Núcleo de Informação e Coordenação do Ponto BR

Programa por uma Internet mais Segura

Ações no IX.br

Introdução

O IX.br está presente em 31 localidades no Brasil, por meio da instalação e operação de Pontos de Troca de Tráfego Internet (PTTs), sendo parte integrante da infraestrutura de rede da Internet do Brasil, onde Sistemas Autônomos (ASs) podem trocar tráfego nas regiões metropolitanas próximas.

Dois tipos de serviços são oferecidos aos participantes da troca de tráfego: (i) **o Acordo de Troca de Tráfego Multilateral** (ATM), chamado em inglês de *Multilateral Peering Agreement* (MLPA) e (ii) a **Troca de Tráfego Bilateral**, em inglês *Bilateral Peering Agreement* (BLPA). Os participantes do ATM trocam tráfego entre si: como regra geral, cada AS troca tráfego com todos os demais. Já na Troca de Tráfego Bilateral apenas dois ASs participam, utilizando-se ou não de um domínio de camada 2 exclusivo (uma VLAN bilateral).

O Acordo de Troca de Tráfego Multilateral (ATM), na prática, funciona com uma VLAN compartilhada para a troca de tráfego IPv4 (ATMv4) e outra para troca de tráfego IPv6 (ATMv6). Cada PTT possui dois ou mais *route servers,* que também são utilizados no Acordo de Troca de Tráfego Multilateral (ATM) para centralizar o recebimento de anúncios de rotas de todos os participantes da troca de tráfego, permitindo que, com uma única sessão BGP, a tabela de rotas da localidade seja carregada e mantida. O estabelecimento de sessões BGP com os *route servers* é condição necessária para participar do ATM. A maior parte dos participantes de um PTT participa da troca de tráfego multilateral, mas nem todos. Mesmo participantes que não estão no ATM podem estar presentes nas VLANs do ATMv4 ou ATMv6, para fins de monitoramento, ou outros fins.

Existem casos em que o participante está presente na VLAN do ATMv4 ou ATMv6 e não fecha sessão BGP com o *route server*, mas fecha sessões BGP diretamente com o roteador de outros participantes com os quais deseja trocar tráfego, usando os IPs fornecidos pelo IX.br. Ou seja, acordos bilaterais de troca de tráfego podem se utilizar tanto da VLAN de uso comum (ATMv4 ou ATMv6), como de VLANs específicas (VLANs bilaterais).

Desta forma, neste cenário, temos em cada PTT do IX.br:

- um **ambiente privado**, formado pelos Acordos Bilaterais com troca direta de tráfego através VLANs, sejam VLANs bilaterais ou as VLANs do ATMv4 e/ou ATMv6, e
- um **ambiente compartilhado** formado pelos participantes presentes nas VLANs do ATMv4 e/ou ATMv6 e com sessões BGP com os route servers.

Dentro do **Programa por uma Internet mais Segura** que o NIC.br está desenvolvendo com a comunidade da Internet, **este documento diz respeito a ações que serão implantadas no IX.br para aumentar a segurança dos *route servers***, onde a ocorrência de problemas em relação à tabela de rotas compartilhada pode afetar seriamente os ASs que participam ou não dos PTTs. **Trata-se de ações sobre o ambiente compartilhado.** Ocorrências no **ambiente privado não estão no escopo de atuação do NIC.br e do IX.br,** mas todas as recomendações feitas no programa por uma Internet mais segura, como por exemplo a adoção das ações propostas na iniciativa MANRS (Mutually Agreed Norms for Routing Security - https://www.manrs.org/), devem ser consideradas e aplicadas pelos gestores dos ASs envolvidos em relações privadas dentro do IX.br.

A segurança da Internet depende fundamentalmente da participação de todos os ASs. A segurança do ambiente de um Ponto de Troca de Tráfego Internet - PTT (*Internet Exchange Point* - IX) reflete o cuidado que cada rede participante adota internamente. Se todas as redes adotarem as melhores práticas recomendadas na configuração dos seus equipamentos, com certeza teremos um ambiente mais saudável no PTT. Configurar uma rede para evitar a propagação de problemas, ou seja, controlar o que sai de uma rede, é muito mais simples e econômico do que proteger a entrada da rede contra tudo o que existe no exterior. Se todos protegerem as saídas de suas redes, não haverá problemas na entrada do PTT. Esta é a filosofia do MANRS, que é uma iniciativa global, apoiada pela Internet Society, que fornece recomendações cruciais para eliminar ameaças causadas pelos problemas de roteamento mais comuns e tem como objetivos:

- Aumentar a conscientização e incentivar ações, com o compromisso dos apoiadores.
- Promover a cultura de responsabilidade coletiva para a resiliência e segurança do sistema de roteamento global da Internet.
- Demonstrar a capacidade do setor para abordar as questões de resiliência e segurança com espírito de responsabilidade coletiva.
- Fornecer uma estrutura para que os provedores de serviços de acesso à Internet (ISP) compreendam melhor e ajudem a solucionar os problemas relacionados à resiliência e segurança do roteamento da Internet.

Nos PTTs não há como atuar em todos os possíveis problemas causados por redes configuradas sem as devidas proteções, por restrições técnicas nos equipamentos de rede. Contudo, **podemos atuar na segurança dos *route servers***, com medidas que diminuam a possibilidade da ocorrência de sequestro de prefixos (*prefix hijack*) ou vazamento de rotas (*route leaks*) que têm causado tanto prejuízo e preocupação aos usuários da Internet brasileira.

Este documento descreve as ações já em uso e outras que serão implantadas em breve. O presente documento foi resultado de um processo amplo de consulta e interação com a comunidade, e leva em consideração o *feedback* recebido.

Aumento da Segurança dos Route Servers

Para aumentar a confiabilidade da tabela local de rotas do ATM de um PTT, validações devem ser executadas nos route servers, testando os prefixos recebidos dos participantes de diversas formas

diferentes, a fim de mitigar eventuais erros, ações maliciosas ou imperícia na configuração dos roteadores dos participantes da troca de tráfego. A partir dessas validações os prefixos são identificados com communities BGP, e por fim filtrados, ou não, de acordo com critérios específicos.

O Processo de Validação dos Anúncios no BGP

O processo como um todo é dividido em diferentes etapas:

1. O **route server recebe os prefixos**.
    - Cada participante tem definido um número máximo de prefixos que pode anunciar aos route servers. Se esse número for ultrapassado a sessão BGP é derrubada para proteção por 10 (dez) minutos. Caso no retorno o número máximo de prefixos seja ultrapassado, a sessão será derrubada indefinidamente e os demais passos do processo não se aplicam. Para aumentar o número máximo de prefixos anunciados o participante deverá abrir um chamado específico no portal do participante.

2. Os **anúncios são validados** segundo diversos critérios:
    - Verificação de prefixos não permitidos, ou AS PATHs não permitidos.
    - Verificação de origem do prefixo.
    - Verificação da política informada pelo participante ao IX.br.

    Para essas validações, diferentes tipos de testes podem ser feitos:
    - Verificação do tipo do AS ou prefixo: stub ou não stub, da região do LACNIC ou de outras regiões.
    - Comparação do anúncio com tabelas estáticas de prefixos ou ASNs não permitidos (bogons, prefixos do IX.br, etc).
    - Consulta a bases de dados externas, como RDAP, RPKI, IRRs ou outras.
    - Consulta a base de dados do IX.br (política definida pelos participantes).

3. **Cada prefixo é marcado com communities**, conforme o resultado das validações.
    - Note-se que para cada tipo de validação uma community BGP diferente, a ser especificada futuramente, será utilizada, de forma que será claro determinar por qual razão um determinado prefixo é considerado inválido.

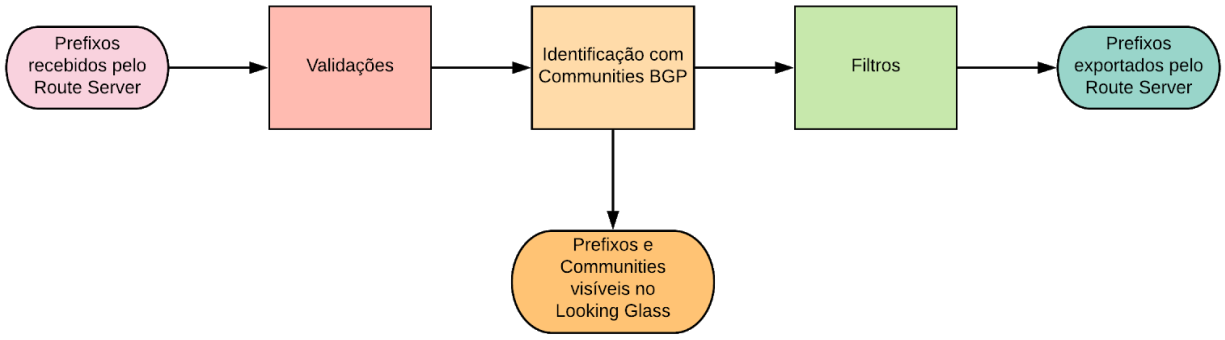
4. O resultado das validações é visível no **Looking Glass Web**, inclusive para prefixos que não sobreviverão aos filtros mais adiante no processo.
    - No Looking Glass Web será possível identificar visualmente de forma simples e descritiva se um prefixo será ou não exportado para os demais participantes e, para o caso do prefixo ser filtrado, qual a validação ou validações responsáveis pelo descarte do anúncio.
    - Note que, como já acontece atualmente, os participantes podem marcar seus anúncios com certas communities BGP, a fim de controlar o comportamento dos Route Servers, permitindo a exportação daquele anúncio específico apenas para um grupo determinado de outros participantes. Nesse caso um prefixo que aparece

no route server pode não ser exportado para um ou mais participantes. Essas communities usadas pelos próprios participantes continuarão visíveis da mesma forma como são hoje no Looking Glass Web, anonimizando os ASNs envolvidos nos filtros, a não ser que quem esteja visualizando esteja vinculado ao AS que fez o anúncio aos Route Servers.

5. Os **prefixos podem ser filtrados ou não, segundo as communities marcadas** e diversos critérios.
    - Alguns critérios são fixos (ex.: bogons são sempre descartados).
    - Alguns critérios podem ser escolhidos pelos participantes (ex.: filtragem ou não de prefixos em que a validação é inconclusiva, ou seja, não aparecem em uma ou mais bases de dados).

6. Os **prefixos que sobreviveram aos filtros são exportados** para os demais participantes.

O diagrama a seguir ilustra as diferentes etapas no Processo de Validação dos Anúncios BGP:



As validações, identificação com communities BGP e filtros são feitos pelos Route Servers, em tempo real, conforme os prefixos são recebidos. Contudo, esse processo em tempo real se baseia apenas na configuração estática dos Route Servers. As bases de dados do IX.br e externas não são consultadas em tempo real.

Informações são coletadas periodicamente, ou no momento da ativação. Informações como por exemplo ASs participantes do IX.br, prefixos anunciados, AS-PATHs, dados informados no portal do IX.br, dados provenientes de bases externas como RDAP, IRR, etc. Com base no conjunto dessas informações são construídas periodicamente prefix lists e outros elementos integrantes das configurações dos Route Servers.

É importante notar então que a mudança de uma informação em uma base externa, como a designação de um prefixo no Registro.br, ou a inclusão de um cliente de trânsito no AS-SET publicado em um IRR, ou mesmo a mudança nas informações prestadas via portal do IX.br, não terão efeito imediato sobre o processo de validação de anúncios BGP nos Route Servers. Os efeitos ocorrerão em até 24h ou com periodicidade menor a ser definida no futuro pelo IX.br.

Um exceção importante é a base RPKI. Os Route Servers são capazes de consultar um espelho local do RPKI em tempo real, de forma que os efeitos de modificações ocorrerão com atrasos menores.

Como será a implantação do Processo de Validação dos Anúncios BGP no IX.br

Apresentamos a seguir uma série de critérios de validação e filtros a serem implantados nos Route Servers do IX.br. Para cada um classificamos como o tempo previsto de implementação como:

- EM USO;
- CURTO (45 dias);
- MÉDIO (120 dias) ou
- LONGO (12 a 18 meses).

O **tempo para implementação** muda de acordo com diversos critérios:

- **Viabilidade técnica e facilidade de implantação:** por exemplo, validação dos prefixos contra uma lista de bogons está já EM USO, é uma validação extremamente simples e muito efetiva;
- **Maturidade técnica ou grau de adoção da tecnologia**: por exemplo, validação de origem para stubs da área do LACNIC no RDAP requer a criação de software específico, por isso o prazo para implantação é MÉDIO, enquanto a validação de origem por IRR, ainda requer um melhor amadurecimento de questões ligadas à segurança e disponibilidade para uso sem custo, por isso seu prazo de implantação é LONGO.

Limite do número de prefixos anunciados

Atualmente, a política padrão EM USO no IX.br é de aceitar até 100 prefixos IPv4 e até 100 prefixos IPv6 nas respectivas sessões com os servidores de rotas. Durante o processo de ativação, ou posteriormente via chamado, esse número pode ser aumentado, se houver necessidade.
Caso esse número seja ultrapassado a sessão BGP é derrubada por 10 (dez) minutos e reativada. Caso o número de prefixos máximo seja ultrapassado a sessão será novamente derrubada e é necessário que o participante abra um chamado para que seja restabelecida manualmente com um novo limite para o número de prefixos. Esse filtro tem o objetivo principal de evitar anúncios,

por erro de configuração, da tabela BGP completa, ou de prefixos aprendidos dos próprios servidores de rotas.

A desagregação dos prefixos na Internet deve ser usada com moderação. A desagregação pode ser feita de forma estudada e planejada, para engenharia de tráfego, por exemplo. Essa quantidade máxima padrão de prefixos relativamente grande aceita pelos servidores de rotas do IX.br não tem de forma alguma o objetivo de estimular a desagregação dos prefixos. Esse número atualmente atende tanto a participantes pequenos, Sistemas Autônomos stubs, que anunciam apenas seus próprios prefixos, como também à maioria dos participantes maiores, que fornecem trânsito para outros Sistemas Autônomos e anunciam uma quantidade relativamente grande de prefixos por essa razão.

Validações

1. **Validação de prefixos ou ASNs não permitidos na rede do IX.br**

    a. **Tamanho dos prefixos**

    Os prefixos com máscaras entre /8 e /24 inclusive para IPv4, ou entre /3 e /48 inclusive para IPv6 serão aceitos. Prefixos IPv4 com máscaras entre /25 (inclusive) e /31 (inclusive) serão marcados como inválidos. Prefixos IPv6 com máscaras entre /49 (inclusive) e /127 (inclusive) serão marcados como inválidos.

    Prefixos IPv4 com máscaras /32 e prefixos IPv6 com máscaras /128 serão considerados como prefixos para blackhole, desde que acompanhados da community apropriada, e analisados posteriormente segundo outros critérios. Eles serão marcados como válidos, pelo critério de tamanho. Caso não estejam marcados com a community apropriada, serão marcados como inválidos.

    Resumindo, para fins de clareza, segue tabela com a classificação do prefixo segundo a análise de tamanho:

Tipo de endereço	Válido	Inválido
IPv6	Entre /3 e /48 /128 (se marcado com community de blackhole)	< /3 > /48 e < /128 /128 (se não marcado com community de blackhole)
IPv4	Entre /8 e /24 /32 (se marcado com community de blackhole)	< /8 > /24 e < /32 /32 (se não marcado com community de blackhole)

Atualmente já existem filtros EM USO na rede do IX.br, descartando anúncios com prefixos maiores que /48 IPv6 e maiores que /24 IPv4. Na nova implementação os anúncios inválidos serão marcados com communities apropriadas e visíveis no Looking Glass Web, para conhecimento e acompanhamento do AS. Posteriormente serão filtrados. A nova implementação também permitirá em alguns casos anúncios de /64 IPv6, /128 IPv6 ou /32 IPv4 como blackholes. Essa mudança também possibilitará o desenvolvimento de ações educativas junto aos ASs, para evitar que este tipo de situação ocorra com outros peers e a geração de um indicador (KPÌ) sobre o tema.

Enquanto a validação e filtros para blackhole não forem implementados, os prefixos /64 ou /128 IPv6, e /24 IPv4, serão considerados inválidos segundo o critério de tamanho.

Tempo para implementação/status: CURTO.

b. Prefixos bogons ou indevidos

Os anúncios recebidos que contenham blocos de endereços utilizando espaço de endereçamento reservado, conforme lista a seguir, são marcados com communities específicas e posteriormente descartados.

Prefixos IPv4 não permitidos:

```
0.0.0.0/8 prefixlen >= 8          # 'this' network [RFC1122]
10.0.0.0/8 prefixlen >= 8         # private space [RFC1918]
100.64.0.0/10 prefixlen >= 10     # CGN Shared [RFC6598]
127.0.0.0/8 prefixlen >= 8        # localhost [RFC1122]
169.254.0.0/16 prefixlen >= 16    # link local [RFC3927]
172.16.0.0/12 prefixlen >= 12     # private space [RFC1918]
192.0.0.0/24 prefixlen >= 24      # IETF Protocol Assignments
192.0.0.0/29 prefixlen >= 29      # DS-Lite [RFC6333]
192.0.2.0/24 prefixlen >= 24      # TEST-NET-1 [RFC5737]
192.88.99.0/24 prefixlen >= 24    # 6to4 Relay Anycast [RFC3068]
192.168.0.0/16 prefixlen >= 16    # private space [RFC1918]
198.18.0.0/15 prefixlen >= 15     # benchmarking [RFC2544]
198.51.100.0/24 prefixlen >= 24   # TEST-NET-2 [RFC5737]
203.0.113.0/24 prefixlen >= 24    # TEST-NET-3 [RFC5737]
224.0.0.0/4 prefixlen >= 4        # multicast
240.0.0.0/4 prefixlen >= 4        # reserved for future use
255.255.255.255/32 prefixlen = 32 # Limited Broadcast [RFC0919]
```

Prefixos IPv6 que são permitidos (todos os demais são identificados como não permitidos):

2001:0200::/23 prefixlen aceitos /23 a /48
2001:0400::/23 prefixlen aceitos /23 a /48
2001:0600::/23 prefixlen aceitos /23 a /48
2001:0800::/23 prefixlen aceitos /23 a /48
2001:0a00::/23 prefixlen aceitos /23 a /48
2001:0c00::/23 prefixlen aceitos /23 a /48
2001:0e00::/23 prefixlen aceitos /23 a /48
2001:1200::/23 prefixlen aceitos /23 a /48
2001:1400::/23 prefixlen aceitos /23 a /48
2001:1600::/23 prefixlen aceitos /23 a /48
2001:1800::/23 prefixlen aceitos /23 a /48
2001:1a00::/23 prefixlen aceitos /23 a /48
2001:1c00::/22 prefixlen aceitos /22 a /48
2001:2000::/20 prefixlen aceitos /20 a /48
2001:3000::/21 prefixlen aceitos /21 a /48
2001:3800::/22 prefixlen aceitos /22 a /48
2001:4000::/23 prefixlen aceitos /23 a /48
2001:4200::/23 prefixlen aceitos /23 a /48
2001:4400::/23 prefixlen aceitos /23 a /48
2001:4600::/23 prefixlen aceitos /23 a /48
2001:4800::/23 prefixlen aceitos /23 a /48
2001:4a00::/23 prefixlen aceitos /23 a /48
2001:4c00::/23 prefixlen aceitos /23 a /48
2001:5000::/20 prefixlen aceitos /20 a /48
2001:8000::/19 prefixlen aceitos /19 a /48
2001:a000::/20 prefixlen aceitos /20 a /48
2001:b000::/20 prefixlen aceitos /20 a /48
2002:0000::/16 prefixlen aceitos /16 a /48
2003:0000::/18 prefixlen aceitos /18 a /48
2400:0000::/12 prefixlen aceitos /12 a /48
2600:0000::/12 prefixlen aceitos /12 a /48
2610:0000::/23 prefixlen aceitos /23 a /48
2620:0000::/23 prefixlen aceitos /23 a /48
2800:0000::/12 prefixlen aceitos /12 a /48
2a00:0000::/12 prefixlen aceitos /12 a /48
2c00:0000::/12 prefixlen aceitos /12 a /48

Além desses, são explicitamente não permitidos:

```
2001::/23 prefixlen >= 23          # IETF Prot Assignments [RFC2928]
2001::/32 prefixlen >= 32          # TEREDO [RFC4380]
2002::/16 prefixlen >= 32          # 6to4 [RFC3056]
2001:2::/48 prefixlen >= 48        # BMWG [RFC5180]
2001:10::/28 prefixlen >= 28       # ORCHID [RFC4843]
```

```
2001:20::/28 prefixlen >= 28        # ORCHIDv2 [RFC7343]
2001:db8::/32 prefixlen >= 32       # document range [RFC3849]
```

Atualmente já existem filtros EM USO na rede do IX.br, descartando anúncios com prefixos bogons. Na nova implementação os anúncios inválidos serão marcados com communities apropriadas e visíveis no Looking Glass Web, para conhecimento e acompanhamento do AS. Posteriormente serão filtrados. Essa mudança também possibilitará o desenvolvimento de ações educativas junto aos ASs, para evitar que este tipo de situação ocorra com outros peers e a geração de um indicador (KPÌ) sobre o tema.

Tempo para implementação/status: CURTO.

c. Prefixos utilizados pelo IX.br

O espaço de endereçamento utilizado para o IX.br a fim de endereçar os roteadores que participam da troca de tráfego da localidade, mesmo que utilize endereços públicos IPv4 e globais IPv6, NÃO DEVE ser roteado (não deve ser anunciado por qualquer participante, e não é anunciado pelo IX.br ou pelo NIC.br).

Endereços públicos IPv4 e globais IPv6 são utilizados para facilitar o trabalho de investigação de problemas de conectividade e/ou roteamento (*troubleshooting*).

Atualmente, já existem filtros EM USO na rede do IX para este caso, descartando os prefixos. Na nova implementação dos filtros, os anúncios inválidos com prefixos utilizados pelo IX.br serão marcados com uma community informando a irregularidade, exportando o anúncio apenas para o Looking Glass Web para conhecimento e acompanhamento do AS.

Tempo para implementação/status: CURTO.

É importante lembrar que a política de Requisitos Técnicos do IX.br já define que: *"o espaço de endereçamento da rede de cada localidade do IX.br, ou seja, o endereçamento utilizado nas portas dos roteadores ligados ao IX, não deve ser anunciado a outras redes. Recomenda-se que esses endereços também não sejam anunciados internamente na rede dos participantes, o que implica no uso de next-hop-self para o anúncio interno de rotas aprendidas via IX"*.

A divulgação da rede do IX.br no roteamento interno de um participante ou para a Internet implica em sério risco de segurança, possibilitando, por exemplo, ataques DDoS direcionados aos roteadores dos demais participantes e aos Route Servers. Se for detectado o anúncio dos prefixos do IX.br por um participante, o mesmo é notificado e, caso a situação persista, pode ser desligado da rede do IX.br.

d. ASNs bogons ou indevidos

Anúncios que contenham ASNs reservados (bogons) em qualquer parte do AS-PATH serão marcados com uma community específica e posteriormente rejeitados.

ASNs não permitidos:

0 - RFC 7607
23456 - RFC 6793 AS_TRANS
64496 a 64511 - RFC 5398 and documentation/example ASNs
64512 a 65534 - RFC 6996 Private ASNs
65535 - RFC 7300 Last 16 bit ASN
65536 a 65551 - RFC 5398 and documentation/example ASNs
65552 a 131071 - IANA reserved ASNs
4200000000 a 4294967294 - RFC 6996 Private ASNs
4294967295 - RFC 7300 Last 32 bit ASN

Tempo para implementação/status: CURTO.

e. ASNs de redes livres de trânsito no AS-PATH

Validação e identificação com a community BGP apropriada como inválidos, dos anúncios que contenham no AS-PATH, após o ASN do participante, o ASN de redes conhecidas como livres de trânsito, tipicamente os principais Tier-1:

174 - Cogent
209 - Centurylink
286 - KPN
701 - Verizon
702 - Verizon
703 - Verizon
1239 - Sprint
1299 - Telia
2828 - XO
2914 - NTT
3257 - GTT Communications
3320 - Deutsche Telekom
3356 - Level 3
3491 - PCCW Global
3549 - Level 3
3561 - Centurylink
4134 - China Telecom
4323 - TWTC
4436 - GTT

5511 - Orange
6453 - Tata Communications
6461 - Zayo
6762 - Telecom Italia Sparkle
6830 - UPC
6939 - HE
7018 - AT&T
12956 - TIWS

A presença destes ASNs no AS-PATH é um indicativo de má configuração no roteador de participante da troca de tráfego. Essas redes tipicamente não contratam trânsito de outras redes. A presença do ASN de uma delas no AS-PATH indica que o participante, ou um cliente de trânsito do participante está 'fornecendo trânsito' à mesma, o que indica um erro de configuração ou outro tipo de problema.

Diversos comentários foram feitos em relação a este tipo de validação, durante a fase de consulta da versão anterior deste documento, resumidos a seguir:

- A hipótese de que as redes listadas são realmente “livres de trânsito” pode não ser válida. Foram relatados casos em que algumas delas contratam trânsito parcial de operadoras locais (brasileiras) para melhorar sua conectividade. Um estudo aprofundado considerando a tabela de rotas das diversas localidades será realizado para determinar a situação atual.
- Foi sugerida a inclusão de redes livres de trânsito no âmbito brasileiro, que só contratariam realmente trânsito internacional, tais como RNP, Embratel Tim, Telefônica, Oi, Claro, etc. A princípio a proposta parece válida, o que será confirmado analisando-se a tabela de rotas das diversas localidades, assim como diretamente com as empresas.
- Inclusão dos ASs de provedores de serviço/conteúdo como Google, Netflix, Amazon, Microsoft, etc. na lista de ASNs. Neste caso podemos solicitar um posicionamento formal destes ASs quanto à política de filtragem a ser adotada nas localidades do IX.br.

Obs: em 28/03/2018 no IX.br SP foram encontrados 90 anúncios contendo os ASNs listados acima, com um tráfego diário de 36.8 TB e uma média de 3.5 Gbps.

A validação e identificação dos prefixos nessa situação será implementada a CURTO prazo. No entanto serão realizados estudos aprofundados e consultas às empresas envolvidas ANTES DE USAR TAL INFORMAÇÃO PARA FILTROS. Caso seja necessário, serão estabelecidos casos de exceção para participantes do IX.br que de fato oferecem trânsito IP para tais redes, para que prefixos nessas condições anunciados por eles não sejam marcados.

Os ASNs presentes nessa lista serão revisados periodicamente, com base na análise da tabela de rotas global da Internet.

Tempo para implementação/status: CURTO.

2. Validação de origem

A validação da origem tem por objetivo verificar se o AS que originou o anúncio, ou seja, o AS mais à direita no AS-PATH, tem realmente o direito de anunciar aquele prefixo.
Nos exemplos de anúncios a seguir, o que se pretende verificar com a validação de origem é se o AS 64511 tem o prefixo 192.0.2.0/24 atribuído para ele; se o AS 65537 tem o prefixo 198.51.100.0/24 atribuído a ele, e se o AS 65536 tem o prefixo 203.0.113.0/24 atribuído a ele.

```
Prefix              AS-PATH
192.0.2.0/24        0 64500 64499 64511 i
198.51.100.0/24     0 64500 64500 64500 65540 65536 65537 i
203.0.113.0/24      0 65536 i
```

Essa ação promove a utilização de bases de dados externas para a validação de anúncios.

Conforme já anunciado anteriormente no documento em que tratamos da “Proposta para mudança nos servidores de rotas e nas políticas de tratamento de communities BGP no IX.br”, os anúncios recebidos pelos route servers serão marcados como válidos, inválidos ou desconhecidos de acordo com pesquisas realizadas em 3 tipos de serviços/bases de dados: RDAP, IRR e RPKI.

a. RDAP

O RDAP (Registration Data Access Protocol) pode ser encarado como uma API para acesso a uma base de dados Whois, como a do Registro.br

O Registro.br e o LACNIC fazem uma correlação direta entre os prefixos e o ASNs atribuídos a uma mesma organização. Ou seja, consultando-se os prefixos é possível relacioná-los a um ASN. E consultando-se um ASN, é possível relacioná-lo aos seus prefixos.

No ARIN não há uma correlação direta para todas as atribuições. Contudo tanto ASNs quanto prefixos são atribuídos a uma organização. Consultando-se um ASN é possível chegar à organização para a qual o mesmo foi atribuído, e então aos prefixos atribuídos àquela organização. De forma similar, tendo-se um prefixo, é possível descobrir o ASN ou ASNs atribuídos à mesma organização.

Nos demais RIRs, até onde os autores deste documento têm conhecimento, não é possível estabelecer, por meio de consultas a bases de dados públicas, uma relação direta entre os prefixos e os ASNs atribuídos a uma mesma organização.

No Brasil, a atualização da base de dados consultada via RDAP é feita pelo Registro.br no processo de atribuição dos recursos de numeração, não sendo necessário qualquer tipo de cadastro por parte do ASN. Por outro lado, é fundamental que delegações ou transferência de blocos entre ASNs sejam devidamente informadas e registradas no Registro.br, sem o que poderá haver rejeição de anúncios.

A validação no RDAP do Registro.br será implementada a CURTO prazo. Haverá uma community BGP apropriada para:

- indicar se o prefixo consta ou não na base, caso não conste na base será marcado como desconhecido
- indicar se o ASN que origina o prefixo, isto é, o ASN mais à direita no AS-PATH, é ou não o mesmo ASN ao qual o prefixo está atribuído na base do Registro.br

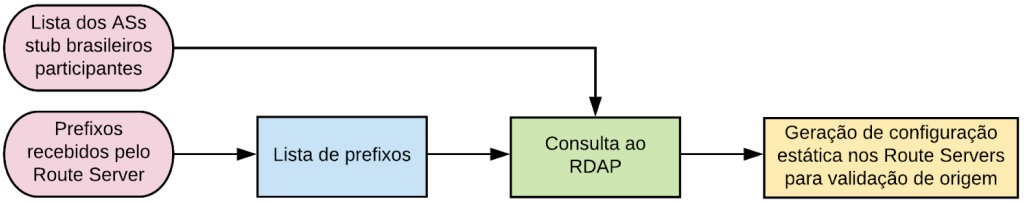
No lugar de consultas diretas ao RDAP, no caso do Registro.br, pode-se optar também por se consultar o arquivo disponível no endereço a seguir, atualizado diariamente, e com informação equivalente:

- ftp://ftp.registro.br/pub/numeracao/origin/nicbr-asn-blk-latest.txt

A possibilidade de validação de origem também no RDAP do LACNIC e do ARIN serão estudadas em maior profundidade. Questões práticas como velocidade das consultas e limite de consultas às respectivas bases precisam ser avaliadas, entre outras. É previsto um tempo para implementação LONGO.

Outra fonte de dados que poderá ser utilizada são os arquivos disponibilizados pelo LACNIC em ftp://ftp.lacnic.net/pub/stats/ contento as atribuições feitas pelos demais RIRs: AFRINIC, APNIC, ARIN, RIPENCC e o próprio LACNIC. Estas informações são disponibilizadas diariamente. Tempo para implementação MÉDIO.

Note que a validação de origem via RDAP ou WHOIS não será feita imediatamente, ao anunciar um novo prefixo para os Route Servers. Estas validações são feitas por meio de uma configuração estática (prefix lists e outras) nos Route Servers. Essas configurações são geradas periodicamente com base em consultas feitas às bases RDAP tendo como base a lista corrente de prefixos anunciada aos Route Servers e a lista de ASs stub brasileiros participantes.



Vale notar que para os Sistemas Autônomos STUB no Brasil, por definição, o AS que origina o prefixo é o mesmo AS do participante do IX.br. Isto é, por definição, só há um AS no AS-PATH. A validação de origem feita no RDAP do Registro.br se aplica também para os Sistemas Autônomos STUB no Brasil.

b. IRR

Os IRRs são bases de dados que armazenam políticas de roteamento descritas em uma linguagem denominada Routing Policy Specification Language (RPSL). Estas bases de dados são distribuídas e operadas por diversas organizações como RIRs (Regional Internet Registry), empresas de telecom, etc. Algumas dessas bases operam como serviços pagos, como o RADB, outras são gratuitas, como o TC e bases operadas por RIRs.

Numa base IRR é possível informar:

- qual AS origina um determinado prefixo (essa é justamente a informação a ser usada na validação de origem dos prefixos):
    - Por exemplo, ao consultar o prefixo 200.160.0.0/24 nas bases de IRR se encontra a seguinte informação, que mostra que o AS que o origina é o AS22548:

```
route: 200.160.0.0/20
descr: Registro.BR Network
origin: AS22548
(...)
```

Os IRRs também armazenam outros tipos de informações:

- quais são os AS que dão trânsito a um determinado AS (políticas de import e export):
    - Por exemplo, ao consultar o AS22548 nas bases de IRR se encontra a seguinte informação, mostrando que seus trânsitos são os ASs 3549, 12989, 16735 e 52320:

```
aut-num: AS22548
(...)
import: from AS3549 accept ANY
import: from AS12989 accept ANY
import: from AS16735 accept ANY
import: from AS52320 accept ANY
mp-import: from AS3549 accept ANY
mp-import: from AS12989 accept ANY
mp-import: from AS16735 accept ANY
mp-import: from AS52320 accept ANY
export: to AS3549 announce AS22548 AND {200.160.0.0/20}
export: to AS12989 announce AS22548 AND {200.160.0.0/20}
export: to AS16735 announce AS22548 AND {200.160.0.0/20}
export: to AS52320 announce AS22548 AND {200.160.0.0/20}
mp-export: to AS3549 announce AS22548 AND {2001:12ff::/32}
mp-export: to AS12989 announce AS22548 AND {2001:12ff::/32}
mp-export: to AS16735 announce AS22548 AND {2001:12ff::/32}
```

```
mp-export: to AS52320 announce AS22548 AND {2001:12ff::/32}
(...)
```

- quais são ASs anunciados via BGP (clientes de trânsito, normalmente) de um determinado AS (AS-SET):
    - Por exemplo, ao se consultar o AS22548 no PeeringDB é possível verificar que o seu AS-SET é denominado AS-NIC-BR

```
Organização: NIC.br
Também conhecido como: Nucleo de Informacao e Coordenacao do
Ponto BR
Website da Empresa: http://nic.br
ASN primário: 22548
Registro de IRR: AS-NIC-BR
(...)
```

    - Ao se consultar o AS SET AS-NIC-BR nas bases de IRR, pode-se observar que os AS anunciados no BGP pelo AS22548 são os ASs 10906, 11284, 11644, etc:

```
as-set: AS-NIC-BR
descr: Nucleo de Informacao e Coordenacao do Ponto BR
members: AS10906
members: AS11284
members: AS11644
members: AS11752
members: AS12136
members: AS14026
members: AS14650
members: AS20121
members: AS22548
members: AS26162
members: AS53035
(...)
```

Existem serviços que têm cópias (espelhos) das diversas bases existentes, de modo a oferecer uma visão mais completa sobre as bases IRR existentes.

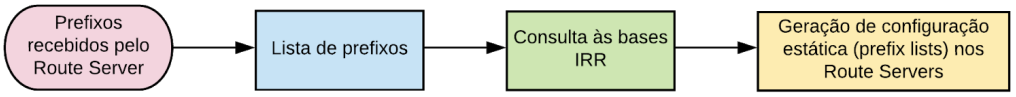
A informação nas bases IRR não é totalmente confiável no que tange a seu uso para validação de origem, visto que é possível que um terceiro insira em uma dada base informações sobre prefixos ou ASNs que não administra. Isso reforça a importância de que os administradores dos ASs tenham suas informações publicadas em pelo menos um IRR. Visto que nesse caso, se alguém inserir indevidamente informações inválidas sobre um prefixo ou ASN, estas ao menos se mostrarão conflitantes numa consulta com as informações corretas, inseridas pelo administrador dos recursos. Se não houver a informação cadastrada pelo real administrador do recurso, tudo que se obterá em uma consulta serão as informações indevidamente inseridas por terceiros, que serão provavelmente interpretadas como corretas.

Para fins de validação de origem no IRR, se houver pelo menos um registro no IRR apontando que a origem é válida, consideraremos como válida, mesmo que haja outros registros conflitantes.

A identificação dos anúncios como válidos ou não, segundo a informação da origem encontrada nas bases IRR, será implementada a LONGO prazo. No entanto serão realizados estudos aprofundados ANTES DE USAR TAL INFORMAÇÃO PARA FILTROS.

Uma community BGP, ou communities BGP apropriadas serão usadas para indicar se o prefixo tem em seu AS-PATH um ASN origem, o mais à direita (right-most) no AS_SEQUENCE, válido segundo as bases IRR, ou se é inválido ou desconhecido nas mesmas.

Note que a validação de origem via IRR não será feita imediatamente, ao anunciar um novo prefixo para os Route Servers. Estas validações são feitas por meio de uma configuração estática (prefix lists e outras) nos Route Servers. Essas configurações são geradas periodicamente com base em consultas feitas às bases IRR tendo como base a lista corrente de prefixos anunciada aos Route Servers.



Tempo para implementação/status: MÉDIO.

c. RPKI

O RPKI (Resource Public Key Infrastructure) é um serviço implementado pelos RIRs e NIRs, por meio do qual a organização detentora de um prefixo informa qual Sistema Autônomo, ou Sistemas Autônomos, estão autorizados a anunciá-lo.

O sistema utiliza uma infraestrutura de certificados de chaves públicas para dar segurança ao roteamento da Internet, através da geração de atestados chamados Route Origination Authorization (ROAs).

O RPKI é muito confiável para a validação de origem, contudo é um serviço ainda não disponível no Brasil e com pouca adesão dos Sistemas Autônomos globalmente.

Uma community BGP, ou communities BGP apropriadas serão usadas para indicar se o prefixo tem em seu AS-PATH um ASN de origem válido, segundo o RPKI, ou se é inválido ou desconhecido.

Tempo para implementação: MÉDIO.

3. Validação da política de roteamento do participante do IX.br

A validação da política de roteamento do participante tem por objetivo verificar se a política de roteamento informada para o IX.br é condizente com os anúncios para os Route Servers.

Por política de roteamento neste contexto entende-se:

- a informação sobre se o participante é ou não um AS stub brasileiro;
- caso não seja, a lista completa de ASs anunciada pelo participante aos Route Servers do IX.br (que consiste normalmente nos ASs clientes de trânsito do participante).

Ou seja, o participante informa ao IX.br por um meio independente do BGP quais anúncios pretende fazer, e o IX.br verifica se os anúncios efetivamente feitos via BGP está de acordo com essa informação.

Cada prefixo recebido pelo Route Server será identificado com uma community apropriada, indicando se o mesmo é válido ou não, segundo a informação do participante.

a. Sistemas Autônomos STUBs brasileiro

ASNs conectados ao IX.br podem ser classificados em duas categorias: stub ou trânsito:

- Um ASN stub é aquele que está conectado diretamente ao IX.br, anunciando apenas os seus próprios prefixos, não existindo outro ASN no AS-PATH.
- Já um ASN trânsito é aquele que anuncia prefixos de outros ASNs, além dos seus, com AS-PATH podendo conter múltiplos ASNs.

Durante a etapa de quarentena do processo de ativação do participante no IX.br, serão analisados os anúncios recebidos e apresentada a classificação do ASN como stub ou trânsito. A classificação inicial poderá ser alterada a qualquer momento através do portal do participante do IX.br.

Quando da implantação do processo, para os participantes já conectados faremos a análise e a classificação baseada na tabela de rotas em vigor.

O AS stub que eventualmente passe a dar trânsito a outros ASs, deverá especificar no portal do participante do IX.br que sua classificação deverá mudar para trânsito.

Para um AS stub, a validação de origem do prefixo, feita via RDAP, é na prática equivalente a validar a política de roteamento, visto que um stub, por definição, apenas anuncia prefixos atribuídos ao próprio AS.

O AS stub brasileiro será identificado como tal por meio de uma community ou communities apropriadas.

Tempo para implementação/status: CURTO.

b. Prefixos e ASNs informados ao IX.br

Para os ASs de trânsito participantes do IX.br é impossível inferir os prefixos que irá anunciar, além dos prefixos atribuídos a ele próprio. Essa informação deve vir obrigatoriamente do próprio participante.

O IX.br solicitará aos participantes ASs de trânsito que:

1. **Cadastre um AS-SET em alguma base IRR**, que englobe TODOS os ASs que pretende anunciar para os Route Servers.

   Por exemplo, o AS-SET do AS22548, foi cadastrado no IRR RADB, com a seguinte informação:

   ```
   as-set: AS-NIC-BR
   descr: Nucleo de Informacao e Coordenacao do Ponto BR
   members: AS10906
   members: AS11284
   members: AS11644
   members: AS11752
   members: AS12136
   members: AS14026
   members: AS14650
   members: AS20121
   members: AS22548
   members: AS26162
   members: AS53035
   (...)
   ```

2. **Informe no campo Registro IRR no PeeringDB o seu AS-SET**, ou seja, informe no PeeringDB o nome do seu AS-SET no formato especificado pela RFC 4012 e preferencialmente a base IRR em que o objeto foi registrado.

   O PeeringDB será a fonte utilizada para a obtenção do nome do AS-SET utilizado, assim é fundamental que este cadastro seja feito.

   Por exemplo, no PeeringDB encontramos a seguinte informação sobre o AS SET do AS22548:

   ```
   Organização: NIC.br
   Também conhecido como: Nucleo de Informacao e Coordenacao do Ponto BR
   Website da Empresa: http://nic.br
   ASN primário: 22548
   Registro de IRR: AS-NIC-BR
   ```

(...)

O PeeringDB é um serviço que facilita a troca de informações relacionadas a peering. Especificamente, é um banco de dados de redes que fazem peering, onde cada AS pode informar se faz peering, em quais IXs ou datacenters, qual sua política de peering, etc. Seu uso é gratuíto.

De posse dessas informações o IX.br poderá validar os AS-PATHs dos anúncios, observando o primeiro ASN imediatamente à direita do ASN do participante.

Por exemplo, vamos considerar o participante AS64500. Ele informou um AS-SET composto pelos ASNs: 64499, 65540, 65550. Os anúncios no Route Server são os seguintes:

```
Prefix               AS-PATH
192.0.2.0/24         0 64500 64499 64511 i
198.51.100.0/24      0 64500 64500 64500 65540 65536 65537 i
203.0.113.0/24       0 64500 65536 i
```

Nesse exemplo, o primeiro e o segundo anúncios são válidos, mas o terceiro não é, porque o AS65536 não está no AS-SET.

O anúncio será identificado com a community, ou communities, apropriadas, para identificar se é válido ou não do ponto de vista da política de roteamento informada, a community ou communities também permitirão identificar se a política de roteamento foi ou não informada.

Tempo para implementação/status: MÉDIO.

4. Validação de prefixos para BLACK HOLE para Sistemas Autônomos STUB brasileiros

Os anúncios recebidos com máscara /128 para prefixos IPv6 ou /32 para prefixos IPv4 serão identificados por meio de uma community, ou communities apropriadas, como prefixos de blackhole. Serão marcados como válidos se:

1. forem de ASs stub brasileiros e também
2. forem válidos via RDAP (base do Registro.br)

Serão marcados como inválidos caso não sejam de ASs stub brasileiros ou caso não sejam válidos via RDAP.

Tempo para implementação/status: MÉDIO.

Resumo das Validações

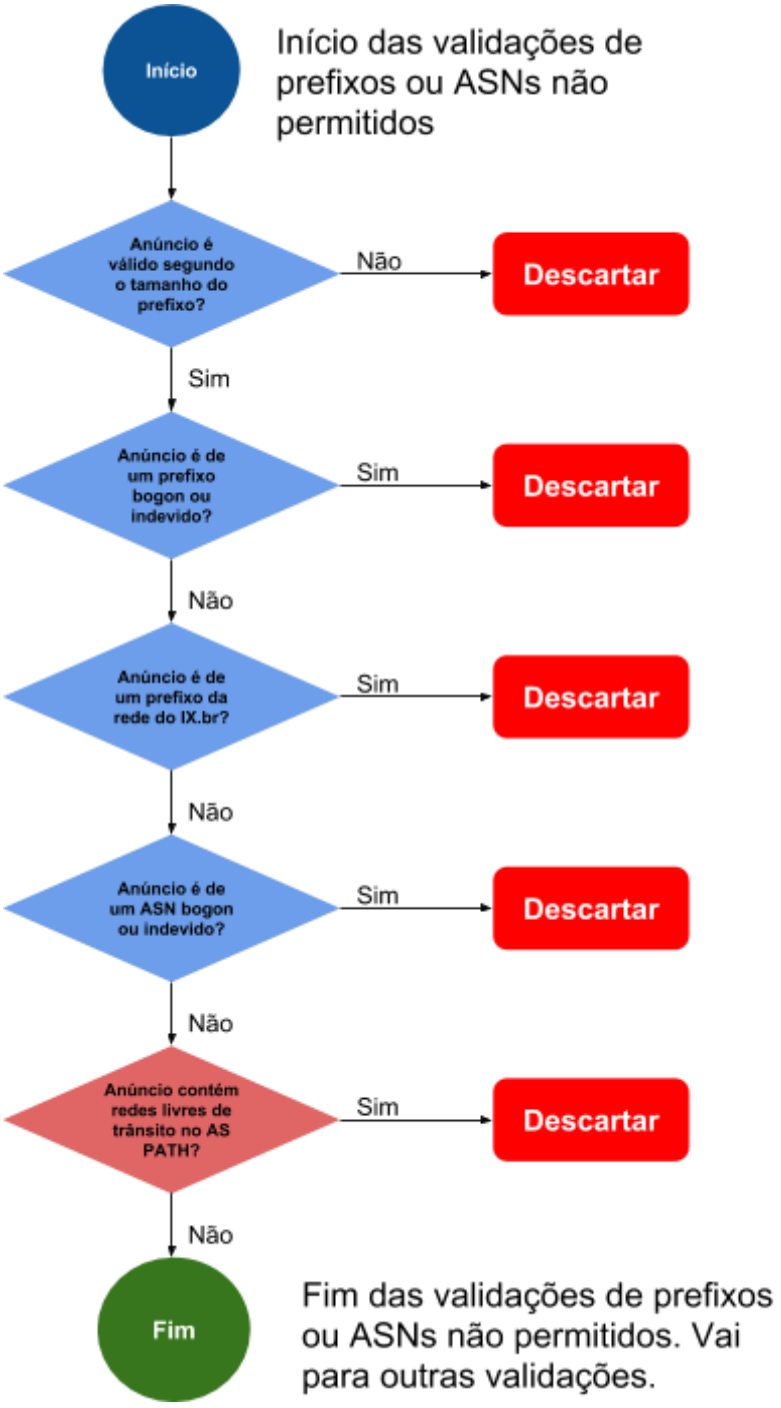
O quadro a seguir resume os tipos de validação realizados, seus prazos de implantação e resultados possíveis.

Tipo	Subtipo	Tempo para implantação da validação	Tempo para implantação do filtro	Resultados possíveis
Validação de prefixos ou ASNs não permitidos na rede do IX.br	Tamanho dos prefixos	EM USO	D0	Válido ou não
	Prefixos bogons ou indevidos	EM USO	D0	Válido ou não
	Prefixos utilizados pelo IX	EM USO	D0	Válido ou não
	ASNs bogons ou indevidos	CURTO	D + 30 dias	Válido ou não
	ASNs de redes livres de trânsito	CURTO	D + 30 dias	Válido ou não
Validação de origem	Prefixo está na base do Registro.br	CURTO	D + 30 dias	Sim ou não
	Origem válida segundo RDAP no Registro.br	CURTO	D + 30 dias	Válido ou não
	Origem válida segundo RDAP/WHOIS no LACNIC e ARIN	LONGO	D + 30 dias	Válido ou não
	Origem válida segundo IRR	LONGO	D + 30 dias	Válido, não válido ou desconhecido
	Origem válida segundo RPKI	MÉDIO	D + 30 dias	Válido, não válido ou desconhecido
Validação da política de roteamento	ASN é stub brasileiro	CURTO	D0	Sim ou não
	Validação do AS-PATH segundo AS SET do participante	LONGO	D + 30 dias	Válido, não válido, ou AS SET não informado
Validação de prefixos para BLACK HOLE	Sistemas Autônomos STUB brasileiros	MÉDIO	D + 30 dias	Válido ou não

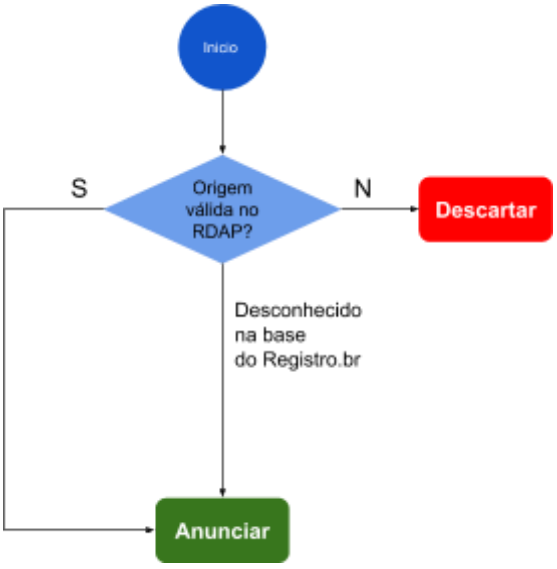
Filtros

Com base nas validações realizadas, serão implementados filtros, antes da exportação dos anúncios para cada participante.

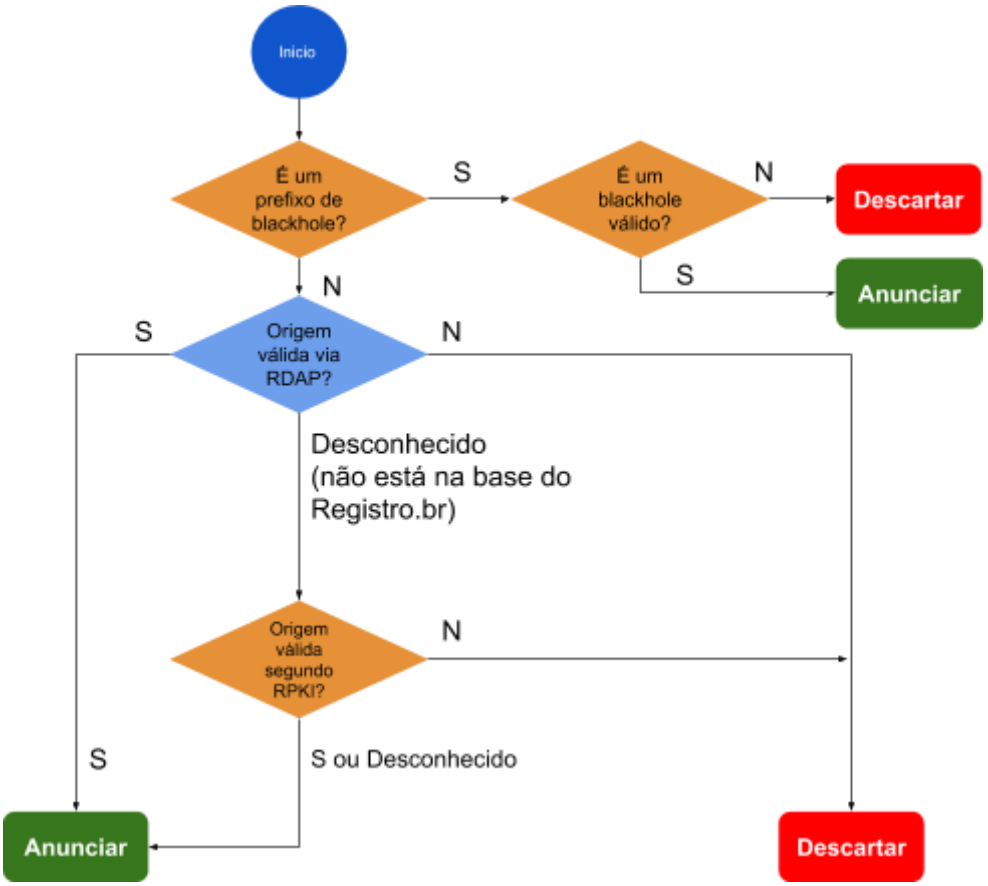
O diagrama abaixo esquematiza o funcionamento dos filtros baseados na validação de prefixos ou ASNs não permitidos na rede do IX.br:



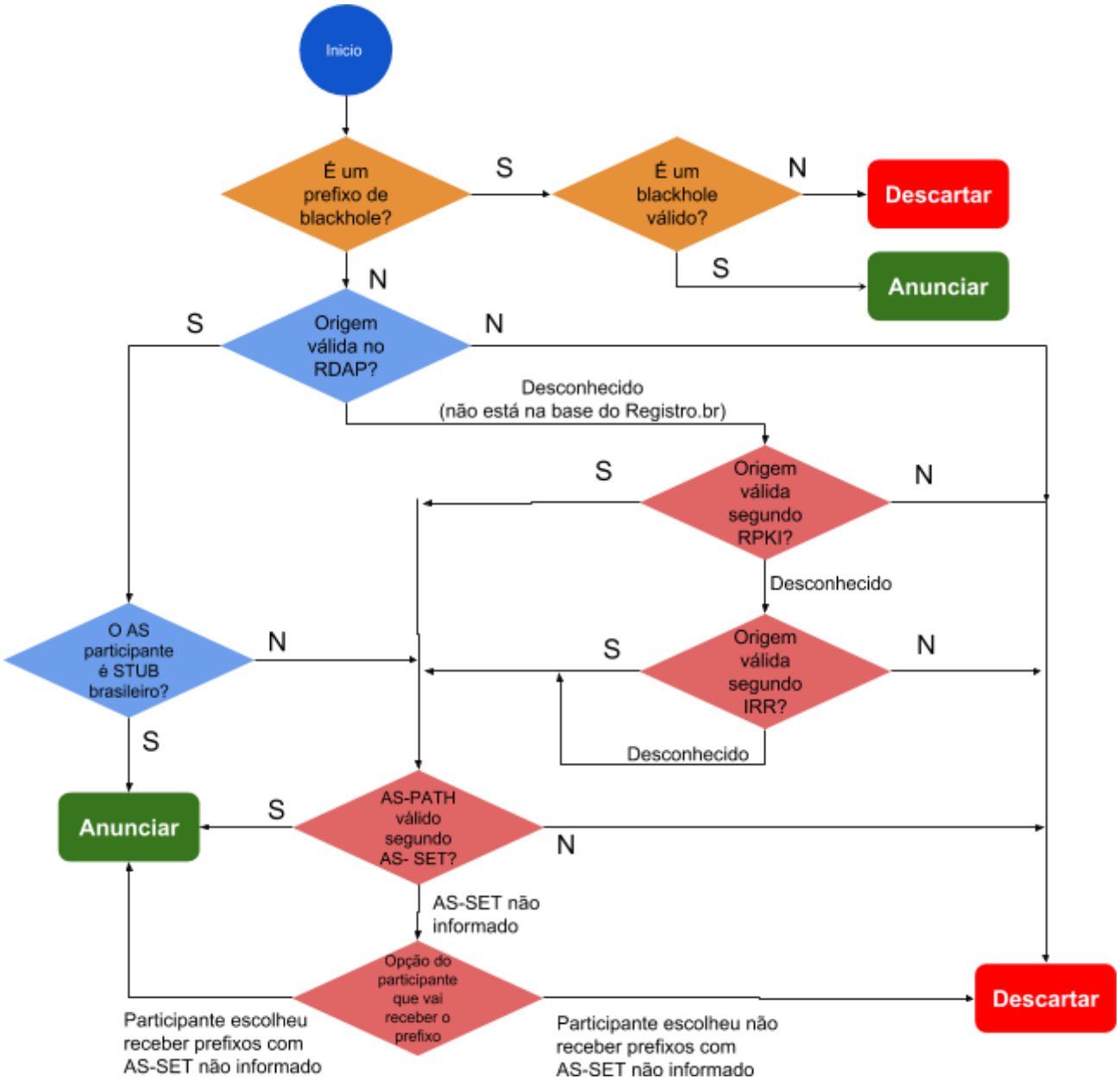
Após a validação de prefixos ou ASNs não permitidos na rede do IX.br, serão feitos os filtros baseados nas demais validações. O diagrama a seguir esquematiza a forma como os filtros serão implementados a CURTO prazo.



O diagrama a seguir esquematiza a forma como os filtros serão implementados a MÉDIO prazo.



O diagrama a seguir esquematiza a forma como os filtros serão implementados a LONGO prazo.



O diagrama de LONGO prazo não contempla ainda os filtros utilizando RDAP do LACNIC ou ARIN. São necessários estudos adicionais para determinar a exata forma como serão inseridos nesse fluxograma.

Para o filtro de AS SET será permitido ao participante, via portal, escolher se quer receber ou não anúncios de participantes de trânsito e que não informaram o AS SET.

É possível que haja também a mesma escolha para origem desconhecida, quando a origem não é conhecida nem via RDAP, nem RPKI, nem IRR. Estudos adicionais, principalmente sobre a eficácia das validações RPKI no seu estado atual de adoção, e do IRR, são necessários para definir se essa opção realmente existirá.

Cronograma de atividades

1) Publicação no site do IX.br da primeira versão do documento: 04/05/18.
2) Apresentação à comunidade: no IX Fórum Regional de São Paulo, no dia 17/05/2018, e na reunião GTER 45, em 22/05/2018.
3) Recepção de comentários através da lista de e-mails da GTER: até 04/06/18.
4) Análise, preparação e publicação no site do IX.br da segunda versão do documento, com a inclusão de sugestões da comunidade: 13/07/2018.
5) Recepção de comentários através da lista de e-mails da GTER: até 27/07/2018.
6) Publicação da versão final do documento com as ações a serem implementadas: 01/08/2018.
7) Cronograma previsto de implantação das ações:

Localidade	Curto	Médio	Longo
Aracaju	não definido	não definido	não definido
Belém	não definido	não definido	não definido
Belo Horizonte	não definido	não definido	não definido
Brasília	não definido	não definido	não definido
Campina Grande	não definido	não definido	não definido
Campinas	não definido	não definido	não definido
Caxias do Sul	não definido	não definido	não definido
Curitiba	não definido	não definido	não definido
Florianópolis	não definido	não definido	não definido
Fortaleza	não definido	não definido	não definido
Foz do Iguaçu	não definido	não definido	não definido
Goiânia	não definido	não definido	não definido
João Pessoa	não definido	não definido	não definido
Lajeado	não definido	não definido	não definido
Londrina	não definido	não definido	não definido
Maceió	não definido	não definido	não definido
Manaus	não definido	não definido	não definido

Maringa	não definido	não definido	não definido
Natal	não definido	não definido	não definido
Porto Alegre	não definido	não definido	não definido
Recife	não definido	não definido	não definido
Rio de Janeiro	não definido	não definido	não definido
Salvador	não definido	não definido	não definido
Santa Maria	não definido	não definido	não definido
São José dos Campos	não definido	não definido	não definido
São José do Rio Preto	não definido	não definido	não definido
São Luis	não definido	não definido	não definido
São Paulo	16/10/2018	15/12/2018	15/09/2019
Teresina	não definido	não definido	não definido
Vitória	não definido	não definido	não definido

Observações:

- São Paulo será a localidade base das novas funcionalidades. Uma vez aprovadas, serão replicadas para as demais localidades.
- Os prazos apresentados são os máximos, podendo ocorrer a implantação de funcionalidades antes da data limite informada.
- A princípio estamos considerando a implantação de todas as funcionalidades em todas as localidades do IX.br.
- As datas propostas estão vinculadas ao Cronograma de Implantação das Mudanças nos Route Servers de São Paulo, publicada no site do IX.br, área de Documentação.

RESUMO DAS CONTRIBUIÇÕES RECEBIDAS (na primeira versão deste documento)

1) Acho que podem incluir um filtro de "4.5-TiER-1-nacionais" colocando na lista

   RNP
   Embratel
   Tim
   Telefonica
   OI,
   Outros?

2) Outra é ter uma classe "grandes provedores de conteúdo" listando os ASNs de provedores de conteúdo/serviço como Google, Netflix e Amazon?? Como regra geral, até onde tenho conhecimento, estes caras não são transportados por ninguém até o PTT.

3) Ação 4: é uma proposta funcionalmente válida, com único contratempo de que centraliza muita responsabilidade em cima do NIC.br a fim de certificarem-se que tem a lista completa de carriers t-1 (falência, novas empresas, etc), além de que acaba sendo suplantado por outras das ações propostas. Sendo assim a curto prazo fazer esta aplicação, e a longo prazo interromper após as outras propostas que incluem este tipo de limitação já estiverem implantadas e em produção.

4) Ações 5, 6 e 8: parcial
   – De acordo com a proposta RDAP da ação 6.
   – O restante das propostas tem basicamente o mesmo intuito e poderiam ser concentradas em um único método:
   — A meu ver o principal problema de propostas como IRR é que trata-se de sistemas descentralizados e gerenciados por entidades totalmente independentes, o que dificulta na identificação de autoridade pois não haver nenhuma entidade raiz (exemplo, os servidores Root que dão autoridade ao DNS global).
   — A proposta RPKI me parece redundante uma vez que o problema de segurança é mais focado em autorização ao invés de comprovação de identidade, elevando desnecessariamente a complexidade.

5) Sugestões:
   O próprio NIC.br deveria ter um sistema integrado, acessado de maneira similar que o registro.br e meu.ix, onde ASNs podem se cadastrar e definir explicitamente quais ASNs/prefixos podem anunciar seus próprios ASN/prefixo(s).
   Desta forma tendo a mesma funcionalidade de uma IRR, porém centralizada e gerenciada pelo próprio NIC.br, garantindo a autoridade sobre os ASs do Brasil.
   Idealmente este processo deve ser totalmente automatizado, via GUI (Português + Inglês) e opcionalmente comandos em textos (para facilitar o uso de scripts dos usuários), mas

caso haja uma certa dificuldade da implantação de tal sistema, basta que essas solicitações sejam realizadas via chamados, similar a solicitações no IX.br.

Para facilitar a vida de ASs de trânsito, ter uma opção de ativamente solicitar a um outro ASN se eles desejam permitir o anúncio de seus prefixos.
No caso, o ASN de trânsito acessaria seu portal no NIC.br e clicaria numa opção "desejo anunciar ASNs/prefixos de terceiros", bastando então apenas preencher quais ASNs e/ou prefixos deseja anunciar.
Feito isto, o sistema do NIC.br automaticamente realiza um whois nos recursos informados e envia um e-mail para a conta de e-mail cadastrada no resultado do whois.
Este e-mail deve conter todas as informações referentes à solicitação e um link de URL onde pode-se clicar para confirmar que permite o trânsito.
Caso este link seja clicado mas queiram revogar a permissão, teriam então que acessar seu portal no NIC.br e editar as permissões (caso ainda não tenham se cadastrado, seria necessário tal).

6) Venho falando desde o ano passado fazer um dashboard, semelhante ao do icloud com todos os serviços e ferramentas do Nic.BR

7) A "Ação 4" me parece um pouco invasiva de mais. Ela ser contemplada como opção do participante escolher se quer ou não receber esses anúncios me parece mais coerente com o discurso de neutralidade que já escutei para justificar negociações de outras sugestões.
Um política mais ampla do IX.br seria mais legal. Criar uma política de "nós não recomendamos esse anúncio" e marcando isso com communities que indiquem porque foi desaconselhado seria legal. Me parece que precisaria de add-paths para isso funcionar mas o IX.br escolheu não usar e parece que isso está atrapalhando. A escolha, ou proposta que ouvi anos atrás, de fazer isso (controle fino do que receber) no portal até agora não rolou e eu prefiro interagir apenas com o roteador conectado ao IX do que com ele e com o portal.

Comentário recebido:
While section 4 indeed requires periodic review, it is a highly effective method to guard against large operational issues. I can assure you that any announcement which as 2914 in the AS_PATH passing through any route server is either a misconfiguration, a software defect or a malicious activity. I do not think it wise to simply dismiss such 'ground truth' information.

Resposta ao comentário:
Imagine the following scenario:
IX RS - AS4 enabled participant - not-AS4 capable downstream - AS4 capable participant

The AS Path on the IX RS could look like this, if all of them were AS4 capable:

65000 - 65001 - 65536

But, since 65001 is not AS4 capable, it will send this path upwards:

65000 - 65001 - 23456

Note that IX RS is AS4 capable, and the IX member (65000) is also AS4 capable. But, 65000 has a customer that it's not, and they in turn have a customer that is an ASN greater than 65535.

So, this scenario requires no misconfigurations, and still present AS_TRANS (23456) in the path.

Resposta ao comentário acima:
No, still in that scenario 23456 is not visible on the route server from a policy perspective, because in that scenario the AS4_PATH attribute is used to tunnel through the non-AS4-capable ASN and 65536 will be the visible ASN on the route server.

The AS4/non-AS4 transition mechanism is quite amazing: https://tools.ietf.org/html/rfc6793

8) A "Ação 5" me parece não ajudar em nada. No máximo isso seria uma tentativa de proteger os outros participantes de erros de um "AS Stub". Já vi erros de ASs pequenos, médios e grandes sendo esses novos ou velhos e se é para estabelecer relações de confiança diferenciada por AS então que se faça algo baseado em comportamento e resultado. Coisas boas aumentam a confiança e direitos e coisas ruins os diminuem. Me parece também que a "Ação 6" e a "Ação 8" sobrepõem a "Ação 5"

   Comentário recebido:
   Concordo que além de não ajudar muito vai gerar muita entropia e será difícil de manter.
   Também concordo que estes problemas serão resolvidos no longo prazo pelas outras ações. Por mim esse item pode ser totalmente suprimido.

9) Ação 2: Sugiro aumentar o escopo dos prefixos filtrados para os dos root-servers e dos clusters anycast do .br, nos AS não-stub; nos AS stub, o que inclui os clusters anycast do .br, o filtro já vai permitir apenas o espaço alocado para esses AS.

10) Ação 3: Será que não vai ser necessário aceitar 23456 caso algum AS path tenha uma combinação de roteadores sem e com suporte a AS 32 bits ? Uma alternativa seria atualizar a documentação de que esse suporte é um requisito tanto para o AS membro quanto para seus downstreams. Ainda na ação 3, talvez colocar um exemplo mostrando que o anúncio será inteiramente rejeitado, e não apenas o AS bogon suprimido. Apesar do texto estar claro, como há equipamentos com essa opção, um exemplo pode ajudar a não permitir Dúvida.

    Comentário recebido:

A BGP speaker which is capable of AS4, should never see AS 23456 in the AS_PATH. Any occurance of AS 23456 visible on a 4-byte ASN capable router is either a misconfiguration, or a software defect. We should not reward misconfigurations by accepting these announcements.

11) Ação 4: Talvez incluir as grandes Web-Scale na mesma lista, como o Google, Netflix, Facebook, Akamai ?

Comentário recebido:
Route server operators should only include such companies in this filter with their explicit permission.

Resposta ao comentário:
Why would that differ from Tier-1 operators ? I could see a point for doing the same for the same Tier-1 operators, but not for treating them differently.

Resposta ao comentário acima:

> [side-note: I prefer to use the term 'transit-free' instead of
> 'tier-1', because the term 'transit-free' is something we can verify
> to a degree, while 'tier-1' has no well-defined meaning.]

All the "Big Content" providers you mention, have some form of a distributed CDN approach where they connect independent clusters (as islands) to the Internet and use the Internet for feeding/filling and serving cached data. In other words, parts of their ASN are not transit-free. This is a fundamental difference compared to the transit-free networks as proposed in the IX.br document, who are expected to operate as a coherent backbone.

I just want to make sure that the filter, _as proposed_, has a lot of value too. This type of filter is documented in various places, such as http://bgpfilterguide.nlnog.net/guides/no_transit_leaks/ Broadening that filter without the ASN owner's consent might be trickier.

If the community decides that transit-free/transit-using networks should all be treated the same, and that those networks can simply email IX.br "never allow announcements that have our ASN anywhere in the AS_PATH on your route servers", that is fine by me too. I'm supportive on an approach opt-in approach, and an approach that is open to everyone that wants to use it. I'm also supportive of the proposed list as-is.

12) Ação 6:
- Na validação RDAP, considerar o 1o. ASN do AS Path independente do AS ser ou não do IX.br. Isso permitirá garantir consistência do anúncio, mesmo antes de se implementar validação RPKI. Não fazer essa validação para AS-Stub brasileiro para maior performance.
- Na validação IRR, considerar suportar não apenas bases RPSLng como TC, RADB e RIPE, mas também RPSL como o Registro.br.

- Ainda na validação IRR, ela pode ser opcional até que ocorra um episódio de hijack naquele membro; mas a partir de então, mandatória.
- Se a rota estiver com RPKI válido, encaminhar mesmo que esteja com RDAP inválido. Isso permite que acordos legítimos para anúncio de um bloco por outro AS sejam reconhecidos.

13) Ação 8: Esta é uma análise potencialmente complexa do grafo da DFZ; sugestão é dividir essa ação em entregáveis menores. Por exemplo, começar apenas com alertas para membros de que seu AS está no importação IRR (ação 6) de outro ou apareceu no anúncio BGP de outro, e caminhar em prazo maior para validações mais preventivas.

14) Gostaria de sugerir a questão dos anúncios blackhole, agora com validação RDAP por exemplo, principalmente para anúncios de AS stub faz sentido ter blackhole implementado também. A maior preocupação antes era sobre a validação do anúncio, para evitar de alguém colocar bloco de outro em blackhole. Agora com essa validação fica mais fácil, principalmente para AS stub.

    Não tenho a resposta para isso, apenas trago a pergunta para discussão.

RESUMO DAS CONTRIBUIÇÕES RECEBIDAS (na segunda versão deste documento)

1) Uma sugestão que me ocorreu é que mudar o limitador de número de prefixos da sessão com o participante para a saída para outros participantes. Isso teria duas vantagens:
   - Para os AS Stub, mesmo que eles façam leak, isso não irá derrubar a sessão com o IX, pois esses prefixos anunciados erradamente foram filtrados. Eventuais anúncios indevidos podem ser tratados por casos abertos pelo NOC do IX junto aos participantes como alarmes de menor gravidade, sem porém impactar funcionamento.
   - Para os AS de trânsito, isso agilizaria a recuperação do serviço, pois as sessões flapando podem impactar os roteadores desses participantes. Além disso, um dos sentidos de tráfego estaria preservado pois ele continuaria a receber os prefixos de outros participantes.

   Comentário Equipe IX.br: a manutenção do limite de prefixos na entrada tem também por objetivo proteger os route servers contra ações mal intencionadas. Uma vez que pretendemos marcar anúncios inválidos para posterior exportação para o Looking Glass Web, o envio de uma infinidade de anúncios com irregularidades poderão consumir os recursos existentes para a operação dos Route Servers.

2) Qual o grau de complexidade do IX utilizar IRR para validar os prefixos/AS-PATH?
   Se os trânsitos filtrassem os prefixos aprendidos via AS-PATH, muitos desses problemas seriam evitados. Boa parte dos maiores trânsitos nacionais já o fazem.

   Resposta ao comentário acima:

   - Segundo o documento postado, o tempo previsto para esse é MÉDIO, ou seja, ordem de meses.
   - Na verdade não, pois hoje o limite de prefixos está direto na sessão do participante, então a sessão irá cair antes que a validação atue. A sugestão que dei foi exatamente de mudar isso, e aí todas as validações aplicáveis atuariam antes do limite de prefixos.
   - O problema de filtragem de AS-Path é que todo AS que aparece no path precisaria ter algum cadastro de AS-Path (IRR ou não) contra o qual se validar... e isso está muito longe da realidade. Notar que o membro do IX ter isso não seria suficiente para validação, pois real validação depende de todos os AS…

3) BCP38..... só isso já ajudava muito.
   O que eu quiz falar é uma forma do nic.br poder validar se realmente o ASN dentro dos IX's estão seguindo recomendações.