

IX Fórum 16



28 de Outubro de 2022 - São Paulo

Templates configurações

Ligações a IXPs


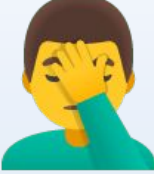


Principais vendedores de routers

Douglas Fernando Fischer

- Engenheiro de Controle e Automação
- Atua na área de redes de telecomunicações desde 1999  
- Trabalhou como engenheiro de pré-vendas e implantação em integradores de tecnologia
- Consultor na área de redes e servidores nos segmentos corporativo e de provedores de Internet
- Tretista com objetivos produtivos nas horas vagas
 - “O segredo de aborrecer é dizer tudo.” Voltaire
- BPF – <http://brasilpeeringforum.org/>
- Made4it - <http://www.made4it.com.br/>



Disclaimer

- Eu falo muitos palavrões!  
- Eles são direcionados a quem está fazendo coisa errada.
 - Se você está fazendo coisa errada:
 - Te mexa! Arrume isso logo!  
 - Se você não está fazendo coisa errada:
 - #FicaEmPaz e me ajude a conscientizar os aBiguinhos.
- Peço desculpas antecipadamente.
- Se observarem que estou fazendo coisa errada, POR FAVOR, me ajudem a corrigir e melhorar.

Sobre o que vamos falar?

- Importação e exportação de rotas para os Route-Servers do IXP
- Proteger a sua caixa
- Prepare sua caixa para falar com tanta gente no mesmo barramento
- Não fazer tanto barulho com ARP e ND
- Não soltar sujeira no ATM do IXP

Motivações para essa apresentação?

- Critérios de bom comportamento para participantes de IXPs

GTER [Mail-List](#)

LACNOG [PDF](#) [Vídeo](#)

- Aumentar Local-Pref e anunciar mais específico é GO-HORSE

GTER [Mail-List](#)

LACNOG [PDF](#) [Vídeo](#)

Sobre o que vamos falar?

- **Importação e exportação de rotas para os Route-Servers do IXP**
- Proteger a sua caixa
- Prepare sua caixa para falar com tanta gente no mesmo barramento
- Não fazer tanto barulho com ARP e ND
- Não soltar sujeira no ATM do IXP

Algumas fontes sobre Melhores Práticas

- <https://bgpfilterguide.nlnog.net/>
- <https://www.manrs.org/netops/guide/>
- <https://cursoseventos.nic.br/curso/curso-bcop-ead/>

Metodologias de filtragem de rotas

- Blacklist

- a. Exceções

- Rotas que seriam negadas na sequência, mas se deseja aceitar por motivos especiais

- b. Nega todos os tipos de rota que não se deseja rejeitar

- c. Permite/Aceita todo o resto

- Whitelist

- a. Exceções

- Rotas que seriam permitidas na sequência, mas se deseja rejeitar por motivos especiais

- b. Permite/Aceita estritamente as rotas que se deseja aceitar

- c. Nega/Rejeita todo o resto

Communities, communities, communities!



Communities, communities, communities!

- Comunidad BGP, el atributo olvidado - Tomás Lynch
LACNOG 2022 [PDF](#) [Vídeo](#)
- Todo IXP ou Fornecedor de trânsito que se preze tem communities
 - Informativas
 - Engenharia de tráfego
- Se você não marca com communities as suas rotas
 - Aprendidas ou Originadas, você está fazendo M...
 - Se você exagerar nas communities, vai estar fazendo M...

Communities, communities, communities!

Marque com communities TODAS as suas rotas BGP vindas de todos os lugares em que você as aprende ou origina:

- Originadas (Networks, ou redistribute)
 - B-RAS
 - Agregação (Talvez coincida com Border)
 - CGNAT
- Aprendidas (Import)
 - Sessão BGP com Upstream
 - Sessão BGP com Downstream
 - Sessão BGP com Parceiros de Peering (PNI - SFI)
 - Sessão BGP com Route-Server IXPs

Communities - Exemplo TOSCO

Não copie esse... Estude, planeje, e crie o seu...

Tipo de Rota	Community
Rotas Próprias	65100:65108
Rotas Aprendidas de Downstream - Cliente de Trânsito	65100:65107
Rotas Aprendidas de Parceiro de Peering - PNI	65100:65106
Rotas Aprendidas de Parceiro de Peering - Bilateral Sobre IXP	65100:65105
Rotas Aprendidas de Route-Server de IXP	65100:65104
Rotas Aprendidas de Upstream - Fornecedor de Trânsito	65100:65101
Redistribute Blackhole	65100:666

Qual metodologia de filtragem usar em que condição?

Tipo de Peer	AS Cone Definido?	Tipo de Filtro a ser usado			
		Importação (in)		Exportação (out)	
iBGP - Rotas Originadas	N/A	Whitelist	Prefix-List	N/A	
iBGP - Vizinhança	N/A	Whitelist	Communities	Whitelist	Communities
Cientes de trânsito Downstreams	Sim	Whitelist	Prefix-List ASN Origin	Whitelist	Communities
Parceiros de Peering (PNI, SFI, etc)	Sim	Whitelist	Prefix-List ASN Origin	Whitelist	Communities
	Não	Blacklist	Varios Critérios	Whitelist	Communities
Fornecedores de trânsito Upstreams	Não	Blacklist	Varios Critérios	Whitelist	Communities
Route-Servers de IXP	Não	Blacklist	Varios Critérios	Whitelist	Communities

Filtros Exportação para Route-Servers de IXP

- Se tiver community de:
 - Rotas Próprias - 65100:65108
 - > Accept
 - Rotas Aprendidas de Downstream - 65100:65107
 - > Accept
- Rotas Próprias - 65100:65108 e e redistribute BlackHole - 65100:666
 - > Aplique community 65535:666 e Accept

Filtros Importação para Route-Servers de IXP

- Validar RPKI
- O que devemos rejeitar?
 - Rejeitar Prefixos:
 - Máscaras Muito Curtas ou Muito Longas
 - Redes Bogons
 - LAN de IXPs
 - Rejeitar AS-Path:
 - Que contenham ASN Bogons
 - Que contenham ASN Tier1
 - Muito Longo (>50)
 - Com muitos prepends(>20)
 - Rejeitar clientes de trânsito (IRR):
 - Regex Community do Peer marcada pelo IXP
 - Regex AS-Path

Filtros Importação para Route-Servers de IXP

- E na hora de aceitar?
 - Aplique **Local-Pref** igual de **Trânsito** e **Accept**

Filtros Importação para Route-Servers de IXP

- E se eu quiser aprimorar?

As Communities são suas amigas! Converse com elas!

- Se Tiver Community de Peer com Loss > 10% 26162:64674
 - Reject
- Se Tiver Community de Peer com Latência < 10 ms (26162:64661)
 - Aplique **Local-Pref = (Trânsito + 20)** e Accept
- Se Tiver Community de Peer com Latência > 250 ms (26162:64667)
 - Aplique **Local-Pref = (Trânsito - 20)** e Accept

- Aplique **Local-Pref igual de Trânsito** e Accept

Sobre o que vamos falar?

- Importação e exportação de rotas para os Route-Servers do IXP
- **Proteger a sua caixa**
- Prepare sua caixa para falar com tanta gente no mesmo barramento
- Não fazer tanto barulho com ARP e ND
- Não soltar sujeira no ATM do IXP

Proteja a sua caixa!

- Fazer do jeito TOP?
 - VRF de gerência
- Pelo Menos o Básico?
 - Prefix-List de origens de acesso de gerência
 - SNMP, Telnet, SSH, HTTP, Winbox, API, NTP.
- Mikrotik
 - [Script RouterOS SetIPServicesAddressByAddressList.rsc](#)

Sobre o que vamos falar?

- Importação e exportação de rotas para os Route-Servers do IXP
- Proteger a sua caixa
- **Prepare sua caixa para falar com tanta gente no mesmo barramento**
- **Não fazer tanto barulho com ARP e ND**
- Não soltar sujeira no ATM do IXP

Preparar para muitos amigos - Não fazer tanto barulho

- Mikrotik - Max-Entry dos protocolos

```
/ip settings set max-neighbor-entries=4096
```

```
/ipv6 settings set max-neighbor-entries=4096
```

- Mikrotik - ARP-Timeout

- Aplicar no Global

```
/ip settings set arp-timeout=4h
```

- Aplicar por interface

```
/interface vlan set [ find default-name=ether1.4 ] arp-timeout=4h
```

Preparar para muitos amigos - Não fazer tanto barulho

- Juniper - CPU Protection

- Criar o policer

```
set firewall policer limite_arp_ix.br-sp if-exceeding bandwidth-limit 2m
```

```
set firewall policer limite_arp_ix.br-sp if-exceeding burst-size-limit 256k
```

```
set firewall policer limite_arp_ix.br-sp then discard
```

- Aplicar por interface

```
set interfaces <interface> unit <unit> family inet policer arp limite_arp_ix.br-sp
```

- Juniper - ARP-Timeout

- Aplicar no Global

```
set system arp aging-timer 240
```

Preparar para muitos amigos - Não fazer tanto barulho

- Huawei - Max-Entry e ARP Timeout

- Aplicar por interface

```
interface XGigabitEthernet0/0/1.4
```

```
arp expire-time 14400
```

```
arp-limit maximum 4096
```

```
arp rate-limit 0
```

- Huawei - CPU-Protection

```
cpu-defend policy 3
```

```
car arp cir 4096
```

```
car ns cir 2048
```

```
slot 3
```

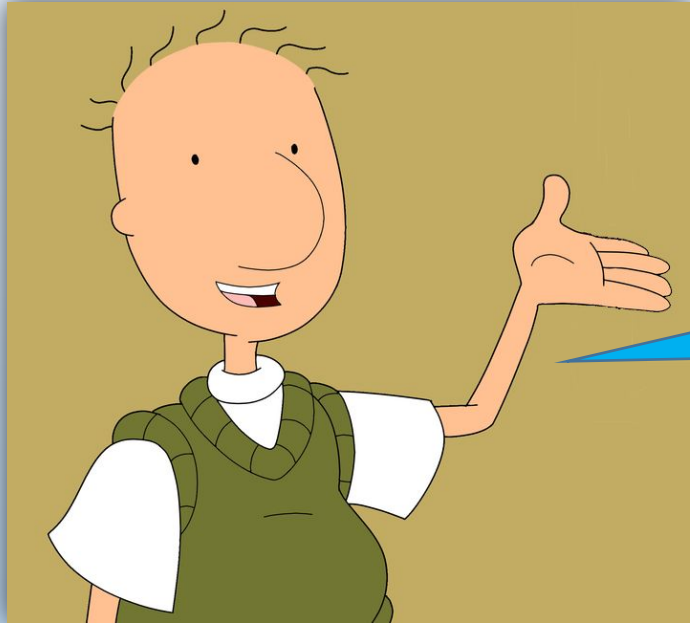
```
cpu-defend-policy 3
```

Sobre o que vamos falar?

- Importação e exportação de rotas para os Route-Servers do IXP
- Proteger a sua caixa
- Prepare sua caixa para falar com tanta gente no mesmo barramento
- Não fazer tanto barulho com ARP e ND
- **Não soltar sujeira no ATM do IXP**

O que poderia ser chamado de “sujeira” num IXP?

- Discovery Protocol (CDP, MNDP, LLDP, etc)
- OSPF, ISIS, RIP, EIGRP
- PPPoE - PADI(Client), PADO(Server)
- DHCP IPv4 e IPv6 - Discover(Client), Offer(Server/Relay)
- ARP Gratuito
- **Proxy ARP, Proxy-ND**
- **IPv6 RA**
- IPv4 na Vlan de IPv6, IPv6 na Vlan de IPv4
- Endereço IP secundário fora da faixa da LAN do IXP



Perguntas?
Sugestões?

“Você tem que ser o que você realmente é.

Pois se você não for quem você é, afinal quem é você?”

Doug Funnie