IX Fórum Regional 54

1 Novembro de 2024 - Cascavel - Paraná

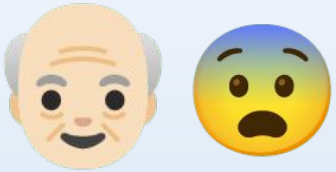
Abuso de tráfego em um IXP:
Como acontece e como se proteger

Autor: Douglas Fernando Fischer – fischerdouglas@gmail.com

Intenções dessa apresentação?

- Visão for Dummies do que é um IXP
- Exemplo de como o tráfego Abusivo pode acontecer através de IXPs.
  - Cold Potato, Hot Potato, “Why am I carrying this potato?”
- Exemplo de como proteger-se de desse tipo de tráfego abusivo
- Perguntas e comentários sarcásticos com objetivos pedagógicos

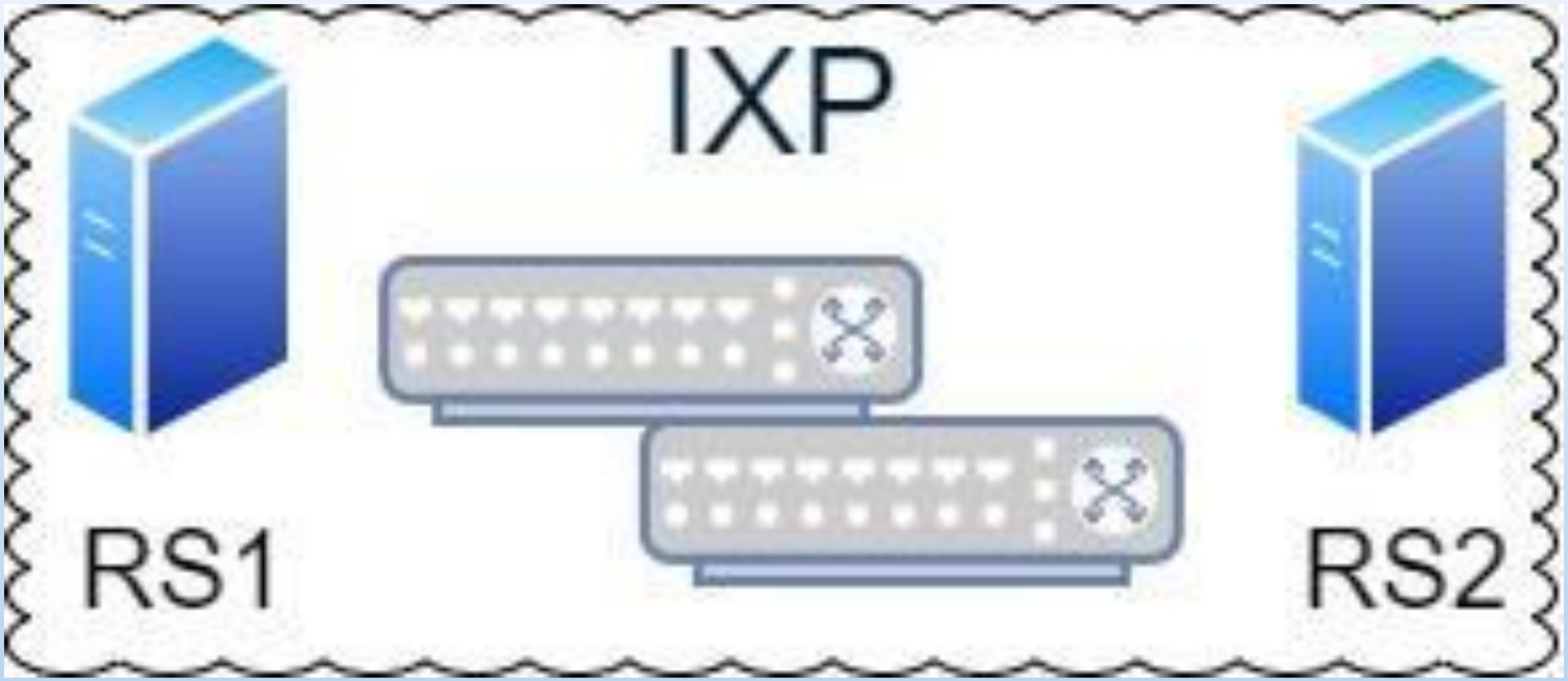
Douglas Fernando Fischer

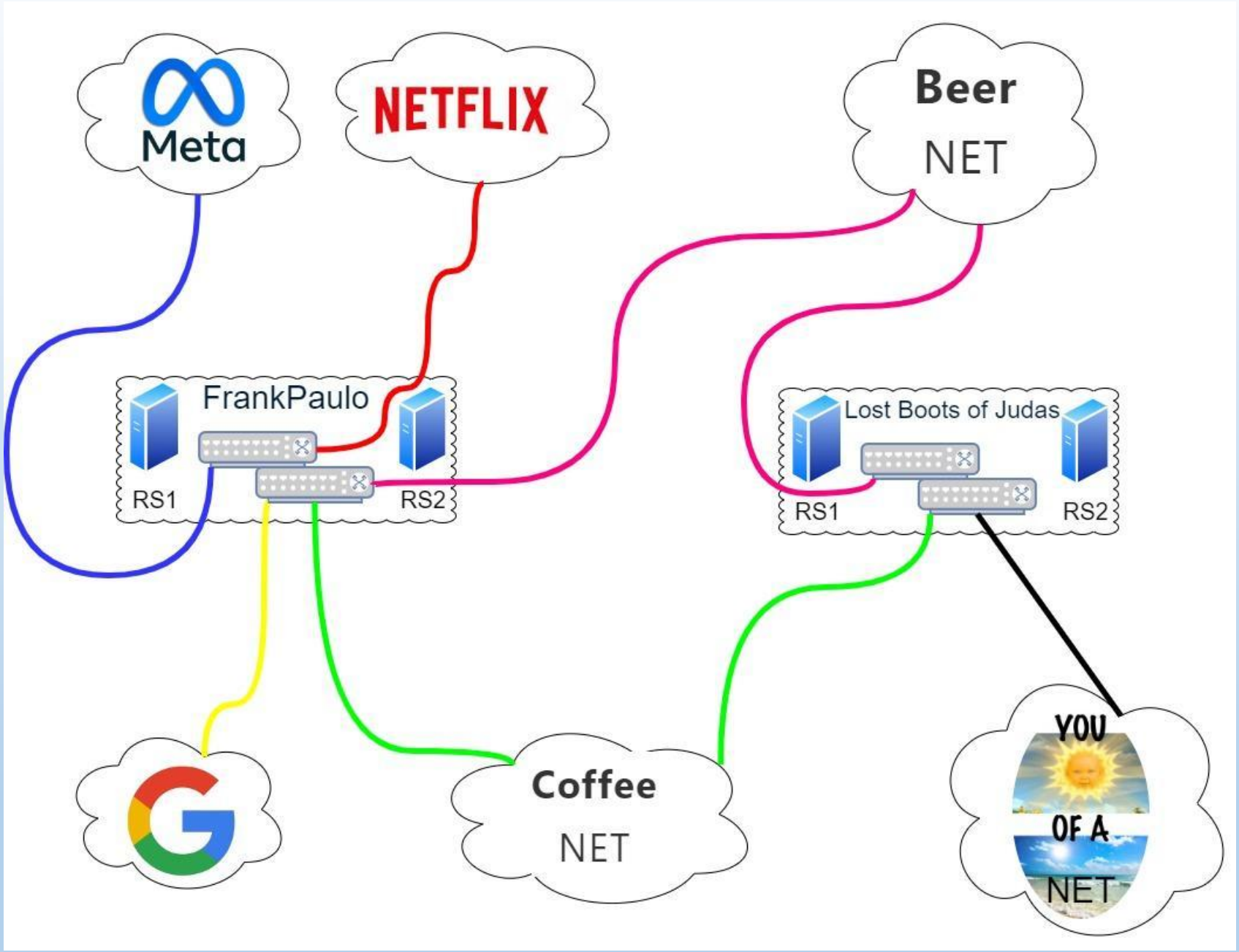
- Engenheiro de Controle e Automação
- Atua na área de redes de telecomunicações desde 1999 - 
- Trabalhou como engenheiro de pré-vendas e implantação em integradores de tecnologia
- Consultor na área de redes e servidores no segmento corporativo e provedores de Internet
- Tretísta com fins produtivos nas horas vagas
  - “O segredo de aborrecer é dizer tudo.” Voltaire

- BPF – http://brasilpeeringforum.org/

Intenções dessa apresentação?

- Visão for Dummies do que é um IXP
- Exemplo de como o tráfego Abusivo pode acontecer através de IXPs.
  - Cold Potato, Hot Potato, “Why am I carrying this potato?”
- Exemplo de como proteger-se de desse tipo de tráfego abusivo
- Perguntas e comentários sarcásticos com objetivos pedagógicos


IXP
RS1
RS2


Meta
NETFLIX
Beer
NET
FrankPaulo
RS1
RS2
Lost Boots of Judas
RS1
RS2
Coffee
NET
YOU
OF A
NET

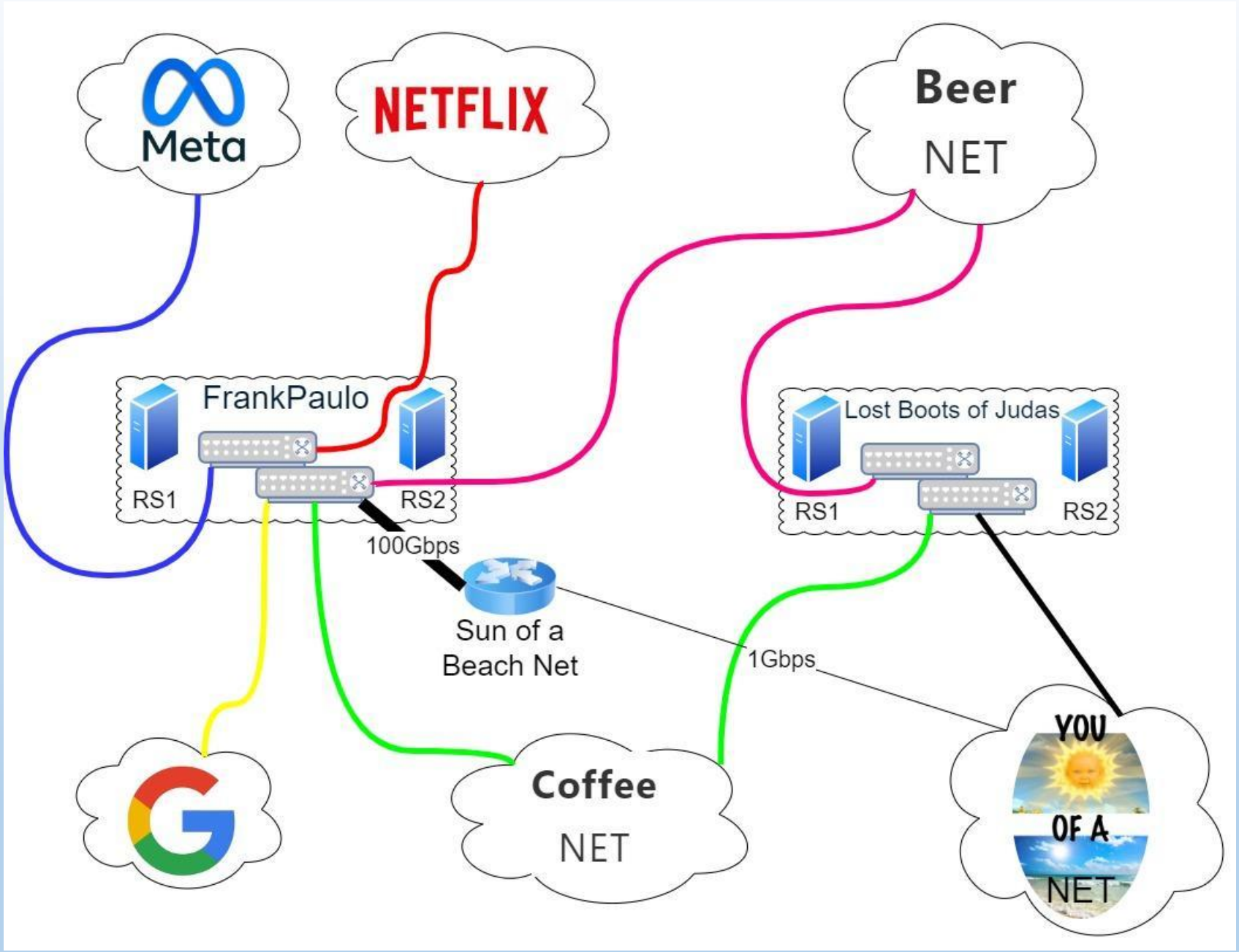
Intenções dessa apresentação?

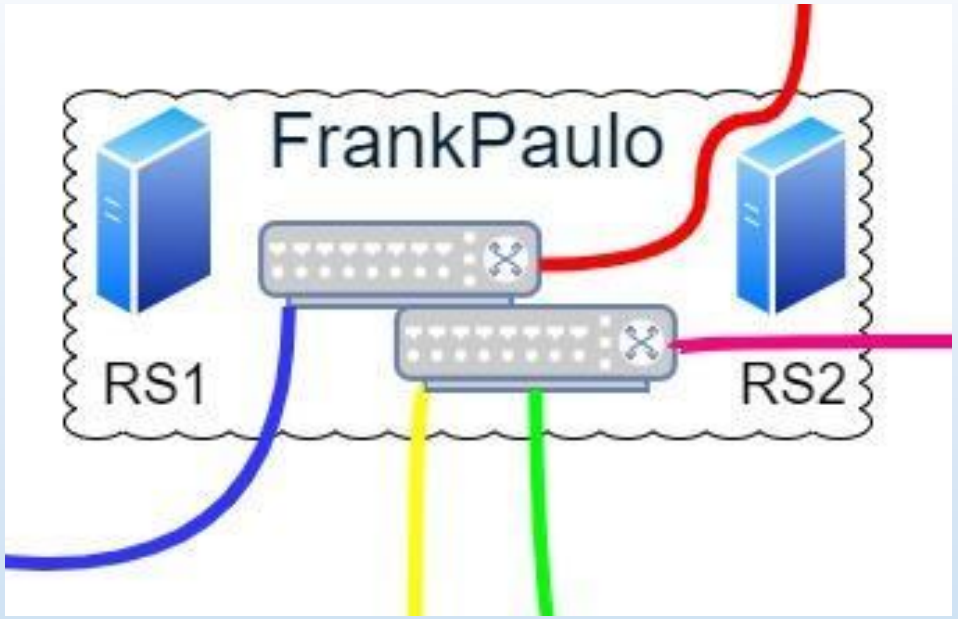
- Visão for Dummies do que é um IXP

- Exemplo de como o tráfego Abusivo pode acontecer através de IXPs.
  - Cold Potato, Hot Potato, “Why am I carrying this potato?”

- Exemplo de como proteger-se de desse tipo de tráfego abusivo

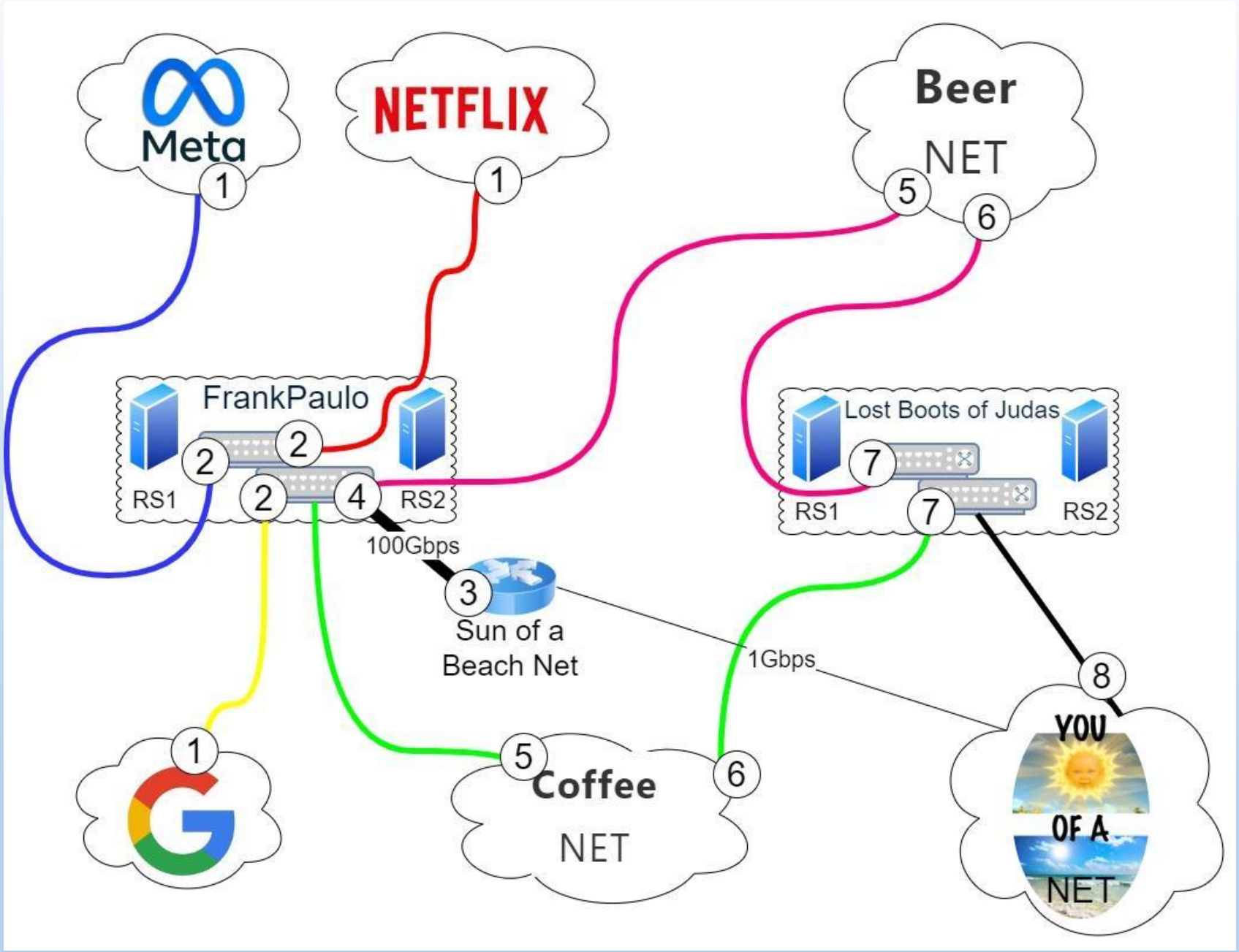
- Perguntas e comentários sarcásticos com objetivos pedagógicos


Meta
NETFLIX
Beer
NET
FrankPaulo
RS1
RS2
100Gbps
Lost Boots of Judas
RS1
RS2
Sun of a
Beach Net
1Gbps
Coffee
NET
YOU
OF A
NET



Receita de como fazer safadeza

- Router de “Lost Boots of Judas” da “Sun of a Beach Net” ensina via Route-Servers do IXP de “Lost Boots of Judas” as suas rotas para Beer Net e Coffee Net
  - Rotas da SunOfABeach estão na FIB da Beer Net e da Coffee Net
- Router de “FrankPaulo” da “Sun of a Beach Net” aprende por iBGP as rotas dos pacotes que ele deveria entregar para “Lost Boots of Judas”
  - Na routing-policy desse iBGP aplica set ip next-hop apontando para os IPs da LAN do IXP de “FrankPaulo” que são da “Beer Net” e da “Coffee Net”.
- Router de “FrankPaulo” ensina para Route-Servers(eBGP) as suas rotas, com seus próprio IP da LAN do IXP de “FrankPaulo”.
  - Aplica community de seletive-no-export para “Beer Net” e para “Coffee Net”.
  - Routers das OTTs aprendem que devem mandar para Router de “FrankPaulo” os pacotes com destino à “Sun of a Beach Net”


Meta
1
NETFLIX
1
Beer
NET
5
6
FrankPaulo
RS1
2
2
2
2
4
RS2
100Gbps
3
Sun of a
Beach Net
Lost Boots of Judas
RS1
7
7
RS2
1Gbps
8
1
5
Coffee
NET
6
YOU
OF A
NET

Intenções dessa apresentação?

- Visão for Dummies do que é um IXP
- Exemplo de como o tráfego Abusivo pode acontecer através de IXPs.
  - Cold Potato, Hot Potato, “Why am I carrying this potato?”
- Exemplo de como proteger-se de desse tipo de tráfego abusivo
- Perguntas e comentários sarcásticos com objetivos pedagógicos

Como proteger-se de desse tipo de tráfego abusivo em IXP?

- Não ficar cego sobre o que passa na sua rede!
  - Netflow, IPFIX, sFlow, etc…
  - Analisadores de Flow.
- Implementar mecanismos de bloqueio de tráfego abusivo!
  - Controlplane
    - Filtrar rotas indesejáveis
  - Data Plane
    - Filter-Policy (ACL)
    - Flowspec
    - Qos Policy Propagation via BGP / Destination Class Policing

Como proteger-se de desse tipo de tráfego abusivo em IXP?

NIC.BR - GTER 27 - 2009

QPPB - Qos Policy Propagation via BGP

https://www.linkedin.com/in/analuciadefaria/

https://ftp.registro.br/pub/gter/gter27/02-ControlandoTrafegoTransito.pdf

https://ftp.registro.br/pub/gter/gter27/videos/mp4/gter-02-controlando_trafego_de_transito_em_um_as.mp4

Detalhamento da Solução via QPPB

- **Configuração do Roteador**

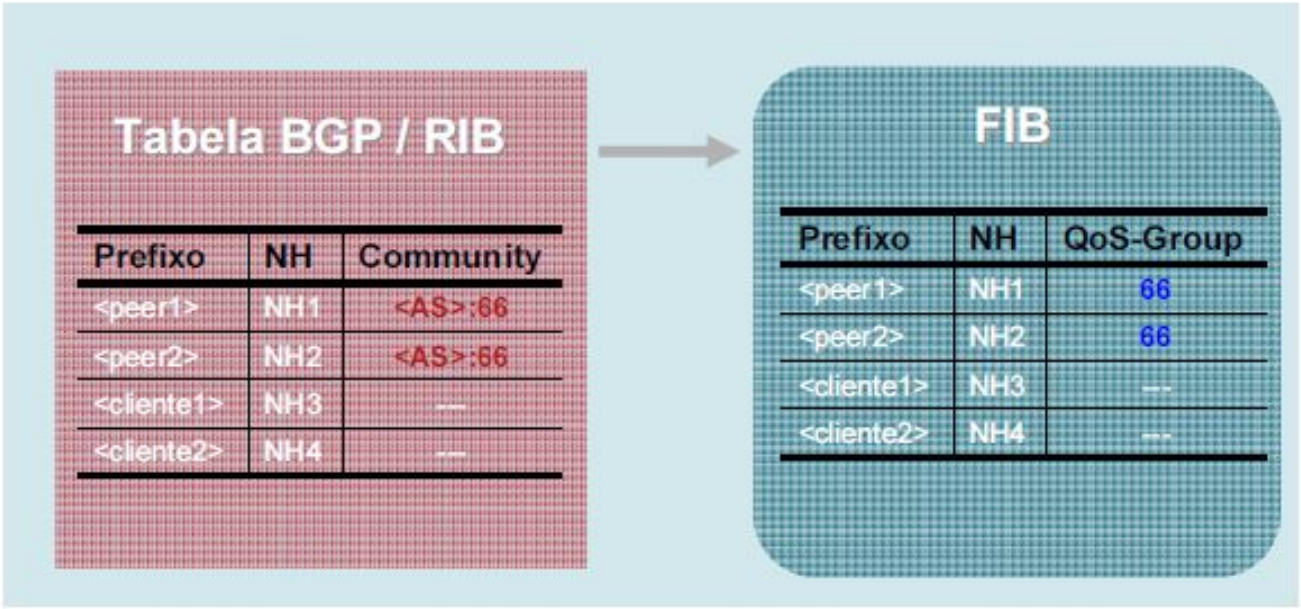
1. Associação de TAG ao prefixo na FIB via BGP
   IOS CLI **table-map**

2. Associação de TAG a pacote recebido no roteador via QPPB
   IOS CLI **bgp-policy**

3. Classificação e descarte de pacote via QoS
   IOS CLI **service-policy**

https://ftp.registro.br/pub/gter/gter27/02-ControlandoTrafegoTransito.pdf

(1) Associação de TAG na FIB via BGP

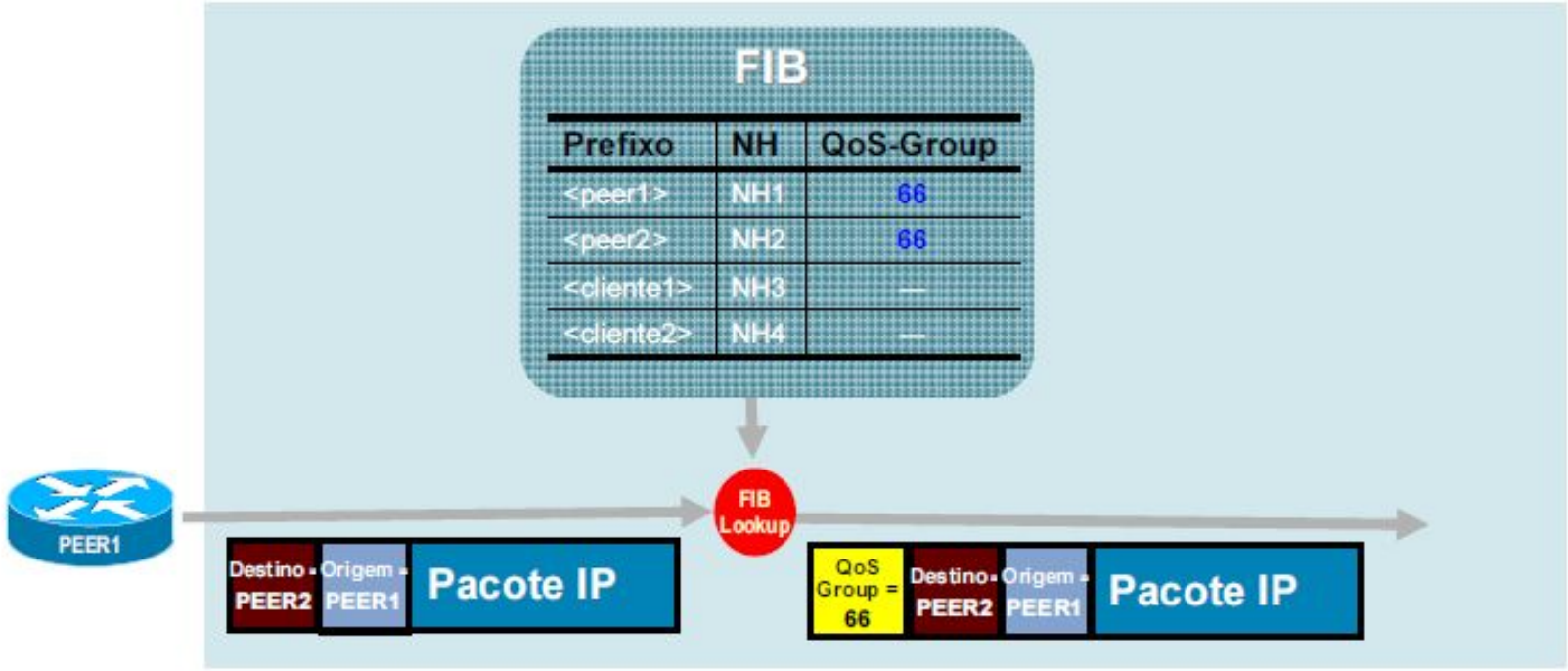



```
!
ip bgp-community new-format
router bgp <AS>
  :
  table-map set-prefix-type
```

```
!
ip community-list 1 permit <AS>:66
!
route-map set-prefix-type permit 10
  match community 1
  set ip qos-group 66
!
```

https://ftp.registro.br/pub/gter/gter27/02-ControlandoTrafegoTransito.pdf

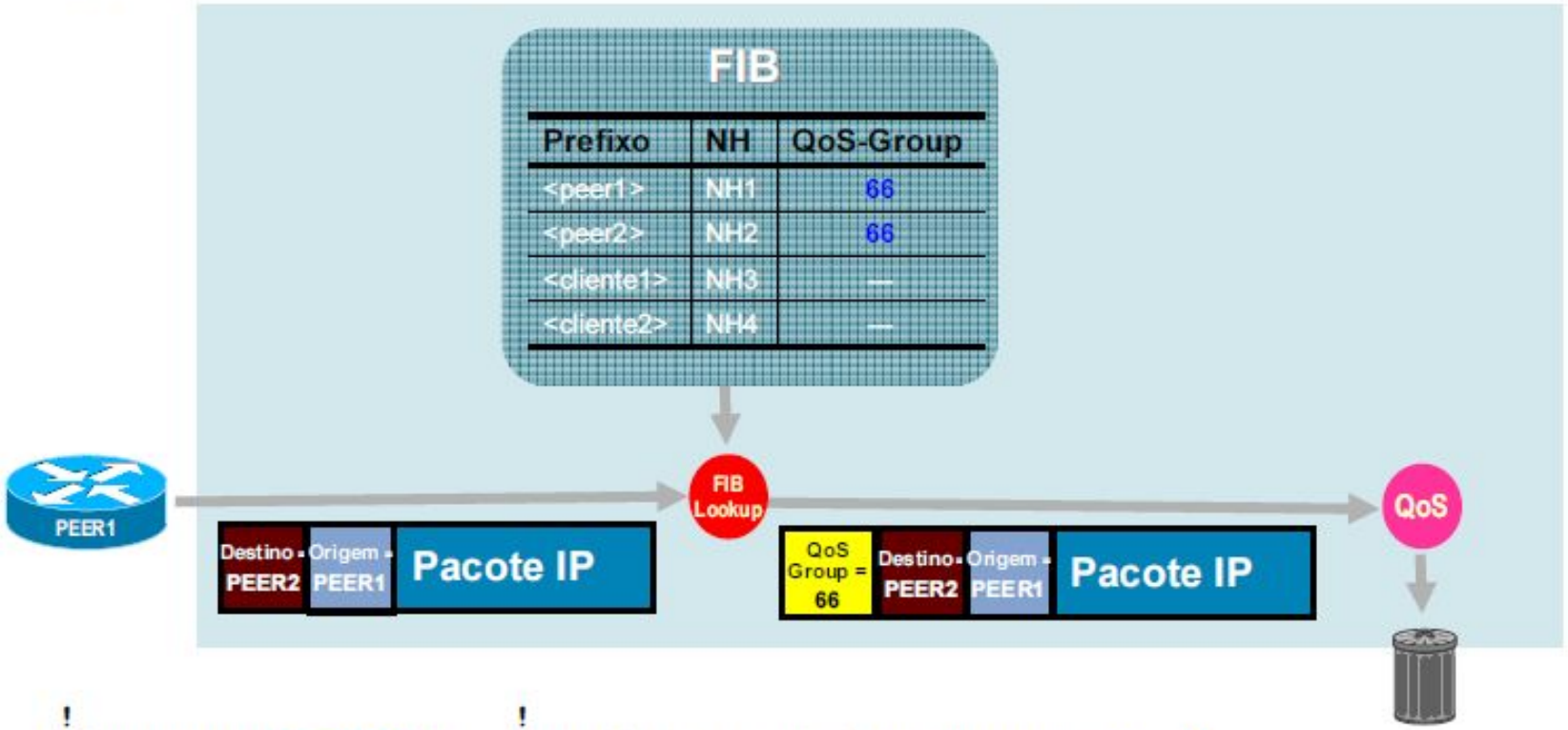
(2) Associação de TAG a pacote via QPPB




```
!
interface <ID da interface com Peer1>
  description Interface conectada ao Peer1
  bgp-policy destination ip-qos-map
```

https://ftp.registro.br/pub/gter/gter27/02-ControlandoTrafegoTransito.pdf

(3) Classificação e descarte de pacote via QoS




```
!
class-map peer-prefix
  match qos-group 66
!
policy peer-in
  class peer-prefix
    drop
```

```
!
interface <ID da interface com Peer1>
  description Interface conectada ao Peer1
  bgp-policy destination ip-qos-map
  service-policy input peer-in
```

https://ftp.registro.br/pub/gter/gter27/02-ControlandoTrafegoTransito.pdf

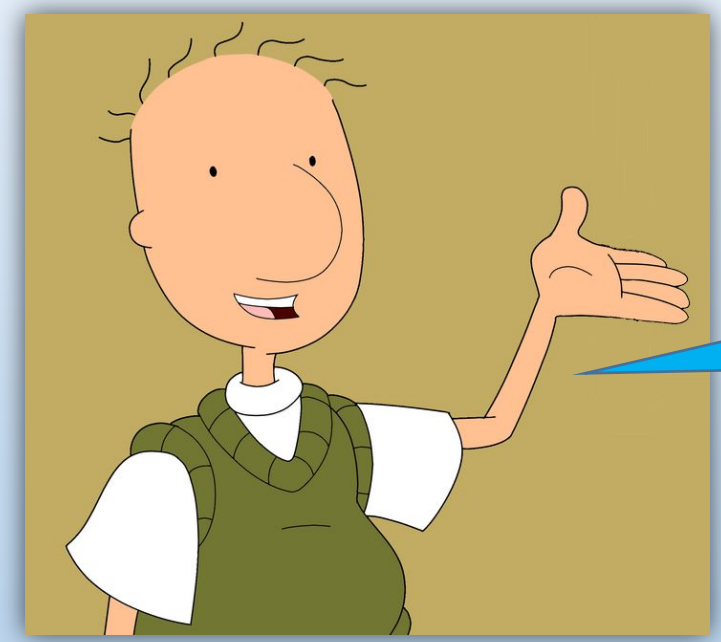
Benefícios da Técnica Proposta

- **Protege contra violações da política de *peering* BGP**
  - Tráfego recebido de um *peer* e destinado a outro *peer* (local ou remoto) é descartado
  - Tráfego recebido de um *peer* e destinado a um cliente é encaminhado normalmente
- **Facilidade operacional**
  - Não são necessárias listas de acesso
  - Associação de TAG na FIB (prefixos de *peers* versus prefixos de clientes) é possível através de política BGP padrão
  - Mudanças na política BGP são refletidas automaticamente no *data plane*
  - Política QoS permite monitoração e registro de violações da política de *peering*
- **Técnica complementa outras aplicações do plano de controle BGP como RTBH**

https://ftp.registro.br/pub/gter/gter27/02-ControlandoTrafegoTransito.pdf

Intenções dessa apresentação?

- Visão for Dummies do que é um IXP
- Exemplo de como o tráfego Abusivo pode acontecer através de IXPs.
  - Cold Potato, Hot Potato, “Why am I carrying this potato?”
- Exemplo de como proteger-se de desse tipo de tráfego abusivo
- Perguntas e comentários sarcásticos com objetivos pedagógicos



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