Proposta para mudança nos servidores de rotas e nas políticas de tratamento de *communities* BGP no IX.br

Versão: 2.05
Data da última modificação:
Qua 26 Out 2016 17:27:44 BRST

1. **Objetivos**

Este documento apresenta uma proposta para modificar o funcionamento dos servidores de rotas e a política de uso das *communities* nos PTTs do IX.br, com o objetivo de:

1. adequar o funcionamento dos servidores de rotas do IX.br às boas práticas documentadas nas RFCs 7947 [1] e 7948 [2];

2. diminuir o trabalho operacional no IX.br e concomitantemente proporcionar agilidade e independência aos participantes na configuração de filtros, implementando com essa finalidade o tratamento de *communities* para filtros nos *route server*s, de forma que a funcionalidade provida por tais *communities* possa substituir a configuração manual de filtros específicos que é feita atualmente;

3. permitir que os participantes do IX.br negociem e utilizem *communities* entre si, para facilitar a implementação de filtros, tornando os servidores de rotas transparentes às mesmas;

4. permitir que o atributo BGP MED seja utilizado para engenharia de tráfego, tornando os servidores de rotas transparentes ao mesmo;

5. permitir que os participantes filtrem os prefixos entrantes mais facilmente, mantendo a marcação existente hoje, do AS de origem, mas acrescentando também marcações de validação de origem, segundo a base do Registro.br, e utilizando também os RIRs e RPKI;

6. permitir que os participantes implementem mais facilmente certas políticas de roteamento, oferecendo por meio de *communities* a adição de *prepends* para destinos específicos.

2. **Os servidores de rotas, ou *route servers***

Os *Internet Exchanges*, como os PTTs do IX.br, disponibilizam a infraestrutura para permitir a troca de tráfego IP entre seus participantes, normalmente usando uma rede compartilhada de camada 2, como a Ethernet. O Border Gateway Protocol (BGP) é usado normalmente para facilitar a troca de informações sobre os endereços presentes em cada rede, nessa infraestrutura.

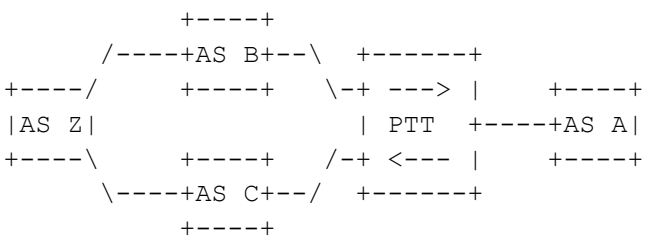
Historicamente, os participantes dos PTTs fechavam sessões BGP bilaterais entre si, para atualizar suas tabelas de rotas. Contudo, para PTTs com muitos participantes, essa abordagem gera um trabalho operacional enorme.

Nos PTTs do IX.br, os servidores de rotas permitem a implantação facilitada, do ponto de vista técnico, do acordo de troca de tráfego multilateral (ATM), onde cada participante concorda em trocar tráfego com os demais. Sua função é a de um *broker*, um intermediário, facilitador ou concentrador: cada participante do acordo multilateral fecha uma sessão com o servidor de rotas. Os prefixos recebidos de cada um serão repassados a os demais, com exceção do próprio participante que originou o anúncio, mas sem acrescentar o ASN do servidor de rotas, e sem modificar o atributo *next_hop*.

Atualmente, o IX.br oferece o serviço de filtro nos servidores de rotas e utiliza como mecanismo de proteção a limitação de número de anúncios por cada participante.

Além das alterações nas políticas de uso de *communities*, que serão discutidas neste documento, há duas alterações, aqui propostas, no funcionamento dos servidores de rotas:

1. **Mitigação de ocultamento de caminhos (path hiding):**



Considere a situação apresentada na figura, onde Sistemas Autônomos A, B e C são participantes de um PTT do IX.br e o AS Z é cliente de trânsito tanto do AS B, quanto do AS C.

O servidor de rotas do IX.br recebe os prefixos do AS Z, tanto via AS B, quanto via AS C. Como ele funciona de forma análoga a um roteador BGP normal, escolhe a melhor rota e repassa somente ela para o AS A. O AS A recebe os prefixos do AS Z apenas via AS B, ou apenas via AS C, não ambos.

Caso o AS A e o AS B tenham filtros implementados no PTT para não receberem as rotas um do outro, e se o servidor de rotas escolher o AS B como melhor caminho para o AS Z, o AS A não recebe os prefixos do AS Z.

Essa situação é diferente do que ocorreria caso o AS A fechasse sessões BGP bilaterais tanto com o AS B, como com o AS C. Nesse caso receberia os prefixos do AS Z por ambos os caminhos.

A situação exemplificada acima é o que chamamos de *path hiding*, ou ocultamento de caminhos. Os PTTs do IX.br, atualmente, com exceção do IX.br em Curitiba, PR, operam atualmente nessa situação.

Há diversas formas de mitigar essa situação, descritas na RFC 7947 [1], que permitem que todos os diferentes caminhos possíveis cheguem aos participantes, imitando de forma melhor o mesmo comportamento que ocorreria caso houvesse sessões bilaterais entre todos os participantes do PTT.

Nos servidores de rotas do IX.br será implementada a abordagem de múltiplas RIBs, de forma que para cada cliente do servidor de rotas exista uma RIB separada.

Estudos mostram que no PTT de São Paulo essa mudança resultará no aumento do número de prefixos anunciados em cerca de 50%. Obviamente isso inclui prefixos repetidos, mas com diferentes AS PATH para cada um deles.

2. Transparência ao atributo MED (MULTI_EXIT_DISC)

O atributo MED é um atributo opcional e não-transitivo, que é usado na interligação entre diferentes ASs com múltiplos pontos de entrada ou saída, para diferenciá-los. Como o servidor de rotas tem o objetivo de ser um elemento 'invisível' na rede, do ponto de vista do BGP, a RFC 7947 [1] especifica que ele deve ser propagado.

Atualmente no IX.br nem todos os servidores de rotas são transparentes ao atributo MED. **Este documento especifica a implementação da transparência ao atributo MED em todos os servidores de rotas dos PTTs do IX.br.**

3. **As *Communities***

As *communities* foram adicionadas ao protocolo BGPv4 com o objetivo de criar um mecanismo para agrupamento de prefixos, de modo que a decisão de roteamento também possa se dar com base na identidade de um grupo, garantindo uma maior flexibilidade na heurística de tomada de decisão para a formação da tabela de rotas BGP. Ou seja, as *communities* permitem marcar grupos de prefixos, e decisões podem ser tomadas com base nessa marcação.

O atributo *community* foi definido por meio da RFC1997 [3], que descreve sua inclusão no protocolo BGPv4. Este por sua vez foi inicialmente definido pela RFC 1271 [4] e atualmente é descrito na RFC 4271 [5].

Exemplos de utilização incluem o controle sobre a propagação de prefixos, a criação de filtros e a mitigação de ataques DDOs.

As *communities* são amplamente difundidas e utilizadas na Internet. **Atualmente, no IX.br, elas são tratadas nos servidores de rotas segundo as seguintes políticas:**

i. Todas as *communities* recebidas de um participante são ignoradas e não são propagadas para os demais.

ii. Cada prefixo recebido e propagado pelo servidor de rotas é marcado com uma *community* para identificar o participante que o originou, no formato 26162:ASN. Se o ASN do participante é de 32 bits, é feita uma conversão estática, usando ASNs de documentação e privados mapeados (estática e manualmente) em uma tabela. O objetivo principal dessa marcação é a utilização dessas *communities* na configuração de filtros manuais entre os participantes internamente, no próprio servidor de rotas do IX.br.

O presente documento propõe **a mudança da política de uso das *communities* no IX.br**, da forma que é **resumida a seguir e detalhada no restante do texto:**

1. **Filtros**: Serão definidas *communities* (no caso de ASNs de 32 bits serão usadas *extended communities* com a mesma sintaxe) [6] específicas para filtros, que serão processadas pelos servidores de rotas, de forma a evitar a propagação dos prefixos marcados para participantes determinados, ou indicar que os mesmos deverão ser propagados apenas para participantes específicos. Essas *communities* não serão propagadas para os demais participantes.

2. ***Prepends*:** Serão definidas *communities* (no caso de ASNs de 32 bits serão usadas *extended communities* com a mesma sintaxe) [6] específicas para aplicação de *prepends* em prefixos enviados para um destino em particular. Essas *communities* não serão propagadas para os demais participantes.

3. **Identificação de origem:** Cada prefixo recebido e propagado pelo servidor de rotas continuará sendo marcado com uma *community* para identificar o participante que a originou, em formato similar ao utilizado atualmente, mas com o uso de *extended communities* no caso de ASNs de 32 bits, para identificar o participante que o originou.

4. **Transparência à *communities*:** As *communities* (e *extended communities*) recebidas continuarão a ser ignoradas pelos servidores de rotas, como é feito hoje, mas deixarão de ser descartadas, ou seja, serão propagadas para os demais participantes, reforçando

a característica de transparência dos servidores de rotas. Há duas exceções: (i) as *communities* dos itens 1 e 2, que se destinam ao próprio servidor de rotas, elas serão tratadas e não serão propagadas e (ii) *communities* no mesmo formato das do item 3, que o servidor de rotas usa para marcar o AS que originou um determinado anúncio, elas não serão propagadas.

5. **Validação de origem:** Os prefixos recebidos e propagados passarão a ser marcados com *communities* que identificarão se a origem do prefixo foi validada com êxito ou não, ou não foi validada, e por qual meio. Serão utilizadas inicialmente validações feitas com consultas à base do Registro.br, aos RIRs e via RPKI.

4. **Detalhes das novas políticas para *communities* no IX.br**

A seguir, o documento descreve em mais detalhes as novas políticas para *communities*:

Política 1: *community* para filtro de ASN de destino

Atualmente dentro do acordo de troca de tráfego multilateral o IX.br oferece o serviço de filtros. A solução atual é manual, o que onera a equipe de operação do IX.br e também causa problemas para os participantes. Diante de um problema mais severo de roteamento, um participante do IX.br não pode contar com o mecanismo de filtragem para mitigar ou atenuar impactos, ao menos não de forma imediata, dependendo da disponibilidade da equipe do IX.br para realizar o filtro.

A nova política propõe um alternativa para realizar os filtros por meio de *communities* públicas. Os filtros deixarão de ser feitos com configurações específicas nos servidores de rotas para cada solicitação, e serão implementados tão somente por meio do processamento da *community* definida.

A *community* para especificar o filtro terá o formato a seguir, sendo possível utilizar *extended communities* (no formato two-octet AS specific *extended community*, como definido na RFC 4360) [5] para especificar ASNs de 32 bits. Será possível especificar vários ASs diferentes, para que não recebam um determinado anúncio, marcando o mesmo com as *communities* apropriadas.

65000:<ASN> - NÃO exporta o prefixo para o AS especificado

É importante notar que essa *community* funcionará como um filtro unidirecional no servidor de rotas, diferenciando-se do atual serviço de filtros do IX.br. O novo modelo para o serviço implica que o AS interessado no filtro deverá também descartar as rotas do AS a ser filtrado na sua política de entrada.

Além dessa *community*, será também aceita e processada a seguinte *community* auxiliar, cujo objetivo é marcar um prefixo que será exportado apenas para o AS especificado. Ela tem o objetivo de permitir que os participantes troquem tráfego com, ou implementem políticas específicas para, apenas um, ou um subconjunto dos ASs presentes no acordo multilateral. Será possível especificar vários ASs diferentes, para que apenas eles recebam um determinado anúncio, marcando o mesmo com as *communities* apropriadas.

65001:<ASN> - exporta o prefixo APENAS PARA o AS especificado

O <ASN> específica o participante alvo. Na interpretação dessas duas *communities* (65000:<ASN>, 65001:<ASN>) pelo servidor de rotas, a segunda é mais prioritária.

Exemplos de uso:

1. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **sem *communities***, ou com qualquer *community* diferente de 65001:* ou 65000:*:
   Ação: **o prefixo 203.0.113.0/24 será exportado para todos os ASs, com exceção do próprio AS 64496, que o originou.**

2. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com a *community* 65000:65551:**
   Ação: o prefixo 203.0.113.0/24 será exportado para todos os ASs, com exceção do próprio AS 64496, que o originou, e do AS 65551, que foi especificado na *community* 65000:65551.

3. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com a *community* 65000:65551, e com a community 65000:64500:**
   Ação: o prefixo 203.0.113.0/24 será exportado para todos os ASs, com exceção do próprio AS 64496, que o originou, e dos ASs 65551 e 64500, que foram especificados nas *communities* 65000:65551 e 65000:64500.

4. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com a *community* 65000:64496:**
   Ação: o prefixo 203.0.113.0/24 será exportado para todos os ASs, com exceção do próprio AS 64496, que o originou. A *community* 65000:64496 nesse caso não tem efeito prático. O mesmo comportamento se dará se a *community* utilizada for 65000:26162, 65000:0, ou se o ASN especificado em 65000:<ASN> não estiver no acordo de troca de tráfego multilateral.

5. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com a *community* 65001:65551:**
   Ação: o prefixo 203.0.113.0/24 será exportado apenas para o AS 65551, especificado na *community* 65001:65551.

6. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com as *communities* 65001:65551 e 65001:64500:**
   Ação: o prefixo 203.0.113.0/24 será exportado apenas para os ASs 65551 e 64500, especificados na *communities* 65001:65551 e 65001:64500.

7. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com a *community* 65001:64496:**
   Ação: o prefixo 203.0.113.0/24 não será exportado para nenhum AS. A *community* 65001:64496 especifica que ele deveria ser exportado apenas para o AS 64496, mas como esse é o próprio AS que originou o anúncio, o servidor de rotas não a exportará. O mesmo comportamento se dará se a *community* utilizada for 65001:26162, 65001:0, ou se o ASN especificado em 65001:<ASN> não estiver no acordo de troca de tráfego multilateral.

8. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com as *communities* 65000:65551 e 65001:64500:**
   Ação: o prefixo 203.0.113.0/24 será exportado apenas para o AS 64500, especificado na *community* 65001:64500. A *community* 65000:65551 nesse caso não tem efeito prático. A *community* 65001:64500 tem preferência na implementação do filtro e determina que o prefixo não será exportado para nenhum outro AS, senão o 64500. Acrescentar a *community* 65000:65551 especificando que o prefixo não deve ser exportado para o AS 65551 é redundante e não tem efeito.

9. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com as *communities* 65000:65551 e 65001:65551:**

Ação: o prefixo 203.0.113.0/24 será exportado apenas para o AS 65551. Note-se que usar ambas as *communities* simultaneamente para um mesmo AS alvo não faz sentido, já que elas especificam ações opostas. Nesse caso, a *community* 65001:65551 é prioritária e é a ação especificada por ela que será realizada.

Uma vez que essas *communities* são especificadas para ações nos servidores de rotas, **elas não serão exportadas.**

Política 2: *community* para acréscimo de *prepends* para um ASN de destino

Em alguns casos pode ser desejável para um participante acrescentar prepends nos prefixos enviados para um determinado AS de destino, como ferramenta de engenharia de tráfego.

Por exemplo, um participante A presente em dois PTTs do IX.br, digamos São Paulo e Rio de Janeiro, troca tráfego com um participante B, também presente nesses dois PTTs, por meio do ATM. O participante A pode preferir que para alguns prefixos o PTT de São Paulo tenha preferência, para o participante B, em relação ao do Rio de Janeiro. Assim, no PTT do Rio de Janeiro, no envio dos prefixos para o participante B, o participante A incluiria prepends.

Em muitas ocasiões o uso de desagregação como ferramenta de engenharia de tráfego é preferível ao uso de *prepends*, mas em alguns casos ela não é sequer possível. Por exemplo, quando o participante tem apenas um bloco /24 IPv4 ou /48 IPv6. Nesses casos, o uso de *prepends*, com parcimônia, pode ser uma alternativa viável.

A nova política propõe uma alternativa para acrescentar 1, 2 ou 3 *prepends* a um anúncio para um AS específico de destino, com o uso *communities* públicas.

A *community* para especificar os *prepends* terá o formato a seguir, sendo possível utilizar *extended communities* (no formato two-octet AS specific *extended community*, como definido na RFC 4360) [6] para especificar ASNs de 32 bits. Será possível especificar vários ASs diferentes, para que recebam um determinado anúncio com *prepends*, marcando o mesmo com as *communities* apropriadas.

64601:<ASN> - adiciona 1 *prepend* no envio do prefixo para o AS especificado
64602:<ASN> - adiciona 2 *prepend* no envio do prefixo para o AS especificado
64603:<ASN> - adiciona 3 *prepend* no envio do prefixo para o AS especificado

Exemplos de uso:

1. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **sem *communities***, ou com qualquer *community* diferente de 64601:*, 64602:* ou 64603:*:
   Ação: **o prefixo 203.0.113.0/24 será exportado normalmente, sem o acréscimo de *prepends*, sem alteração do AS PATH.**

2. O servidor de rotas recebe do AS 64496 o prefixo 203.0.113.0/24 **marcado com a *community* 64603:65551, cujo AS PATH original é**
   203.0.113.0/24 64496 i :
   Ação: o prefixo 203.0.113.0/24 será exportado:
   (a) para o AS 65551, com 3 *prepends* no AS PATH:

203.0.113.0/24 64496 64496 64496 64496 i
(b) para todos os demais ASs, com exceção do próprio AS 64496, que o originou, e do AS 65551, especificado na *community*, o prefixo será exportado sem adição de *prepends* ou alteração de AS PATH:
203.0.113.0/24 64496 i

Política 3: Identificação de origem

Atualmente, cada prefixo recebido e propagado pelo servidor de rotas é marcado com uma *community* para identificar o participante que o originou, no formato:

26162:<ASN>

O prefixo será marcado também com uma segunda *community*, destinada a identificar o PTT (localidade) do IX.br, no formato:

26162:65XXX

onde XXX representa o PTT de origem do prefixo, conforme a tabela a seguir:

PTT (localidade)	XXX
Belém, PA	091
Belo Horizonte, MG	031
Brasília, DF	061
Campina Grande, PB	083
Campinas, SP	019
Cuiabá, MT	065
Caxias do Sul, RS	054
Curitiba, PR	041
Florianópolis, SC	048
Fortaleza, CE	085
Foz do Iguaçu, PR	045
Goiânia, GO	062
Lajeado, RS	051
Londrina, PR	043
Manaus, AM	092
Maringa, PR	044
Natal, RN	084
Porto Alegre, RS	051
Recife, PE	081
Rio de Janeiro, RJ	021
Salvador, BA	071
São Carlos, SP	016
S. J. dos Campos, SP	012
S. J. Rio Preto, SP	017
São Paulo, SP	011
Vitória, ES	027

Hoje não são usadas *extended communities*. Se o ASN do participante é de 32 bits, é feita uma conversão estática, usando ASNs de documentação e privados mapeados por meio de uma tabela, mantida manualmente e não divulgada. Embora as *communities* sejam propagadas para os participantes, seu principal objetivo é ser usadas internamente.

Com a nova política, cada prefixo recebido e propagado pelo servidor de rotas continuará sendo marcado com uma *community* para identificar o participante que a originou, em formato similar ao utilizado atualmente. A principal diferença é o suporte a *extended communities*, abrangendo assim também os ASNs de 32 bits sem necessidade de uma tabela de conversão. Além disso uma segunda *community* destinada a identificar o PTT (localidade) de origem do anúncio também será utilizada.

As *communities* para a identificação de origem passarão a ter uma importância maior no novo contexto. Isso porque **o novo modelo para os filtros**, que não serão mais feitos manualmente e serão baseados exclusivamente nas *communities*, **exige que o AS interessado no filtro também descarte as rotas do AS a ser filtrado** na sua política de entrada. **As *communities* de identificação de origem facilitam essa tarefa.**

Política 4: Transparência a *communities*

Todas as *communities* ou *extended communities* recebidas, exceto as definidas na política 1 (65000:<ASN> e 65001:<ASN>) **continuarão a ser ignoradas pelos servidores de rotas, como é feito hoje, mas deixarão de ser descartadas**, ou seja, serão propagadas para os demais participantes.

Essa nova política tem a função de permitir que os participantes do IX.br negociem e utilizem *communities* entre si, para facilitar a implementação de filtros.

Uma discussão em curso na comunidade de participantes do IX.br é que o mesmo poderia oferecer mecanismos de mitigação de ataques DDOS, como filtros de *black hole*. Embora isso seja tecnicamente possível, há um risco inerente que pode trazer implicações administrativas e jurídicas, por exemplo, se um evento de falha ocorrer direcionando uma rota não desejada para o *black hole*. Isso tornaria a ferramenta de proteção na própria causa de um DOS.

Uma alternativa interessante é que alguns participantes, como grandes provedores de *hosting* ou de trânsito possam oferecer o mecanismo de *black hole* em suas próprias redes, por meio de *communities* específicas, e divulgadas para os demais participantes. Quiçá *communities* padronizadas. O *black hole,* dessa forma, estaria mais próximo à origem do ataque do que se implementado no próprio IX. O tráfego bloqueado nem alcançaria a rede do IX.

Além disso, a nova política reforça a característica de transparência dos servidores de rotas, o que é uma premissa de funcionamento. Isso está de acordo com o que tem sido discutido na comunidade técnica [1] no processo de elaboração de uma BCP sobre o assunto.

Política 5: Validação de prefixos

O BGP é um protocolo pouco seguro. Erros de configuração, com a digitação de números errados, ou uma configuração intencionalmente maliciosa pode resultar na captura de prefixos

de uma rede, por outra. Ou seja, um AS pode, intencionalmente ou por acidente, anunciar rotas de outro, desviando o tráfego, o que pode permitir a obtenção de informações sensíveis, ou causar a indisponibilidade do serviço da vítima.

A estrutura de RPKI que está lentamente sendo implantada na Internet tem por objetivo ser uma solução para mitigar parcialmente esse problema. No RPKI a entidade que detém um determinado prefixo consegue especificar, em uma base de dados que é oferecida pelo RIR, quais Sistemas Autônomos podem anunciar o prefixo em questão. Os roteadores BGP têm mecanismos para aferir os anúncios nessa base de forma automática e segura, efetuando a validação de origem dos mesmos. Essa estrutura, contudo, ainda é incipiente, tem pouco uso, e não está disponível para Sistemas Autônomos brasileiros

Pode-se reduzir o risco inerente ao *peering* reduzindo-se o número de *peers*. Por exemplo, no lugar de participar do acordo multilateral, pode-se fazer *peering* apenas com poucos ASs, entre os quais exista uma boa relação de confiança. Contudo é uma prática de utilidade duvidosa, pois mesmo que possa diminuir o risco relacionado às más intenções, é praticamente impossível evitar erros ocasionais. Além disso, é uma prática que vai contra a própria concepção dos *Internet Exchange*s, que têm o objetivo de estimular a troca de tráfego.

O serviço de validação de prefixos, será oferecido como uma ferramenta adicional para diminuir o risco de captura de prefixos por terceiros. Consiste na análise de consistência de cada anúncio, com base na comparação com bases externas, e na marcação dos mesmos com as *communities* apropriadas.

Com base na análise dessas *communities* um participante poderá saber de que um prefixo cujo anúncio foi originado por um determinado AS foi realmente designado a ele pelo Registro.br ou um RIR. Além da base do Registro.br, será feita a validação nas bases dos RIRs, além da base do RPKI.

Para cada nova rota injetada no servidor de rotas, um agente busca nessas diversas bases a informação do vínculo entre aqueles prefixos e o ASN que formou o anúncio. Três estados são possíveis, para cada uma das bases:

- **prefixo inválido:** o prefixo consta na base e não corresponde ao ASN;
- **prefixo válido:** o prefixo consta na base e corresponde ao ASN;
- **prefixo desconhecido:** o prefixo não aparece na base, ou a base não está disponível para consulta.

O servidor de rotas marcará cada prefixo **sempre** com três *communities*, correspondentes à validação em cada uma das bases:

- Base do Registro.br (uma das três *communities* marcará o prefixo):
  - **26162:65110 - inválido no Registro.br**
  - **26162:65111 - válido no Registro.br**
  - **26162:65112 - desconhecido no Registro.br**

- Base dos RIRs (uma das três *communities* marcará o prefixo)::
  - **26162:65120 - inválido no RIR**
  - **26162:65121 - válido no RIR**
  - **26162:65122 - desconhecido no RIR**

- RPKI (uma das três *communities* marcará o prefixo):
  - **26162:65130 - inválido no RPKI**
  - **26162:65131 - válido no RPKI**
  - **26162:65132 - desconhecido no RPKI**

5. **Implicações na segurança e estabilidade da plataforma**

No que tange à segurança, **as mudanças no comportamento dos servidores de rotas, quanto à mitigação da ocultação de caminhos, e à transparência ao MED**, bem como as **políticas em relação às communities 1 (filtros), 2 (*prepends*) e 3 (identificação de origem)** não provocam mudanças na situação atual.

A **política 4 (transparência)** pode ter efeitos positivos a médio prazo, se a comunidade implementar o tratamento de *communities* para *black hole*, recebidas via IX.br.

Existe, contudo, o risco de que alguns participantes tenham configurado hoje o tratamento para certas *communities* para anúncios recebidos via IX.br, como para as *well known communities* e de *black hole*. Atualmente não há risco porque os servidores de rotas impedem a propagação de qualquer *community*. A transparência proposta na política 3 abriria a possibilidade de um ataque perpetuado por um AS X, envolvendo o anúncio dos prefixos do AS A, marcados com a *community* de *black hole* do AS B. Isso efetivamente interromperia a comunicação entre os ASs A e B, consistindo em um ataque de DOS. Para diminuir esse risco, o participante que implementar a *black hole* pode fazer uso das *communities* de validação de origem, aplicando-a apenas para anúncios confiáveis.

A **política 5 (validação de origem)** dependerá para seu êxito de seu uso efetivo pela comunidade de participantes. As informações de validação dos prefixos implícitas nessa *communities* serão úteis apenas se usadas para implementar filtros, e têm o potencial de aumentar a segurança e estabilidade do IX.br. Contudo, se os participantes não implementarem os filtros, o efeito será nulo. E se os filtros forem mal implementados pelos participantes, o efeito poderá ser o contrário, com riscos à segurança e à estabilidade da plataforma. Erros no processo de validação também podem oferecer risco se os filtros estiverem implementados de forma muito restritiva, aceitando apenas prefixos válidos, por exemplo.

6. **Implantação e diálogo com a comunidade**

As mudanças propostas nas políticas para o tratamento das *communities* no IX.br têm por objetivo resolver problemas operacionais claros e bem definidos e, por isso mesmo, têm potencial para resultar em ganhos tanto na operação do IX.br quanto para seus participantes.

O IX.br dá continuidade, com este documento, ao processo de diálogo sobre este assunto com a comunidade de participantes iniciado no IX Fórum em dezembro de 2015.

Dependendo do resultado de tal diálogo, o cronograma proposto para essas implementações é:

- **dezembro de 2016:** transparência ao MED, políticas em relação às *communities* 1 (filtros), 2 (*prepends*), 3 (identificação de origem) e 4 (transparência);

- **até julho de 2017:** mitigação de ocultamento de caminho e *community* de validação de origem.

Comentários e sugestões podem ser feitos via lista de e-mails do Grupo de Trabalho de Engenharia de Redes (GTER).

7. **Referências**

[1] https://tools.ietf.org/html/rfc7947
[2] https://tools.ietf.org/html/rfc7948
[3] https://tools.ietf.org/html/rfc1997
[4] https://tools.ietf.org/html/rfc1271
[5] https://tools.ietf.org/html/rfc4271
[6] https://tools.ietf.org/html/rfc4360