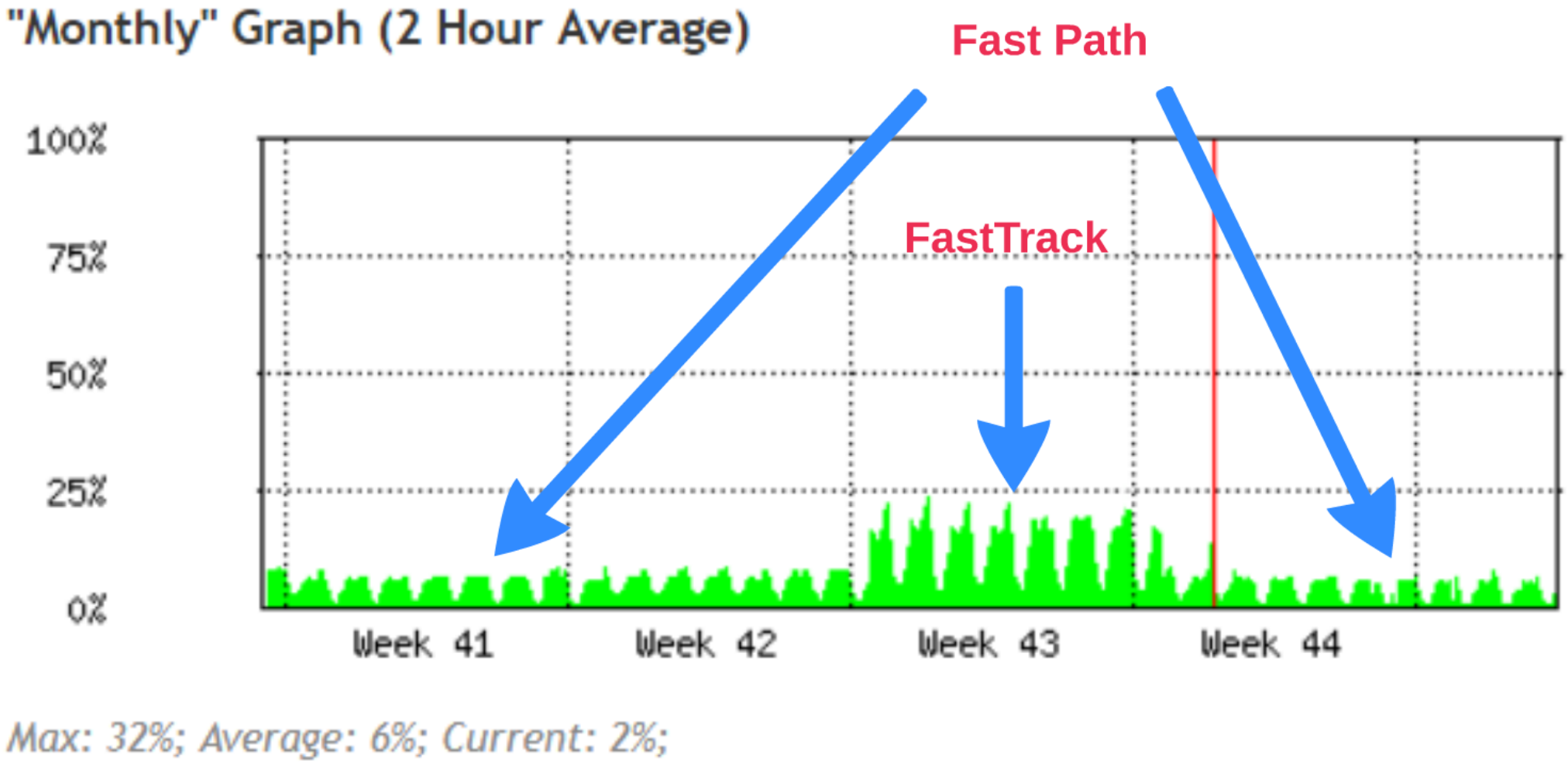


Amostra do gráfico de processamento, 2016 - ativo de borda - Hardware: RouterBoard CCR1072-1G-8S+



Amostra do gráfico em throughput acima de 5Gbps (em uma interface) - Hardware: RouterBoard CCR1072-1G-8S+


6 Gbit/s
5 Gbit/s



Uso de boas praticas + Route Server

Fonte: Autoria própria, 2017

Date: Nov/09/2017 CPU: 7% Uptime: 7d 04:16:08

Terminal

```
      rx-packets-per-second:  1 143 873
         rx-bits-per-second:    7.7Gbps
   fp-rx-packets-per-second:  1 143 873
      fp-rx-bits-per-second:    7.7Gbps
        rx-drops-per-second:          0
       rx-errors-per-second:          0
      tx-packets-per-second:  1 135 713
         tx-bits-per-second:    7.7Gbps
   fp-tx-packets-per-second:  1 143 873
      fp-tx-bits-per-second:    7.7Gbps
        tx-drops-per-second:          0
       tx-errors-per-second:          0
-- [Q quit|D dump|C-z pause]
```

Referências Bibliográficas:

- http://nic.br/
- https://wiki.mikrotik.com
- https://cert.br
- http://www.rfc-editor.org/info/rfc1918
- http://www.team-cymru.org/
- https://tools.ietf.org/html/bcp194
- *Artigo: "BOAS PRÁTICAS EM ROTEAMENTO DE BORDA PARA SISTEMAS AUTONOMOS PROVEDORES DE ACESSO À INTERNET EM PROCESSO DE DUAL STACK"* João Alberto B. Oliveira, 2016

Agradecimentos Especiais:

- Família
- Radar WISP
- UEG - Campus Trindade-GO
- NIC.br

Profissionais:

Francisco Neto (Redes Brasil)

Lacier Dias (Solintel)

Wardner Maia (MD Brasil)

Dúvidas?

?

Obrigado!

MUM MIKROTIK USER MEETING

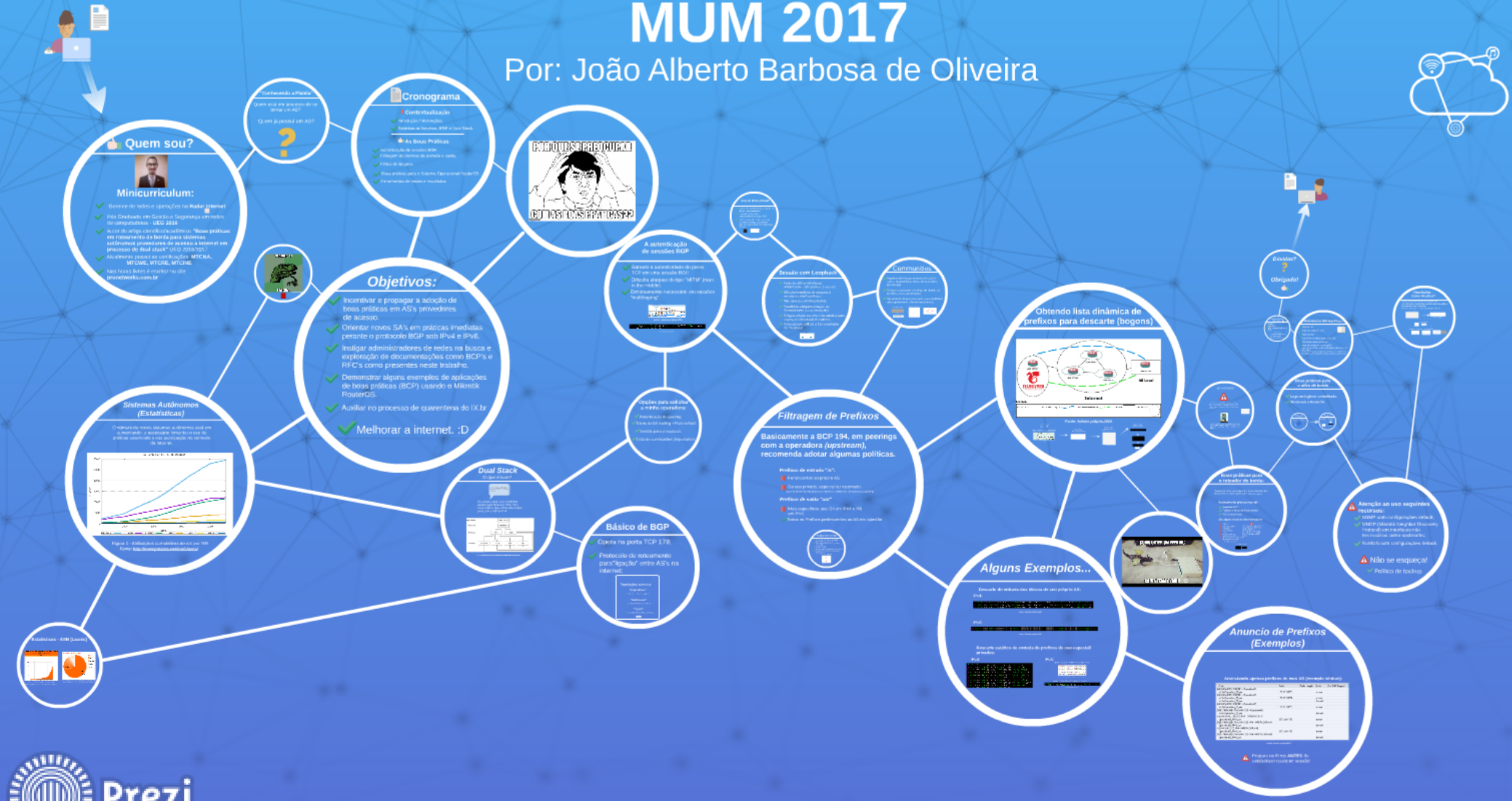
Radar INTERNET BANDA LARGA

MUM MIKROTIK USER MEETING

"BOAS PRÁTICAS EM ROTEAMENTO DE BORDA PARA NOVOS SISTEMAS AUTONOMOS PROVEDORES DE ACESSO À INTERNET"

MUM 2017

Por: João Alberto Barbosa de Oliveira



Prezi