

The background of the entire image is a dark grey circuit board pattern with white lines representing traces and components. In the center, there is a white horizontal band containing the logos and text.

**nic.br** **egi.br**

Núcleo de Informação  
e Coordenação do  
Ponto BR

Comitê Gestor da  
Internet no Brasil

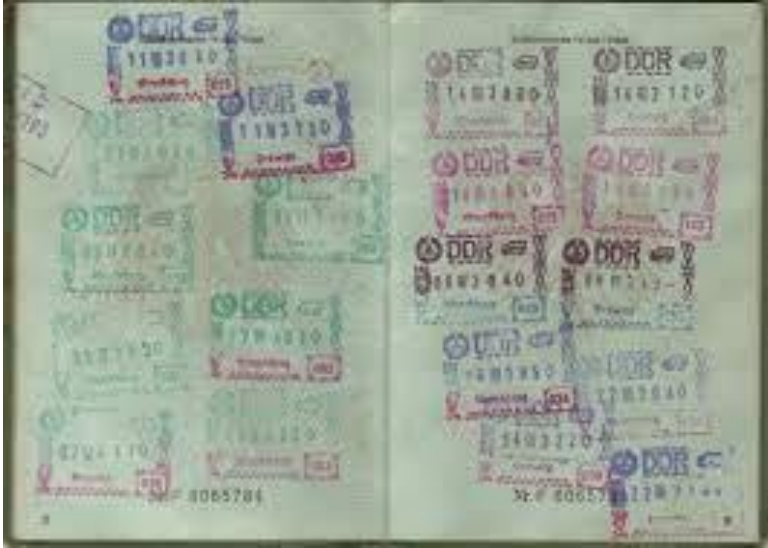
**registro.br** **cert.br** **cetic.br** **ceptro.br** **ceweb.br** **ix.br**

# Communities BGP: como melhorar a segurança e a gestão das redes

Eduardo Barasal Morales

ceptro.br nic.br cgi.br

# O que são communities?



# O que são communities?

- Tudo que é feito com communities pode ser feito de outra forma.
- Communities auxiliam os administradores de rede
- Facilitam as configurações de rede

Função de loop

```
int i;  
for (i=0; i <= 2; i++) {  
    if (i == 2) {  
        x = 3; } }
```

Pode ser feita com as funções if e else de

```
int i = 0;  
if ( i == 2) {}  
else {  
    i++; }  
if ( i == 2) {}  
else {  
    i++; }  
...  
if ( i == 2) {  
    x=3; }
```

# Entendendo o BGP

# O que é o BGP

- Protocolo de Roteamento usado para trocar informações sobre caminhos entre diferentes redes (ASes diferentes)
- O BGP é um protocolo do tipo “path vector”
- Tem várias opções diferentes para implementação de políticas de tráfego
- Usado no backbone da Internet pelos ASes

# Conceitos de BGP

- BGP é um protocolo fofoqueiro!

## Minha Rota

2001:db8::/32

## Rota Recebida

2001:db8::/32 65537 65536 i



# Conceitos de BGP

- Quem conta o conto pode aumentar um ponto!

## Minha Rota

2001:db8::/32

## Rota Recebida

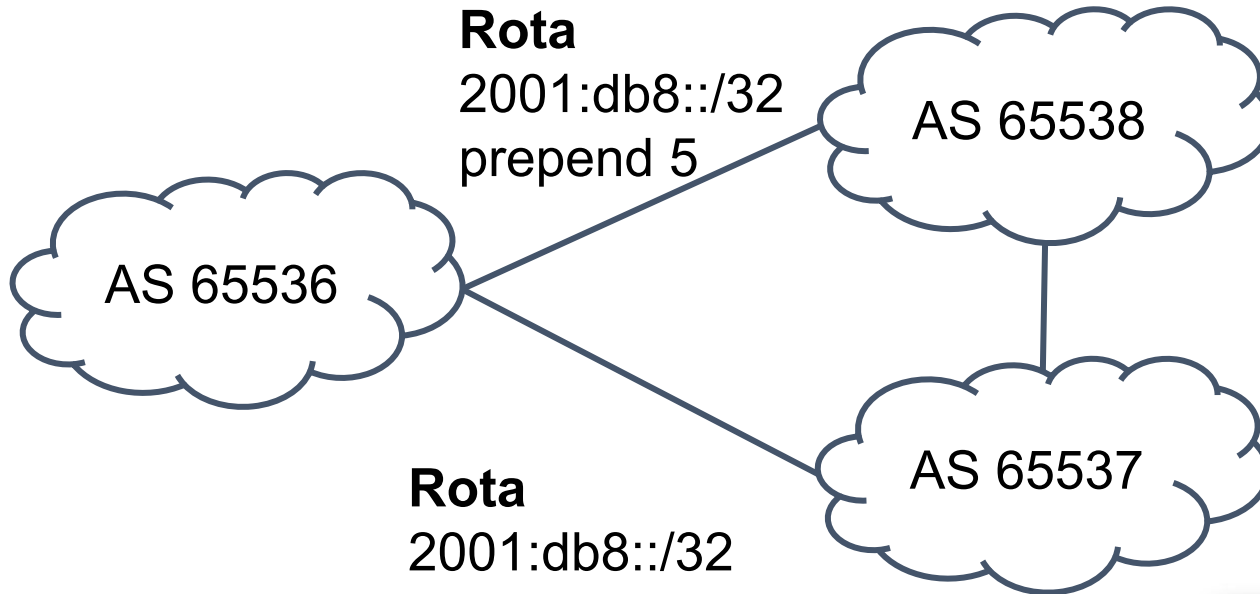
2001::/16 65537 i





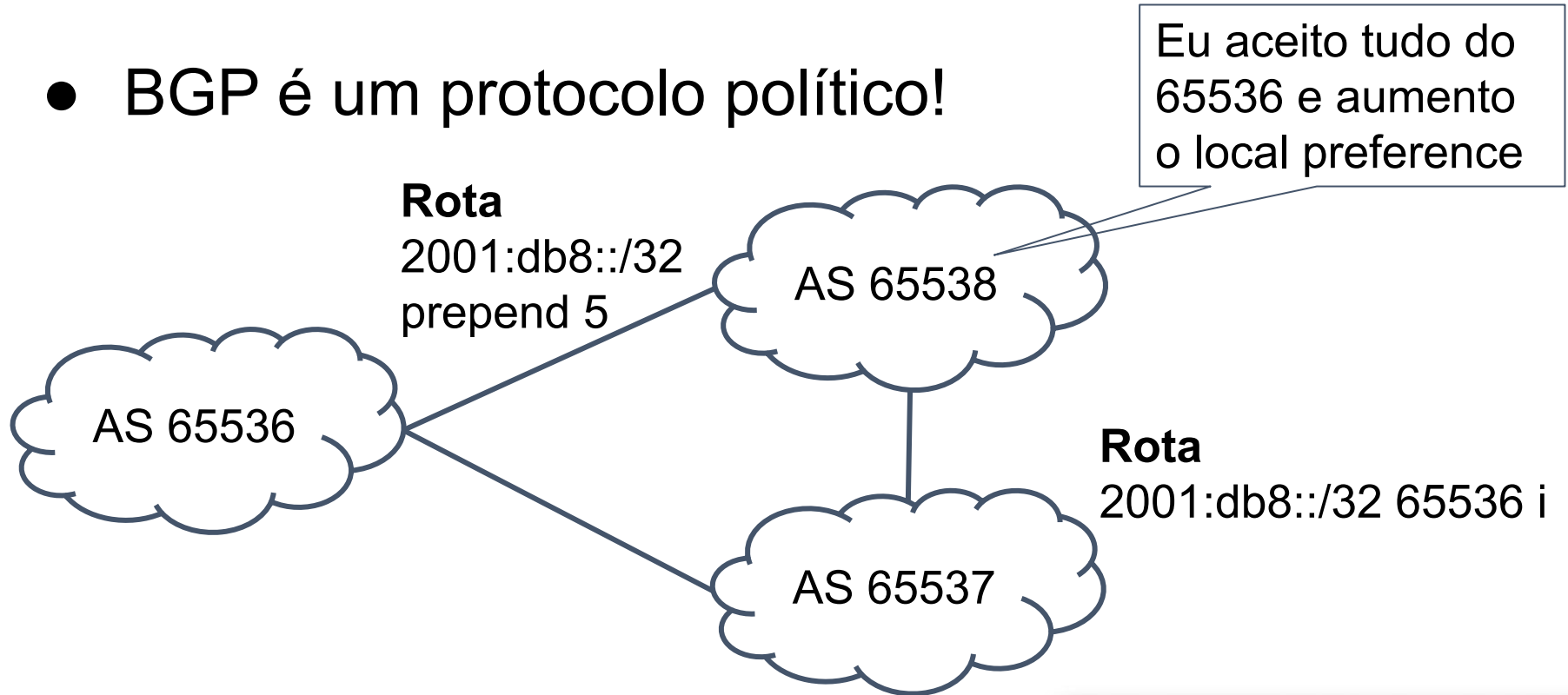
# Conceitos de BGP

- BGP é um protocolo político!



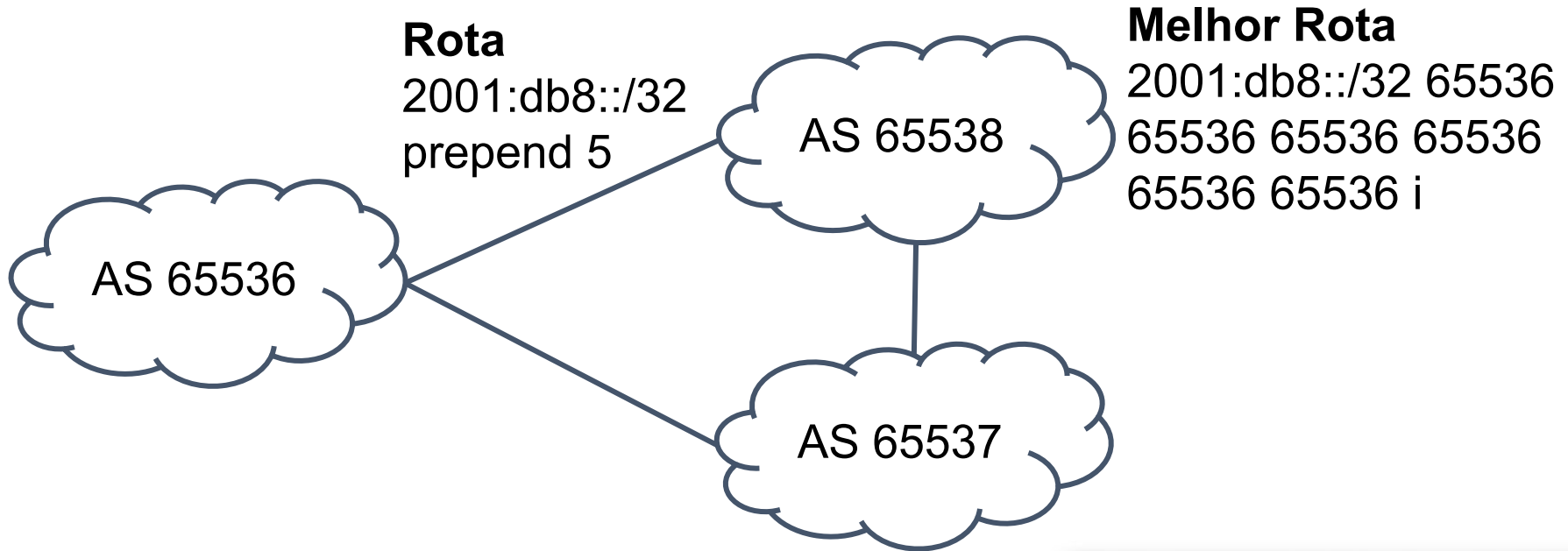
# Conceitos de BGP

- BGP é um protocolo político!



# Conceitos de BGP

- BGP é um protocolo político!



# Entendendo o BGP

- É importante sempre conversar com outros sistemas autônomos.
- Não adianta configurar e largar!
- Precisa monitorar e entender que seu funcionamento depende de todos.

# Communities

# Communities

- Atributo adicionado a rota no BGP
- Transitivo e Opcional
- Uma rota pode ter várias communities atreladas
- Existem 3 tipos
  - Standard Communities (ou regular)
  - Extended Communities
  - Large Communities

# Standard Communities

- Definido na RFC1997 (ano de 1996) - mais antigo
- Amplamente utilizado!
- Número de 32 bits (integer)
  - 2 campos de 2 octetos
  - Formato
    - 16 bits : 16 bits
  - Para evitar repetições
    - Primeiros 16 bits normalmente são ASNs
    - Número de AS : Número de Community
    - E quando o ASN tem 32 bits?

# Extended Communities

- Definido na RFC4360 (ano de 2006)
- Número de 64 bits (integer)
  - 1 ou 2 octetos para identificar o Tipo
    - Tipos registrados pela IANA
    - <https://www.iana.org/assignments/bgp-extended-communities/bgp-extended-communities.xhtml>
  - Formato diversos
    - (Tipo)16 bits : (ASN) 16 bits : (Local) 32 bits
    - (Tipo)16 bits : (IPv4) 32 bits : (Local) 16 bits
    - (Tipo)16 bits : (Local) 48bits



# Large Communities

- Definido na RFC8092 (ano de 2017) - novo
- Crescendo em implantação.
- Número de 96 bits (integer)
  - 3 campos de 4 octetos
  - Formato
    - 32 bits : 32 bits : 32 bits
    - ASN : Função : Parâmetro
      - Comum - Meu ASN : Ação : outro ASN

# Como usar Communities?

- Duas categorias
  - **Marcação Informativas**
    - Servem para trazer alguma referência sobre a rota
      - Ex: De que país veio a rota
  - **Marcação de Ação**
    - Servem para influenciar nas políticas de roteamento
      - Ex: aumente o local preference de determinada rota

# Communities Informativas

- Geralmente o foco em transmitir:
  - Onde a rota foi aprendida
    - Rotas continentais, nacionais, regionais ...
  - Como a rota foi aprendida
    - Trânsito, peer, cliente, interna ...
- Ela pode ser usada para tomar alguma ação
  - Por você
  - Por um trânsito
  - Por um outro

# Communities Informativas

- Não existe um padrão definido
- Cada rede faz a sua regra
- Mas seguem algumas sugestões
  - Separar os dígitos para cada ideia
    - Um dígito para geografia, outro para relacionamento
  - Pensar em dividir em 9 seções
    - 0-9 o que cabe num dígito
  - Planejar o futuro
    - Uma vez criado e divulgado pode ser difícil mudar

# Standard Communities Informativas

- Exemplo: 64500 : TCPRE
- T - Tipo de relacionamento - Trânsito, Peer, IX, cliente, interno...
- C - Continente - América, África, Europa, Ásia e Oceania
- P - País - Brasil, Argentina, Paraguai, Uruguai, Chile...
- R - Região - Sudeste, Sul, Norte, Nordeste e Centro-oeste
- E - Estado - São Paulo, Rio de Janeiro, Espírito Santo, Minas Gerais

# Standard Communities Informativas

- Exemplo: 64500 : 31524
  - T - Trânsito
  - C - América
  - P - Brasil
  - R - Sudeste
  - E - São Paulo
- 
- O mesmo pensamento pode ser passado para as extended e large communities.

# Large Communities Informativas

- Exemplo: 64500 : F : P
- Função - Como as rotas foram aprendidas
  - 1 - Código de região
  - 2 - Código de País
  - 3 - Tipo de relacionamento
- Parâmetro - informação extra que especifica a função
  - 1 : 2 rotas aprendidas da África (UNSD)
  - 2 : 076 rotas aprendidas do Brasil (ISO 3166-1)
  - 3 : 1 rotas aprendidas internamente (você decide)

# Recomendações

- Não confunda as communities Informativas com as de ação!
  - Deixe fácil de identificar cada uma delas
    - Ex: Informativas 5 dígitos e Ação 4 dígitos
- Não deixe que outros te enviem as suas communities informativas
  - Filtre elas antes que tenha problemas!



# Communities de ação

- Principais funções
  - Manipular os atributos de BGP
    - AS-PATH
    - Local-Preference
    - Multi-Exit Discriminator (MED)
    - Next-Hop Address
    - Entre outros
  - Influenciar nas rotas repassadas
    - Repassa ou não (export)

# Communities de ação

- Muitas vezes o repasse de rotas pode ser escolhido
  - Geografia
    - Não repassar as rotas internacionais
  - Relacionamento
    - Não repassar as rotas para o IX
  - Para um AS específico
    - Não repassar as rotas para o ASXXX
  - Ou outra regra que queira inventar e divulgar
    - Não deixe de publicar.

# Large Communities de Ação

- Exemplo: 64500 : F : P
- F - Função escolhida
  - 1 - No export para os vizinhos do País X (Código)
  - 2 - No export para outro ASN
  - 3 - Adiciona um prepend para o vizinho AS X
- P - informação extra que especifica a função
  - 1 : 076 não exporta para ASes do Brasil (ISO 3166-1)
  - 2 : 64501 não exporta para o AS 64501
  - 3 : 64502 adiciona um prepend para o AS 64502

# IX.br possui communities

## Traffic engineering

function	standard	extended	large
not announce to ASN	65000:dest-asn	(ro rt):65000:dest-asn	65000:0:dest-asn
export only to ASN	65001:dest-asn	(ro rt):65001:dest-asn	65001:0:dest-asn
add one prepend	64601:dest-asn	(ro rt):64601:dest-asn	64601:0:dest-asn
add two prepend	64602:dest-asn	(ro rt):64602:dest-asn	64602:0:dest-asn
add three prepend	64603:dest-asn	(ro rt):64603:dest-asn	64603:0:dest-asn
graceful shutdown	65535:0	-	-
do not announce to Afrinic (ASNs)	65002:0	(ro rt):65002:0	65002:0:0
do not announce to Apnic (ASNs)	65002:1	(ro rt):65002:1	65002:0:1
do not announce to Arin (ASNs)	65002:2	(ro rt):65002:2	65002:0:2
do not announce to Lacnic (ASNs)	65002:3	(ro rt):65002:3	65002:0:3
do not announce to Ripe (ASNs)	65002:4	(ro rt):65002:4	65002:0:4
do not announce to Brasil (ASNs)	65002:5	(ro rt):65002:5	65002:0:5
export to Afrinic (ASNs)	65003:0	(ro rt):65003:0	65003:0:0
export to Apnic (ASNs)	65003:1	(ro rt):65003:1	65003:0:1
export to Arin (ASNs)	65003:2	(ro rt):65003:2	65003:0:2
export to Lacnic (ASNs)	65003:3	(ro rt):65003:3	65003:0:3
export to Ripe (ASNs)	65003:4	(ro rt):65003:4	65003:0:4
export to Brasil (ASNs)	65003:5	(ro rt):65003:5	65003:0:5
do not announce to IXP	65004:65XXX	(ro rt):65004:65XXX	65004:0:65XXX

do not announce to rtt > 10ms	65010:10	(ro rt):65010:10	65010:0:10
do not announce to rtt > 50ms	65010:50	(ro rt):65010:50	65010:0:50
do not announce to rtt > 100ms	65010:100	(ro rt):65010:100	65010:0:100
do not announce to rtt > 150ms	65010:150	(ro rt):65010:150	65010:0:150
do not announce to rtt > 200ms	65010:200	(ro rt):65010:200	65010:0:200
do not announce to rtt > 250ms	65010:250	(ro rt):65010:250	65010:0:250
do not announce to rtt = unknown	65010:999	(ro rt):65010:999	65010:0:999
one prepend to rtt > 10ms	64611:10	(ro rt):64611:10	64611:0:10
one prepend to rtt > 50ms	64611:50	(ro rt):64611:50	64611:0:50
one prepend to rtt > 100ms	64611:100	(ro rt):64611:100	64611:0:100
one prepend to rtt > 150ms	64611:150	(ro rt):64611:150	64611:0:150
one prepend to rtt > 200ms	64611:200	(ro rt):64611:200	64611:0:200
one prepend to rtt > 250ms	64611:250	(ro rt):64611:250	64611:0:250
one prepend to rtt = unknown	64611:999	(ro rt):64611:999	64611:0:999
two prepend to rtt > 10ms	64612:10	(ro rt):64612:10	64612:0:10
two prepend to rtt > 50ms	64612:50	(ro rt):64612:50	64612:0:50
two prepend to rtt > 100ms	64612:100	(ro rt):64612:100	64612:0:100
two prepend to rtt > 150ms	64612:150	(ro rt):64612:150	64612:0:150
two prepend to rtt > 200ms	64612:200	(ro rt):64612:200	64612:0:200
two prepend to rtt > 250ms	64612:250	(ro rt):64612:250	64612:0:250
two prepend to rtt = unknown	64612:999	(ro rt):64612:999	64612:0:999

three prepend to rtt > 10ms	64613:10	(ro rt):64613:10	64613:0:10
three prepend to rtt > 50ms	64613:50	(ro rt):64613:50	64613:0:50
three prepend to rtt > 100ms	64613:100	(ro rt):64613:100	64613:0:100
three prepend to rtt > 150ms	64613:150	(ro rt):64613:150	64613:0:150
three prepend to rtt > 200ms	64613:200	(ro rt):64613:200	64613:0:200
three prepend to rtt > 250ms	64613:250	(ro rt):64613:250	64613:0:250
three prepend to rtt = unknown	64613:999	(ro rt):64613:999	64613:0:999
do not announce to loss > 2%	65011:2	(ro rt):65011:2	65011:0:2
do not announce to loss > 10%	65011:10	(ro rt):65011:10	65011:0:10
do not announce to loss = unknow	65011:999	(ro rt):65011:999	65011:0:999
one prepend to loss > 2%	64621:2	(ro rt):64621:2	64621:0:2
one prepend to loss > 10%	64621:10	(ro rt):64621:10	64621:0:10
one prepend to loss = unknown	64621:999	(ro rt):64621:999	64621:0:999
two prepend to loss > 2%	64622:2	(ro rt):64622:2	64622:0:2
two prepend to loss > 10%	64622:10	(ro rt):64622:10	64622:0:10
two prepend to loss = unknown	64622:999	(ro rt):64622:999	64622:0:999
three prepend to loss > 2%	64623:2	(ro rt):64623:2	64623:0:2
three prepend to loss > 10%	64623:10	(ro rt):64623:10	64623:0:10
three prepend to loss = unknown	64623:999	(ro rt):64623:999	64623:0:999

## Informatives

function	community	extended	large
Origin ASN	rs-asn:peer-asn	(ro rt):rs-asn:peer-asn	rs-asn:0:peer-asn
IXP location (XX = DDD)	rs-asn:65XXX	(ro rt):rs-asn:65XXX	rs-asn:0:65XXX
ASN - RTT 0.001ms < 10ms	rs-asn:64661	(ro rt):rs-asn:64661	rs-asn:660:1
ASN - RTT 10ms < 50ms	rs-asn:64662	(ro rt):rs-asn:64662	rs-asn:660:2
ASN - RTT 50ms < 100ms	rs-asn:64663	(ro rt):rs-asn:64663	rs-asn:660:3
ASN - RTT 100ms < 150ms	rs-asn:64664	(ro rt):rs-asn:64664	rs-asn:660:4
ASN - RTT 150ms < 200ms	rs-asn:64665	(ro rt):rs-asn:64665	rs-asn:660:5
ASN - RTT 200ms < 250ms	rs-asn:64666	(ro rt):rs-asn:64666	rs-asn:660:6
ASN - RTT > 250ms	rs-asn:64667	(ro rt):rs-asn:64667	rs-asn:660:7
ASN - RTT = unknown	rs-asn:64669	(ro rt):rs-asn:64669	rs-asn:660:9
ASN - LOSS 0%	rs-asn:64671	(ro rt):rs-asn:64671	rs-asn:670:1
ASN - LOSS 0.001% < 2%	rs-asn:64672	(ro rt):rs-asn:64672	rs-asn:670:2
ASN - LOSS 2% < 10%	rs-asn:64673	(ro rt):rs-asn:64673	rs-asn:670:3
ASN - LOSS > 10%	rs-asn:64674	(ro rt):rs-asn:64674	rs-asn:670:4
ASN - LOSS = unknown/100%	rs-asn:64679	(ro rt):rs-asn:64679	rs-asn:670:9
ASN from Afrinic	rs-asn:64680	(ro rt):rs-asn:64680	rs-asn:680:0
ASN from Apnic	rs-asn:64681	(ro rt):rs-asn:64681	rs-asn:680:1
ASN from Arin	rs-asn:64682	(ro rt):rs-asn:64682	rs-asn:680:2
ASN from Lacnic	rs-asn:64683	(ro rt):rs-asn:64683	rs-asn:680:3
ASN from Ripe	rs-asn:64684	(ro rt):rs-asn:64684	rs-asn:680:4
ASN from Brazil	rs-asn:64685	(ro rt):rs-asn:64685	rs-asn:680:5



## Filtro

function	standard	extended	large
BH announce	65535:666	(ro rt):65535:666	65535:616:666
Confirmed BH	rs-asn:666	(ro rt):rs-asn:666	rs-asn:616:666
registro.br invalid	rs-asn:65110	(ro rt):rs-asn:65110	rs-asn:100:0
registro.br valid	rs-asn:65111	(ro rt):rs-asn:65111	rs-asn:100:1
registro.br unknown	rs-asn:65112	(ro rt):rs-asn:65112	rs-asn:100:2
IRR - prefix present in AS-SET	rs-asn:65121	(ro rt):rs-asn:65121	rs-asn:200:1
IRR - prefix not present in AS-SET	rs-asn:65122	(ro rt):rs-asn:65122	rs-asn:200:2
RPKI invalid	rs-asn:65130	(ro rt):rs-asn:65130	rs-asn:300:0
RPKI valid	rs-asn:65131	(ro rt):rs-asn:65131	rs-asn:300:1
RPKI unknown	rs-asn:65132	(ro rt):rs-asn:65132	rs-asn:300:2
RIRs invalid	rs-asn:65140	(ro rt):rs-asn:65140	rs-asn:400:0
RIRs valid	rs-asn:65141	(ro rt):rs-asn:65141	rs-asn:400:1
RIRs unknown	rs-asn:65142	(ro rt):rs-asn:65142	rs-asn:400:2
Invalid prefix length	rs-asn:65190	(ro rt):rs-asn:65190	rs-asn:190:0
Bogon prefix	rs-asn:65191	(ro rt):rs-asn:65191	rs-asn:190:1
Bogon asn	rs-asn:65192	(ro rt):rs-asn:65192	rs-asn:190:2
Transit free	rs-asn:65193	(ro rt):rs-asn:65193	rs-asn:190:3
Never via RS	rs-asn:65194	(ro rt):rs-asn:65194	rs-asn:190:4
IXPs prefixes	rs-asn:65195	(ro rt):rs-asn:65195	rs-asn:190:5

# No IX.br

- Todas as localidades possuem communities
  - Algumas possuem todas as communities
  - Algumas estão em fase de implantação
  - Precisa conferir a situação da sua localidade

[http://docs.ix.br/doc/communities-table-ix-br-v2\\_0-22032022.pdf](http://docs.ix.br/doc/communities-table-ix-br-v2_0-22032022.pdf)

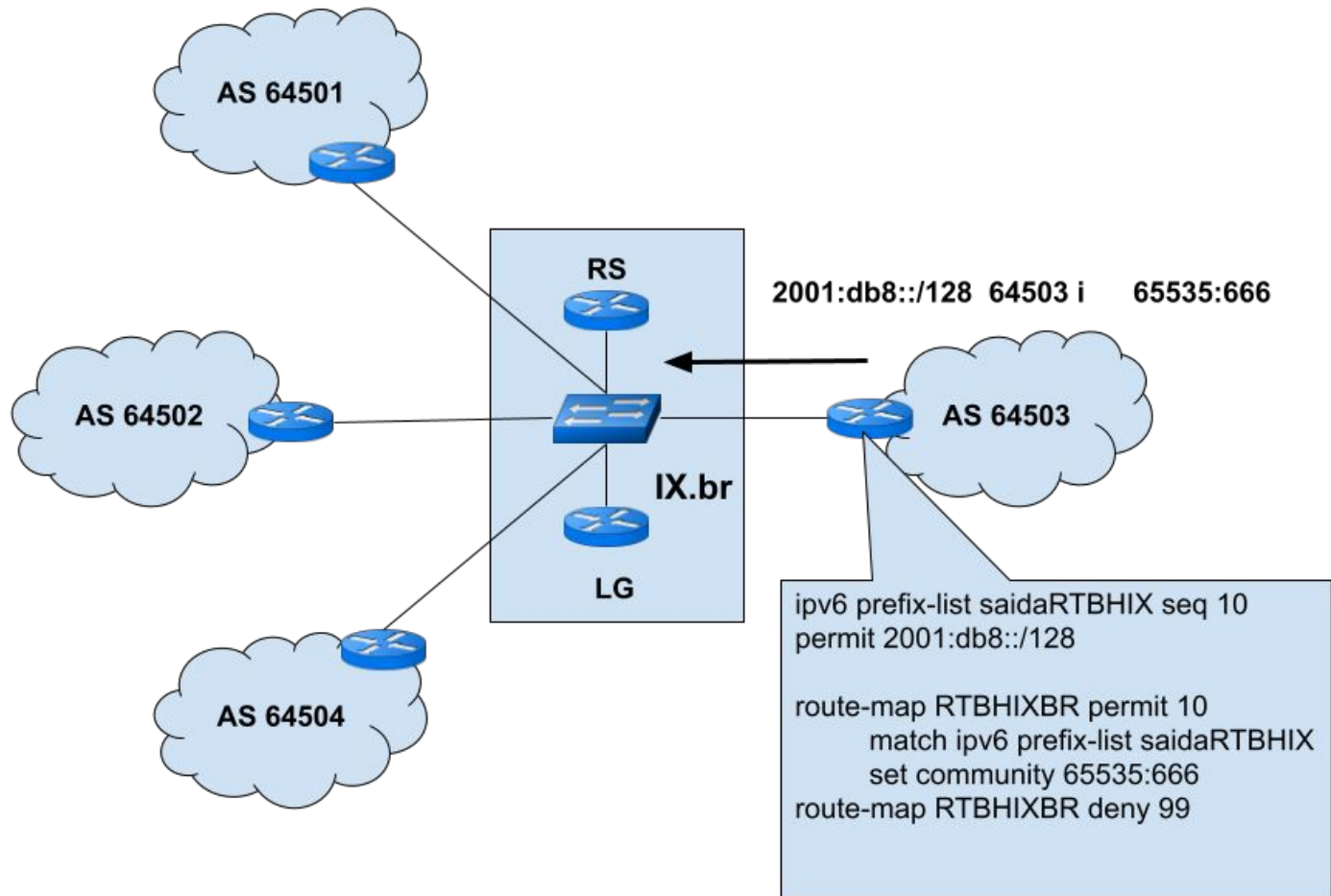
# Casos de estudo

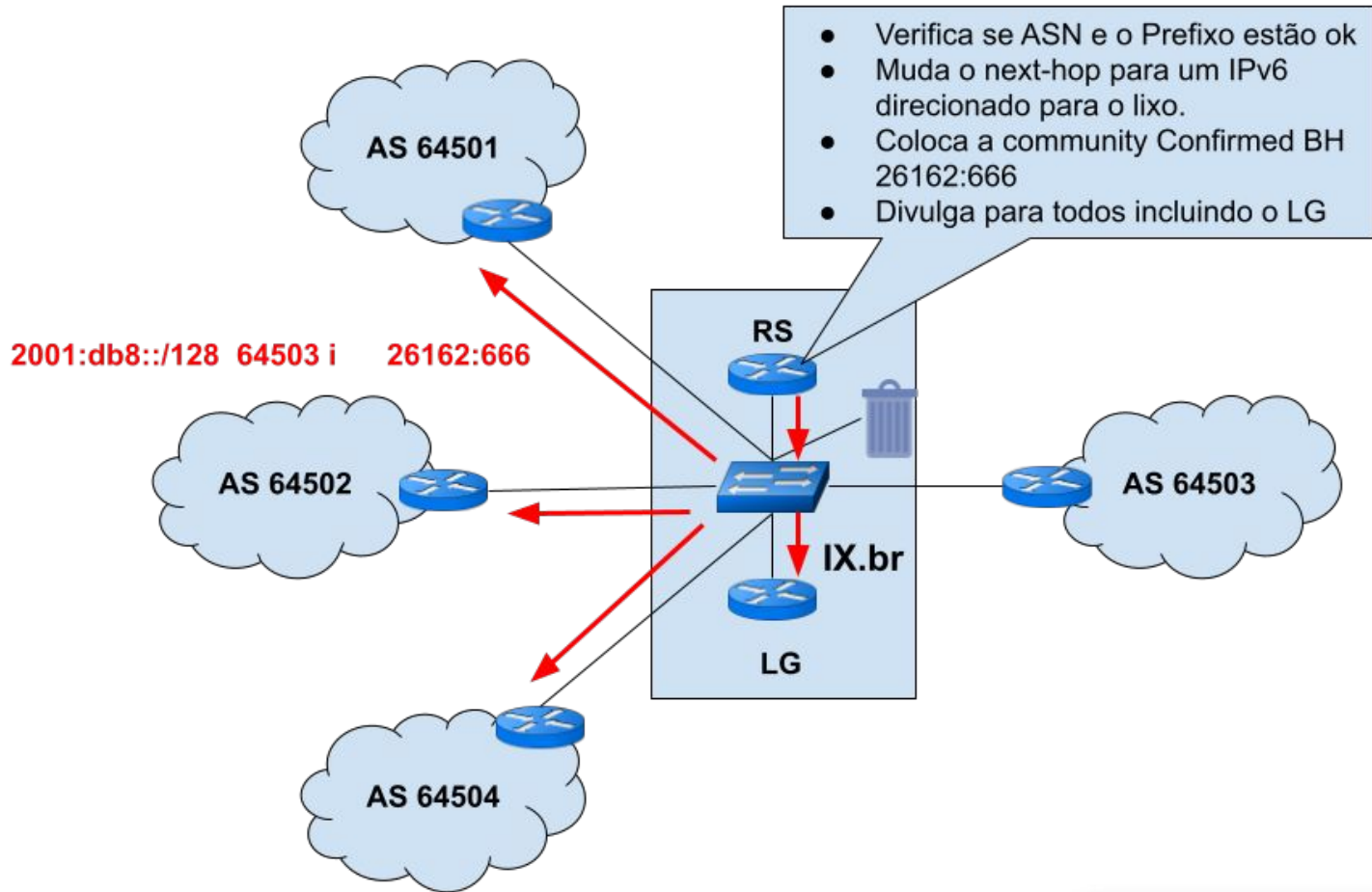
# Caso 1

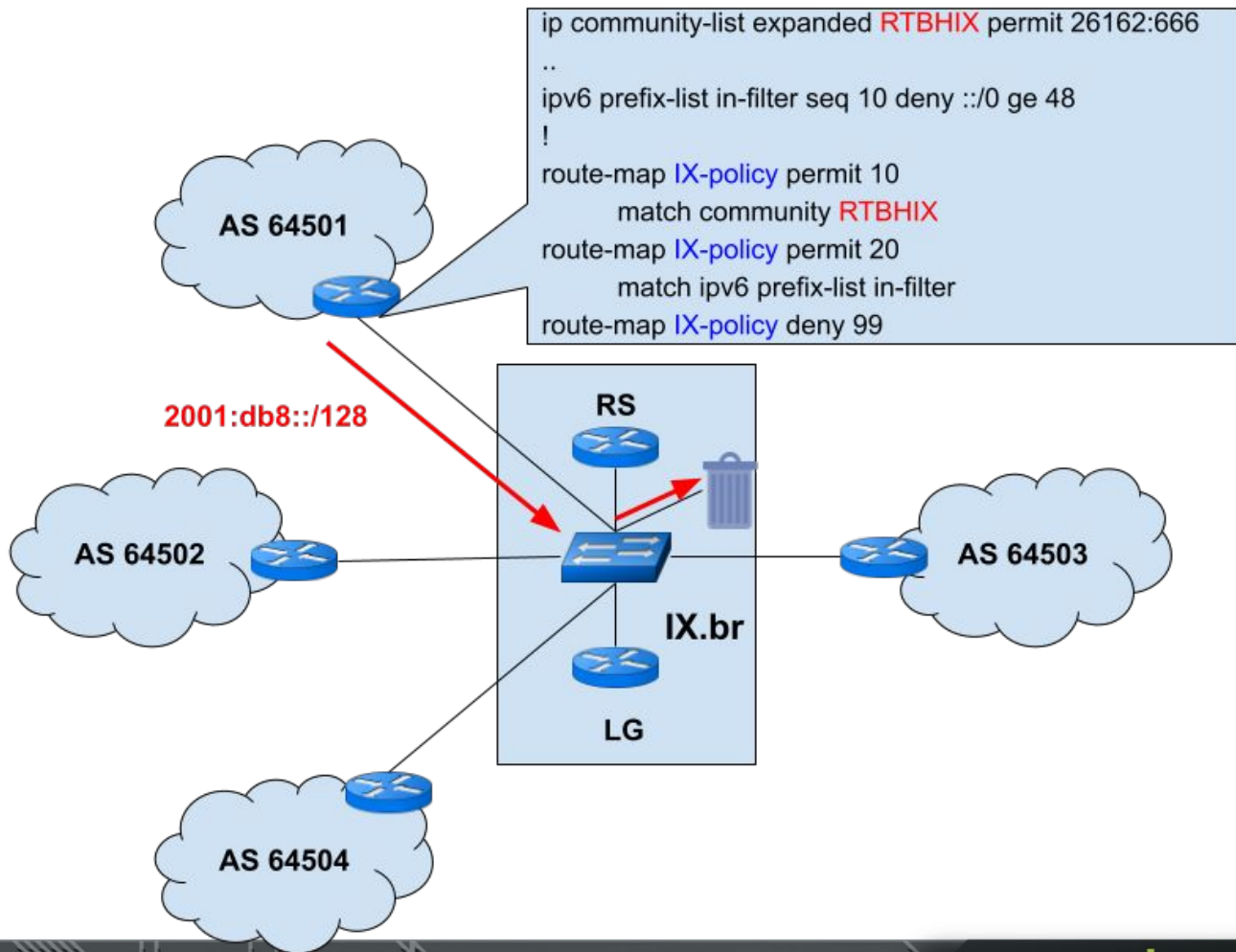
## RTBH no IX.br

# No IX.br

- Para se utilizar o Blackhole é preciso
  - Ser um Sistema Autônomo registrado no Registro.br(whois)
  - Usar rotas /32 em IPv4 ou /128 em IPv6
  - Ser o detentor da Rota (as-path com origem seu ASN)
  - Não pode ter intermediários (as-path não pode ter outro ASN além do seu)
  - Usar **65535:666** ou **(ro|rt):65535:666** ou **65535:666:0**







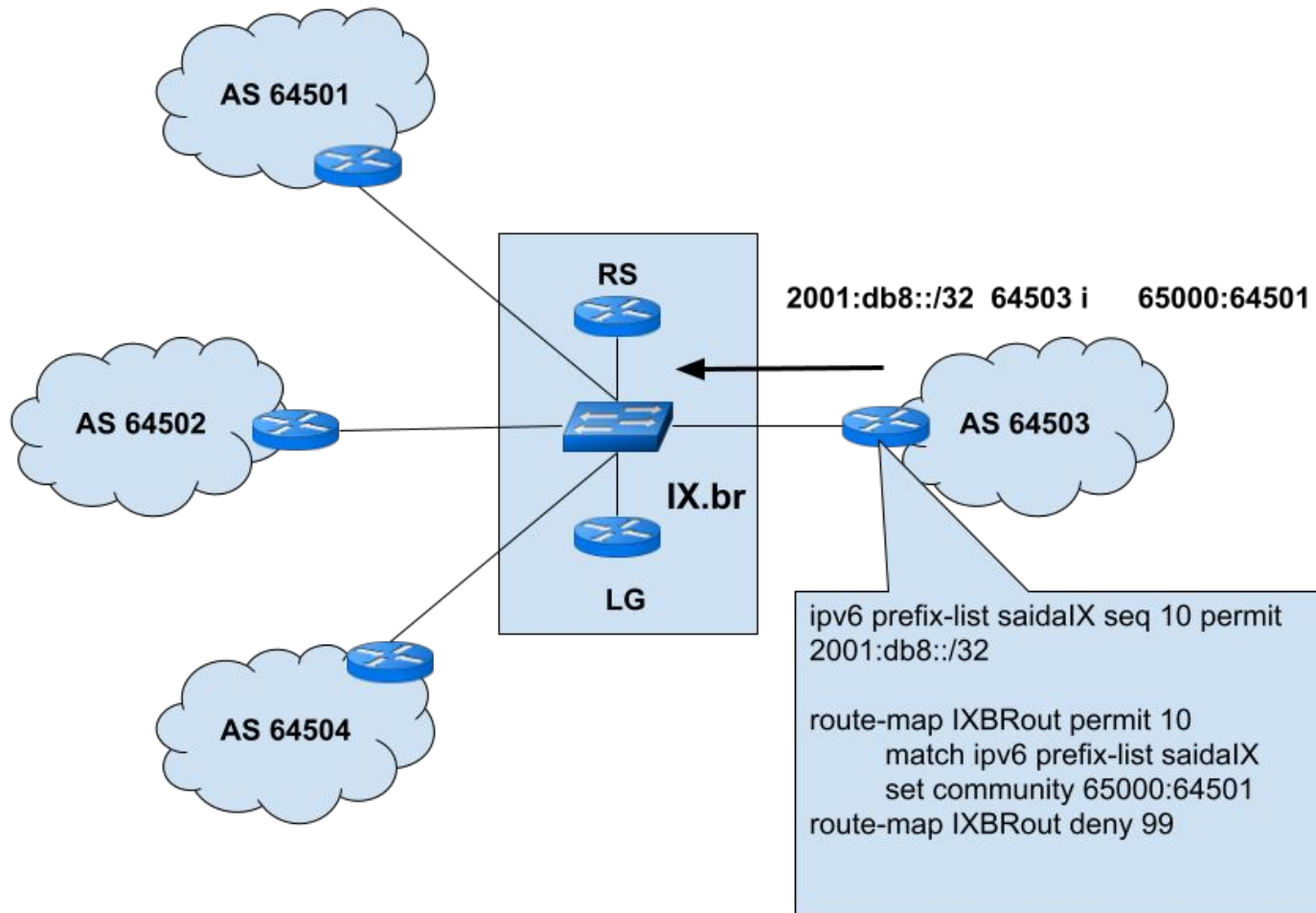


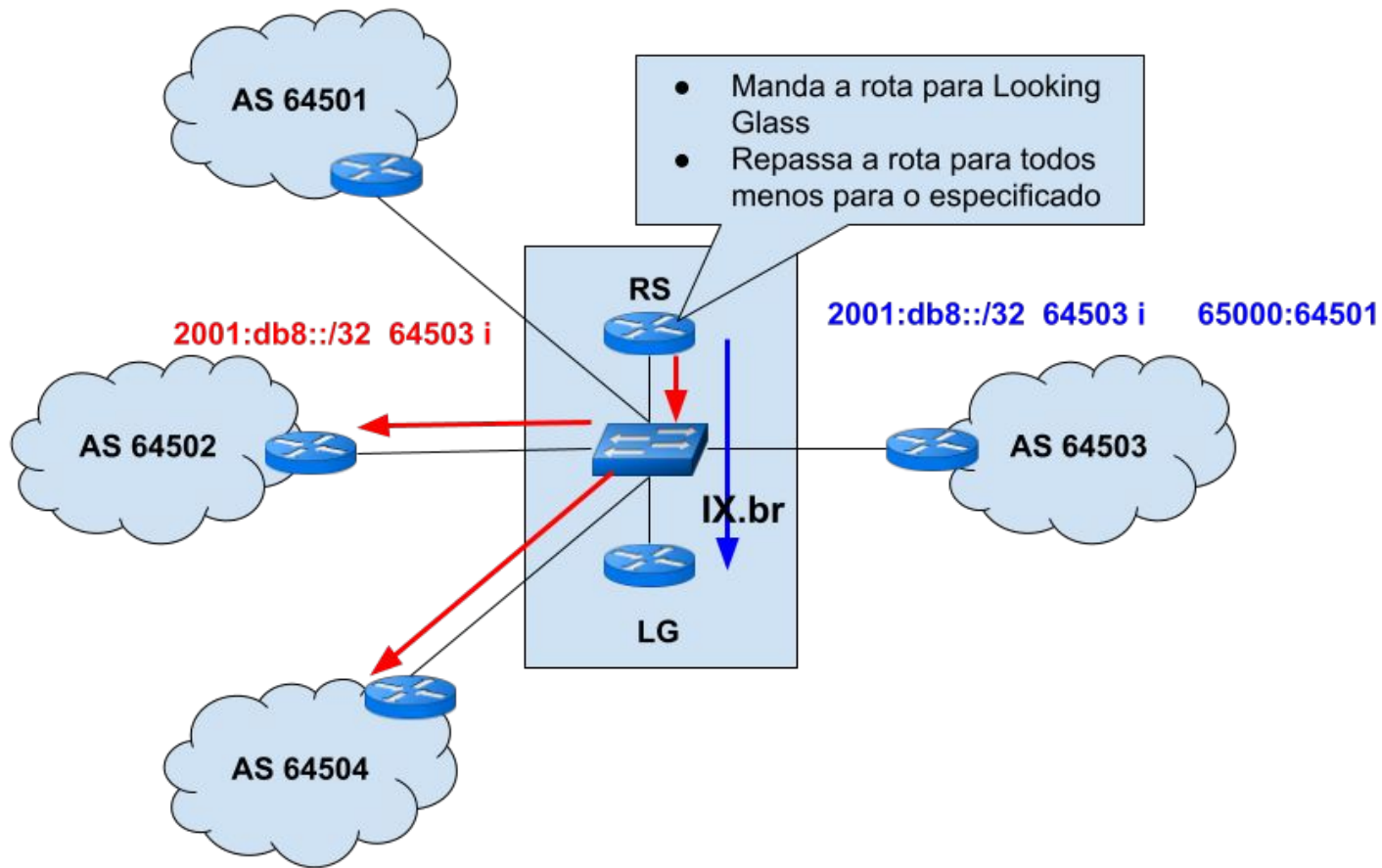
# Caso 2

## IX.br No Export

# IX.br No Export

- Uma forma de não enviar as rotas para um determinado participante do IX.br
- Em breve vai poder ser condicional com o RTT e a Perda
- Fica visível no Looking Glass



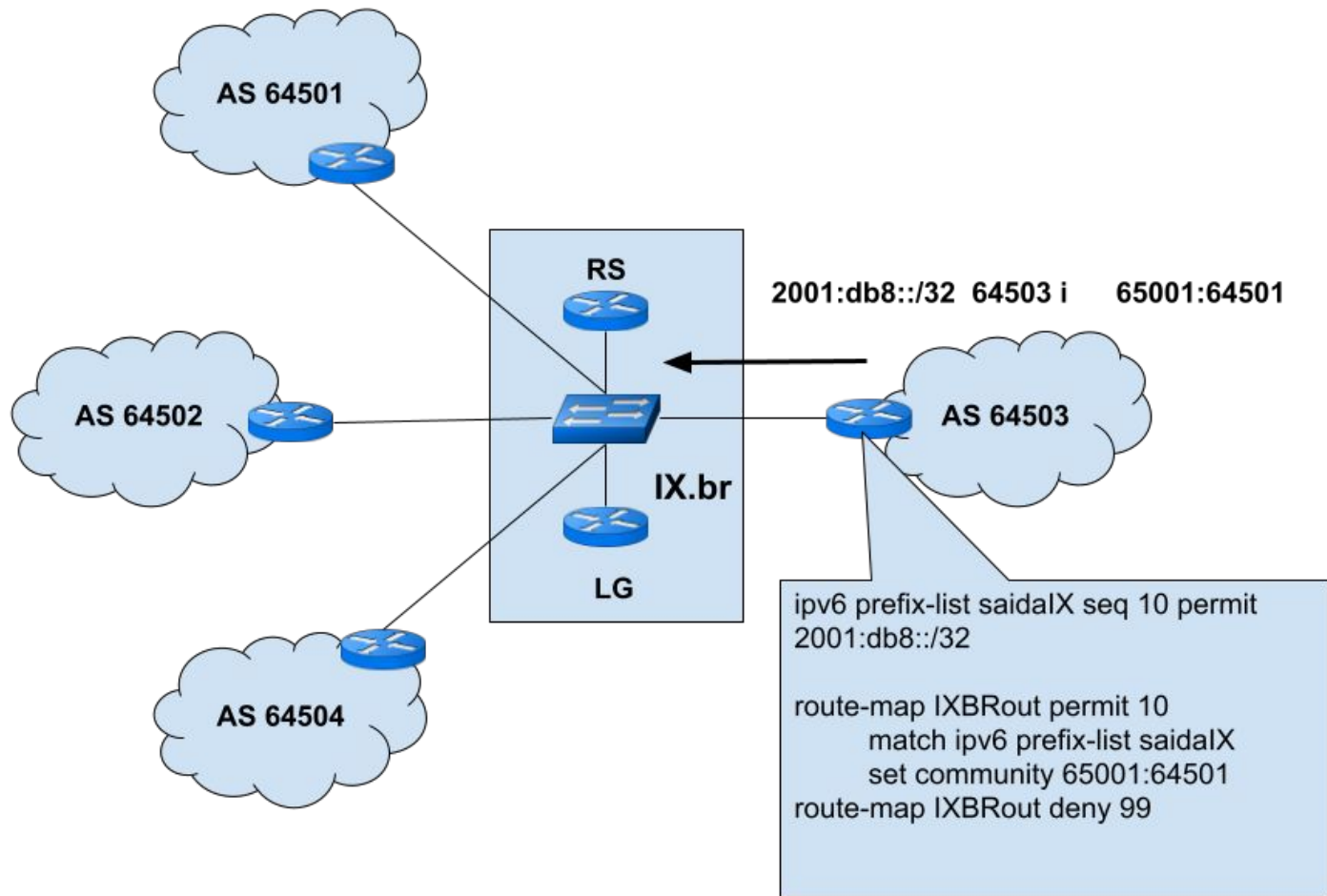


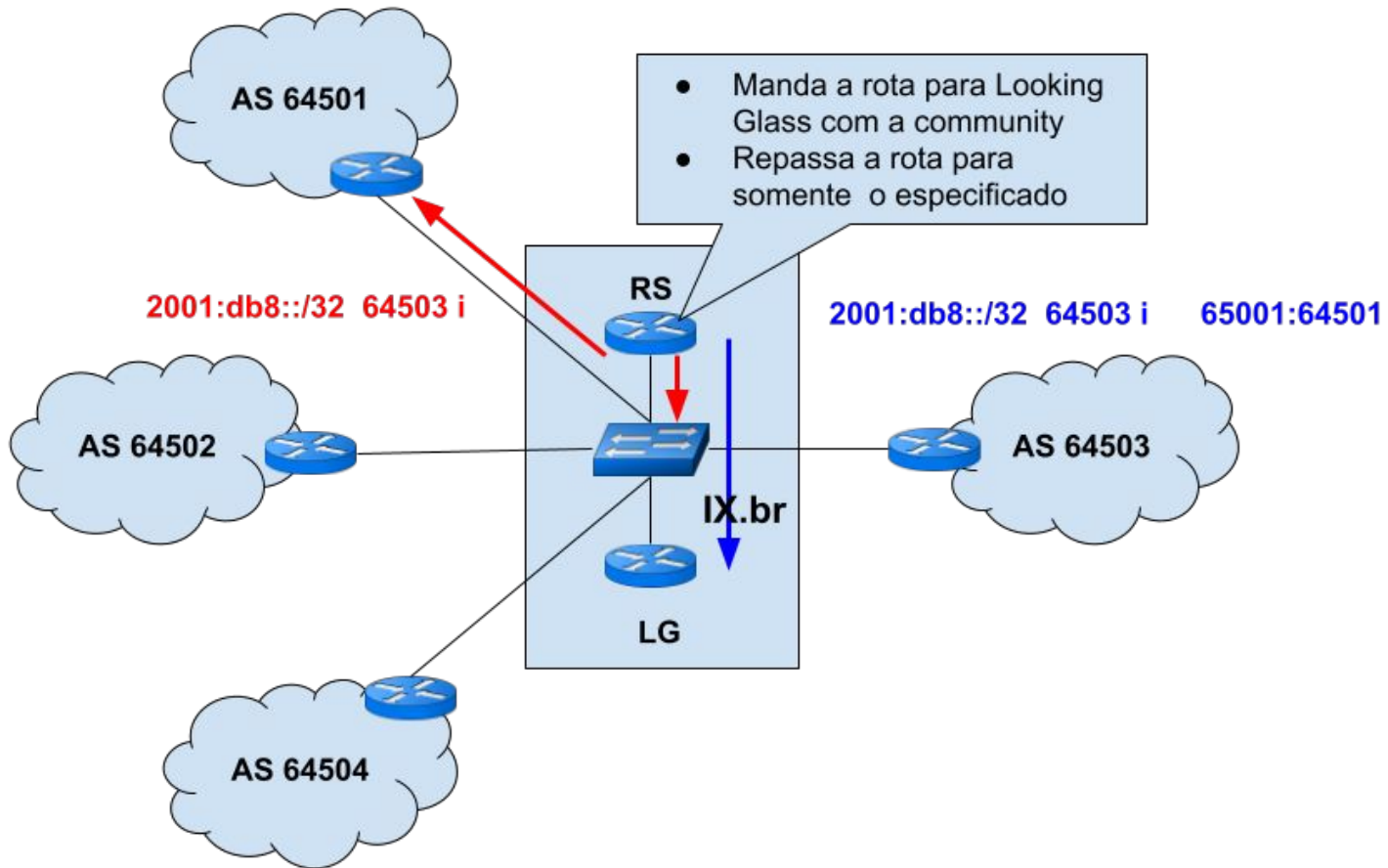
# Caso 3

## IX.br Only Export

# IX.br Only Export

- Uma forma de enviar as rotas para um determinado participante do IX.br - Oposto do No export
- Às vezes pode ser mais interessante escolher a dedo para quem enviar as rotas do que remover da lista de todos os participantes quem não deve receber.
  - São Paulo tem muitos de participantes.







# Obrigado!!!

Equipe de cursos do CEPTRO.br

@ cursosceptro@nic.br

@ ipv6@nic.br

São Paulo, Abril de 2022

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)