Boas Práticas de BGP

ceptro.br nic.br cgi.br

Atributos do BGP

ceptro.br nic.br cgi.br

Licença de uso do material

Esta apresentação está disponível sob a licença

Creative Commons
Atribuição - Sem Derivações 4.0 Internacional (CC BY-ND 4.0)
https://creativecommons.org/licenses/by-nd/4.0/legalcode.pt



Você tem o direito de:

- **Compartilhar -** copiar e redistribuir o **material** em qualquer suporte ou formato para qualquer fim, **mesmo que comercial.**
- *O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.*

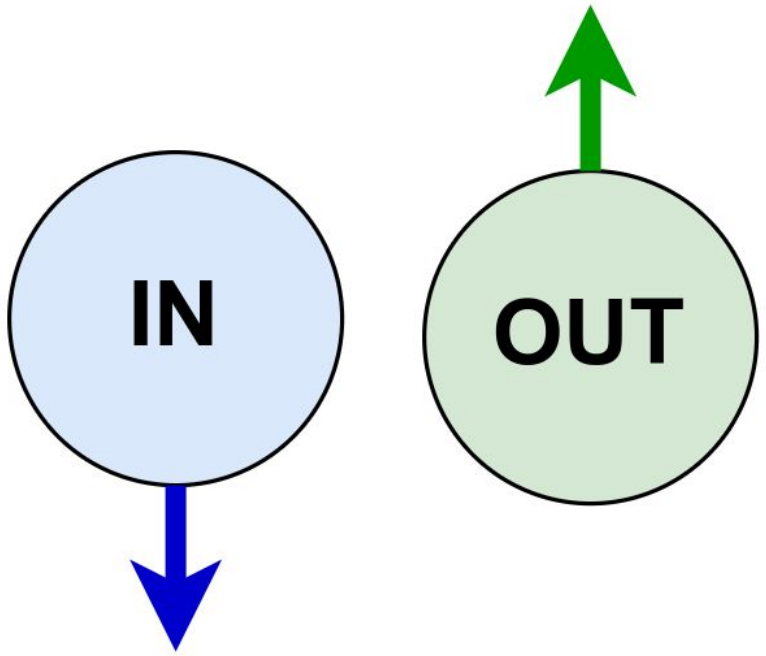
De acordo com os termos seguintes:

- **Atribuição** - Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso. Ao distribuir essa apresentação, você deve deixar claro que ela faz parte do **Curso de Boas Práticas Operacionais para Sistemas Autônomos do CEPTRO.br/NIC.br**, e que os originais podem ser obtidos em http://ceptro.br. Você deve fazer isso sem sugerir que nós damos algum aval à sua instituição, empresa, site ou curso.
- **Sem Derivações** - Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

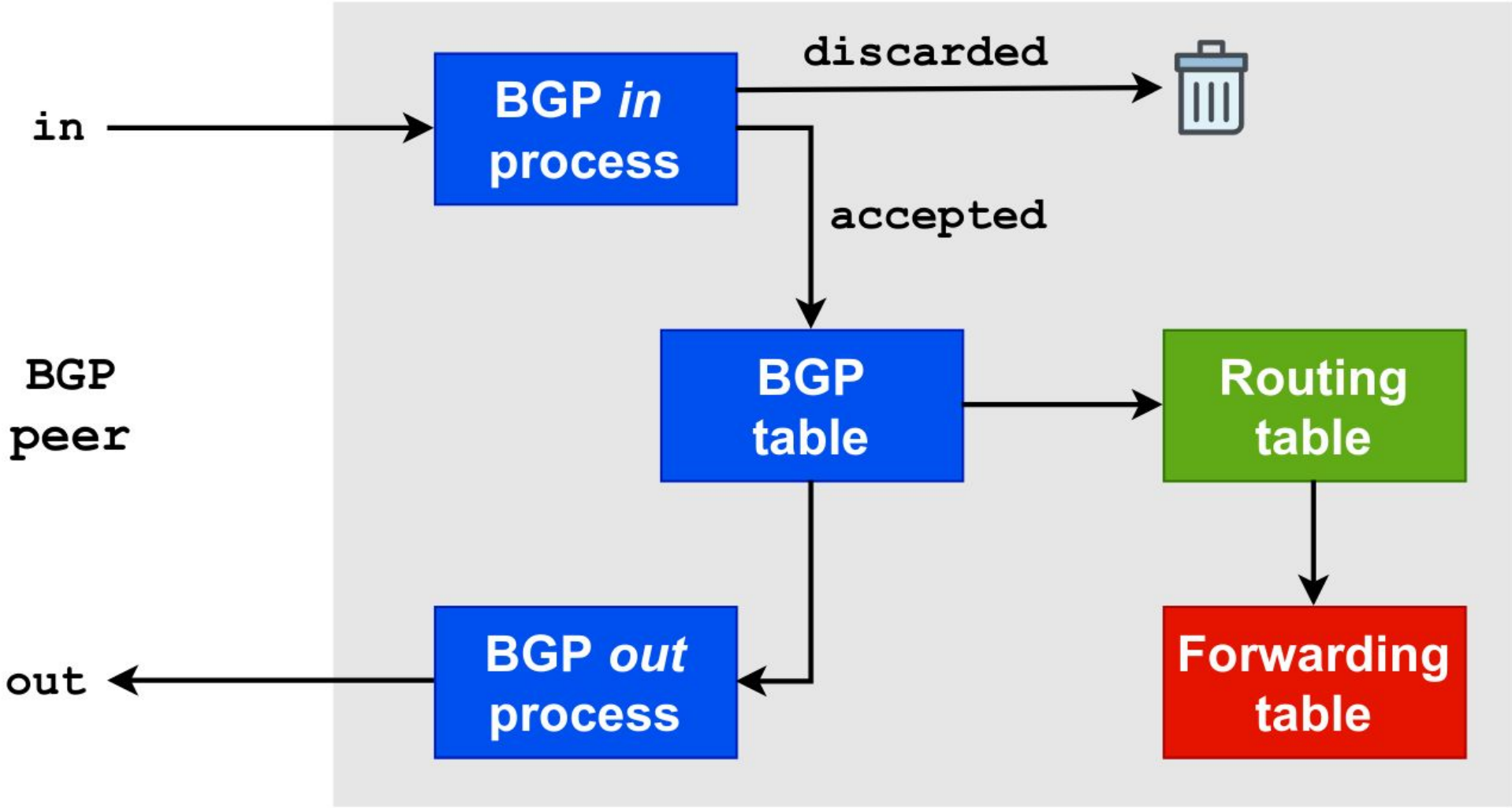
Se tiver dúvidas, ou quiser obter permissão para utilizar o material de outra forma, entre em contato pelo e-mail: info@nic.br.

BGP IN e OUT

- **Processo de entrada (in)**
  - Recebe o caminho dos peers
  - Os caminhos são inseridos na tabela BGP
  - O melhor caminho (best path) é marcado
- **Processo de saída (out)**
  - O melhor caminho é anunciado aos peers

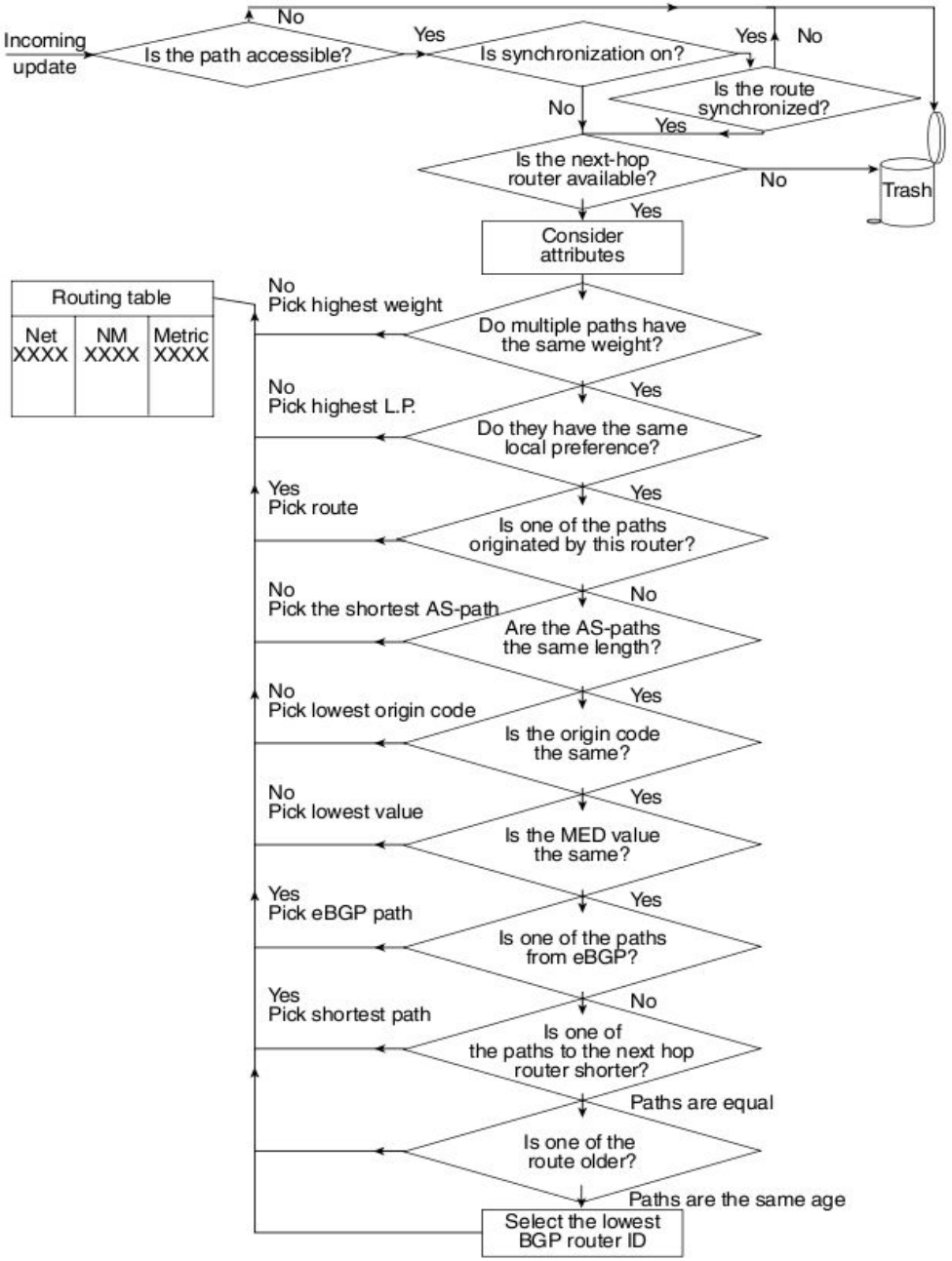


Funcionamento do BGP

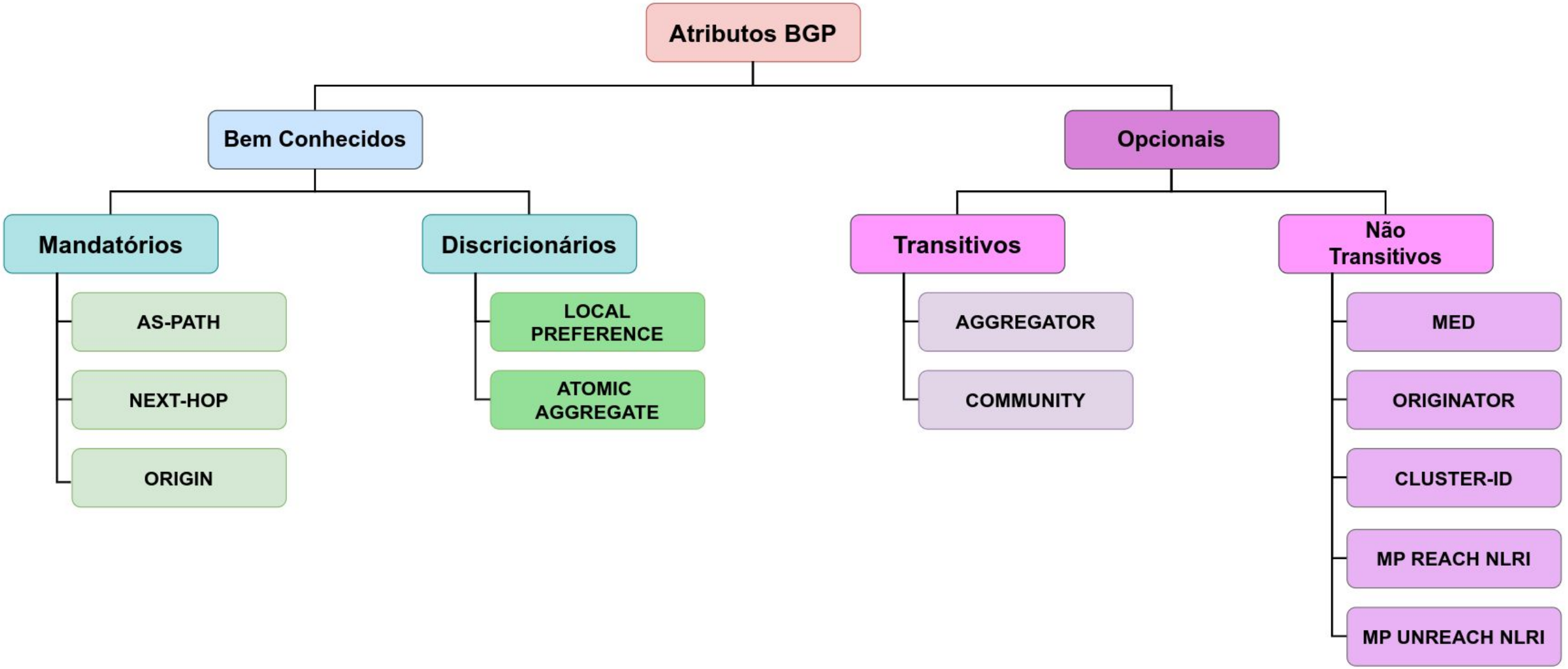


Atributos do BGP

- Os atributos são considerados na seleção dos caminhos
- Se este for conhecido, acessível e se o next hop estiver disponível
- A forma de seleção pode variar com a implementação do BGP

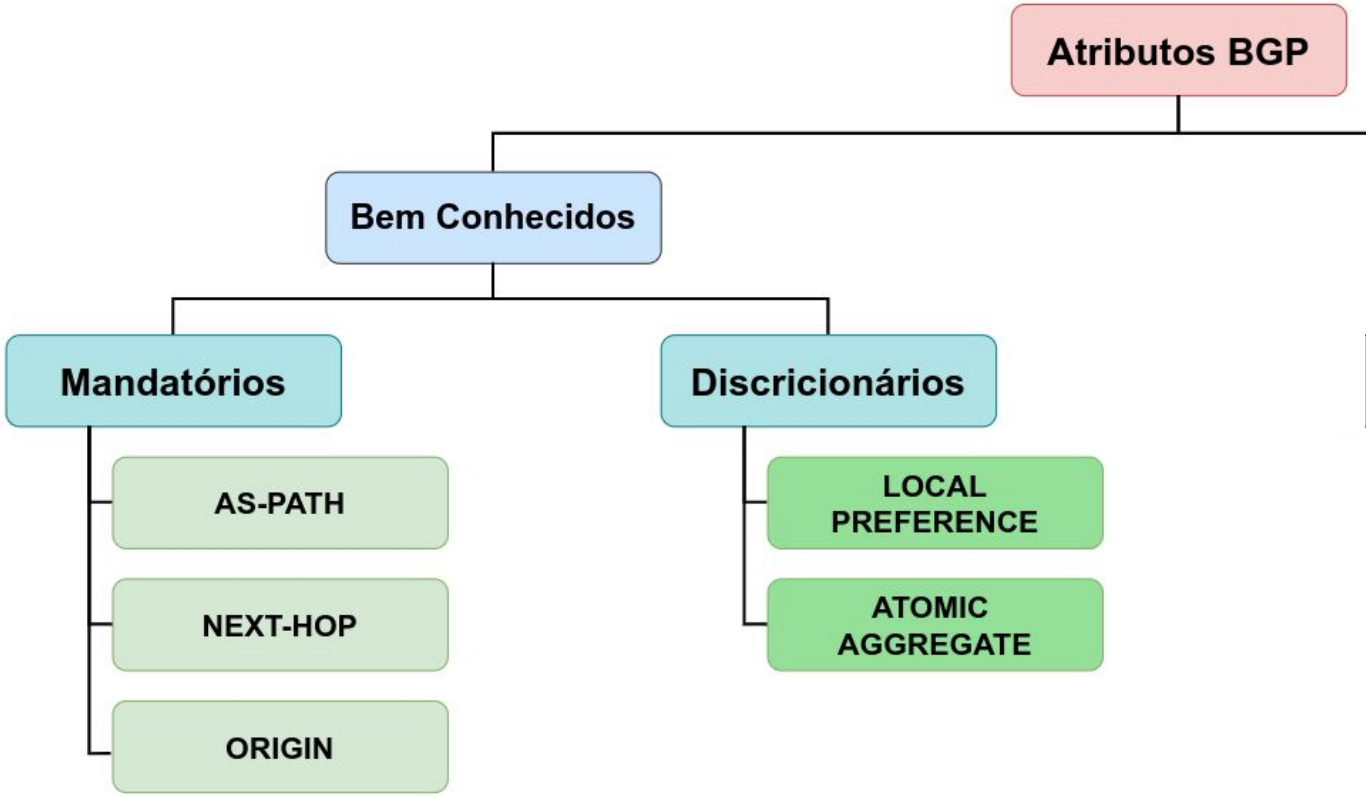


Atributos do BGP



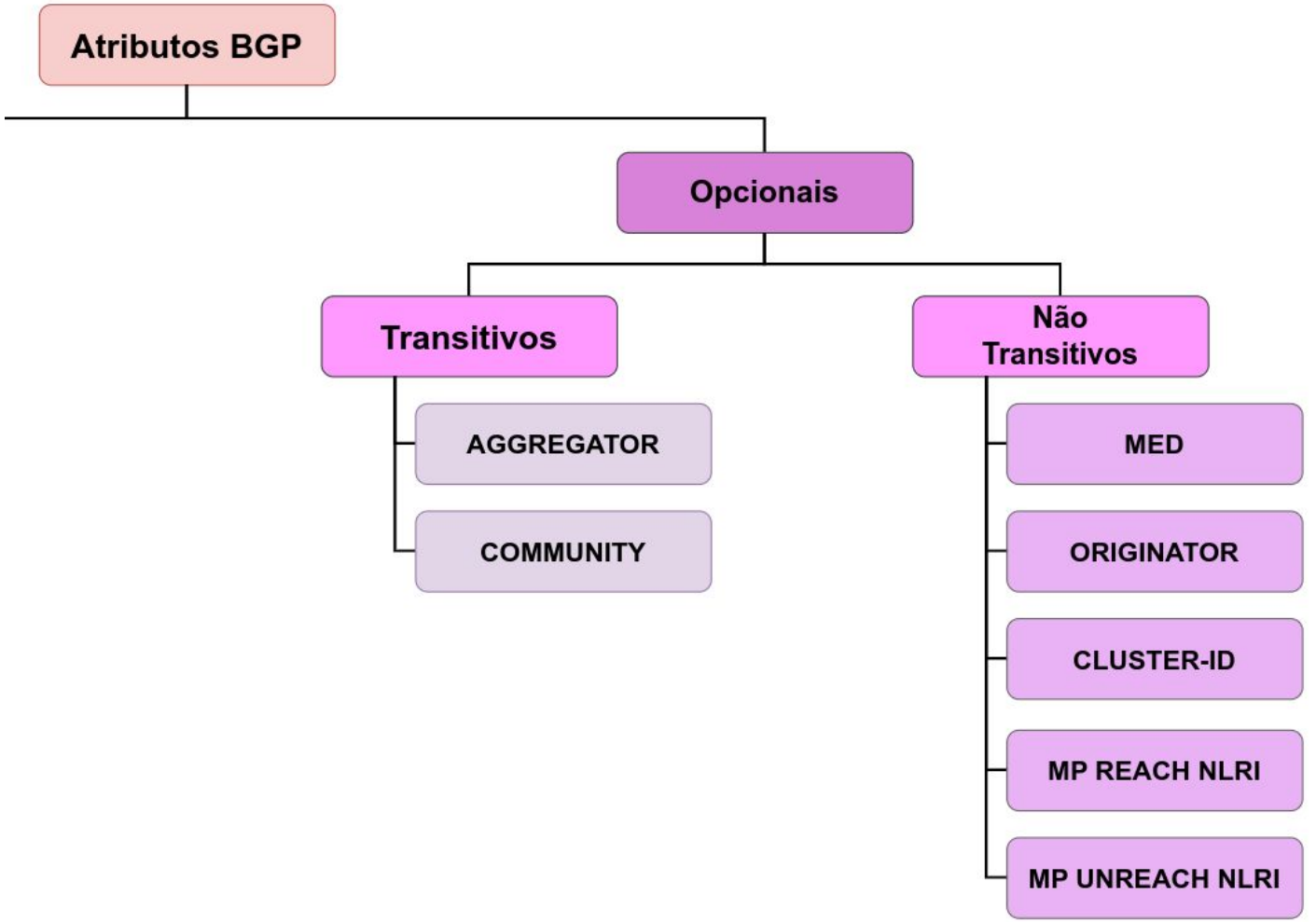
Tipos de Atributos - Bem conhecidos

- Todas as implementações BGP os reconhecem
- **Mandatórios**
  - Sempre estão presentes nos updates que carregam informações de prefixos (NLRI - Network Layer Reachability Information)
- **Discricionários**
  - Não estão em todos os updates



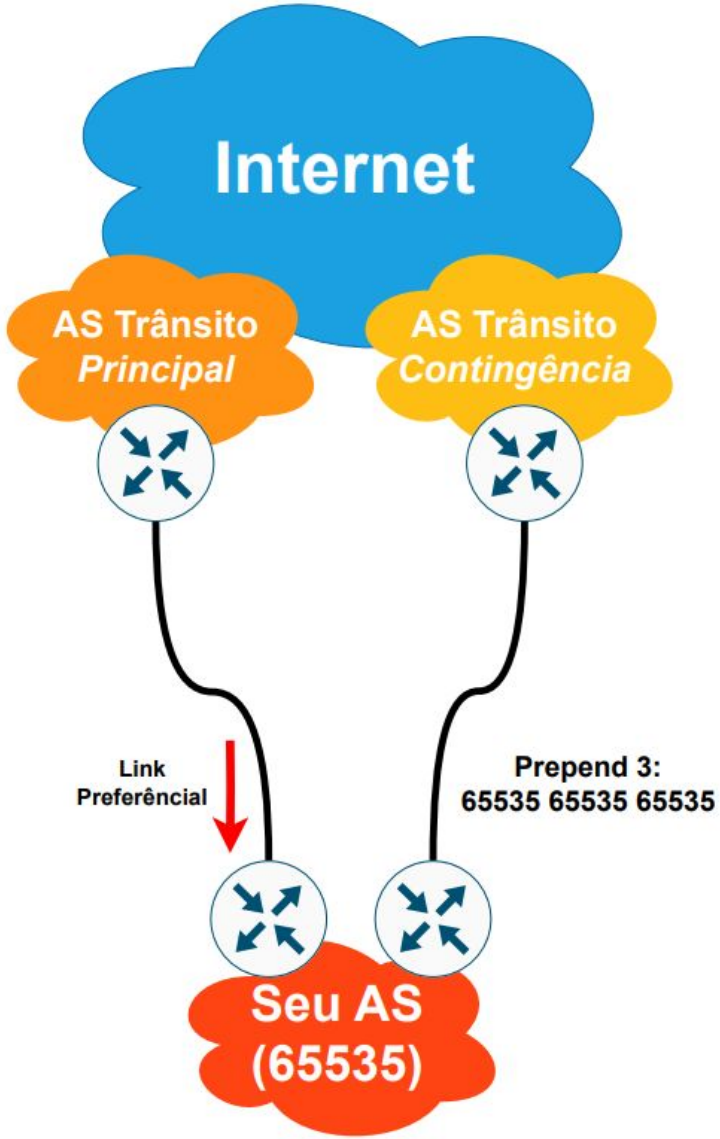
Tipos de Atributos - Opcionais

- Não são suportados por todas as implementações BGP
- **Transitivos**
  - São repassado para os *peers* vizinhos.
  - Se não for reconhecido pelo roteador é marcado como *partial* e enviado para os *peers* vizinhos
- **Não Transitivos**
  - Não são repassados para os *peers* vizinhos
  - Se não são reconhecidos, são descartados



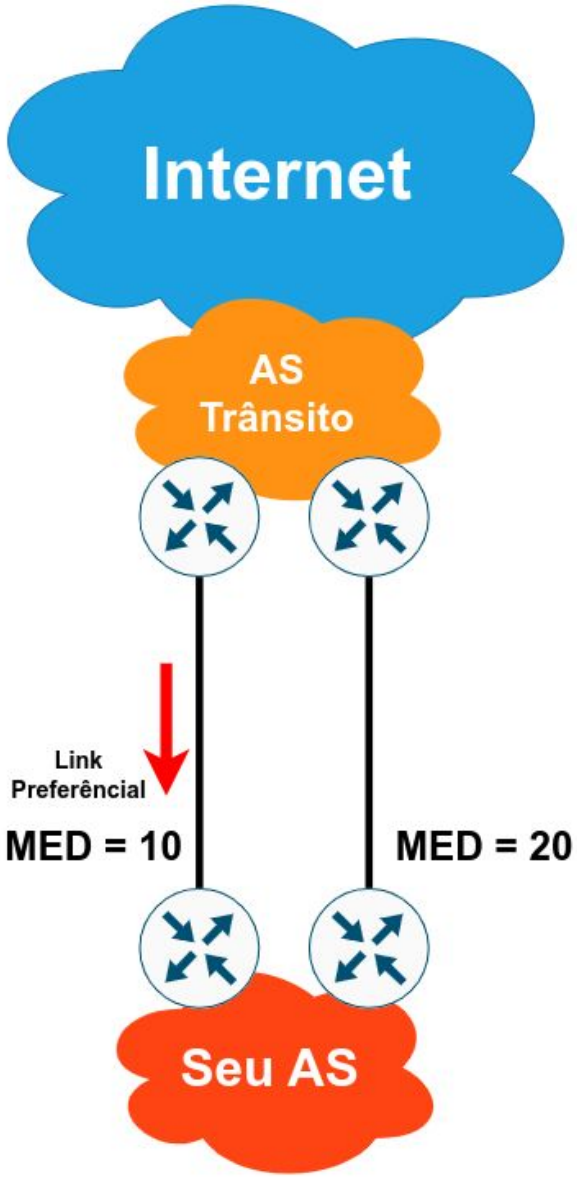
Atributos do BGP - AS PATH

- **Bem Conhecido** e **Mandatório**
- Indica o caminho para se chegar a um destino, incluindo todos os ASes intermediários
- É usado para:
  - Detectar loops
  - Aplicar políticas **(Prepend)**



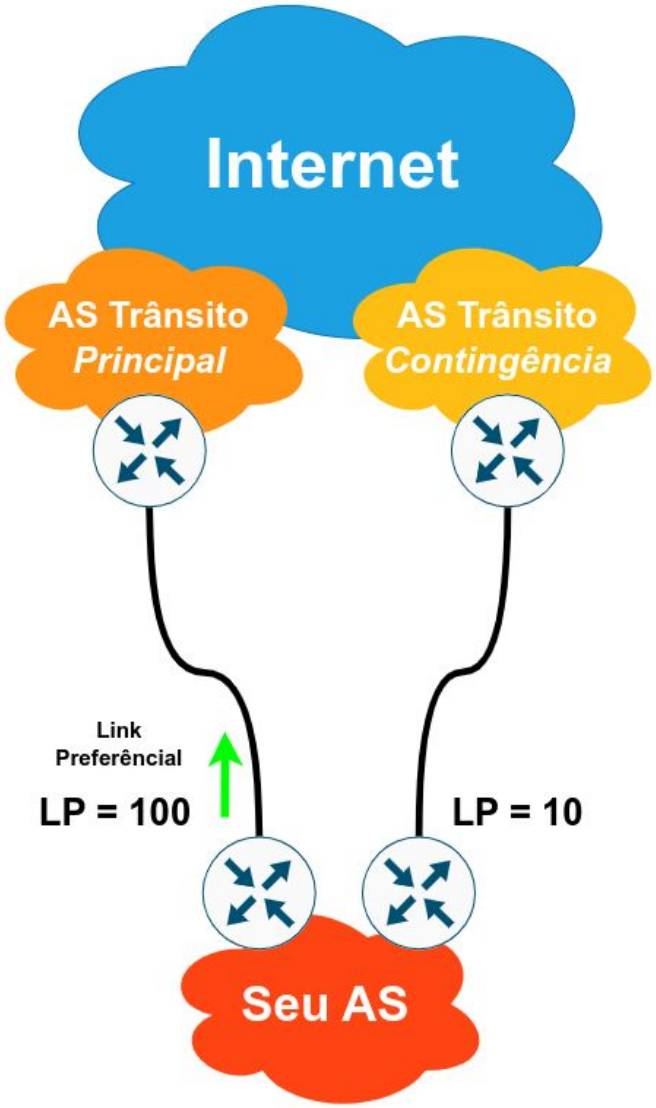
Atributos do BGP - MED

- **M**ulti-**E**xit **D**iscriminator
- **Opcional** e **Não Transitivo**
- Indica para os **vizinhos BGP externos qual o melhor caminho** para uma determinada rota do AS, influenciando o **tráfego de entrada**
- O **menor MED** ganha
- Ausência de MED implica **MED=zero**
- Utilizado quando há **duas saídas** para **um mesmo AS**



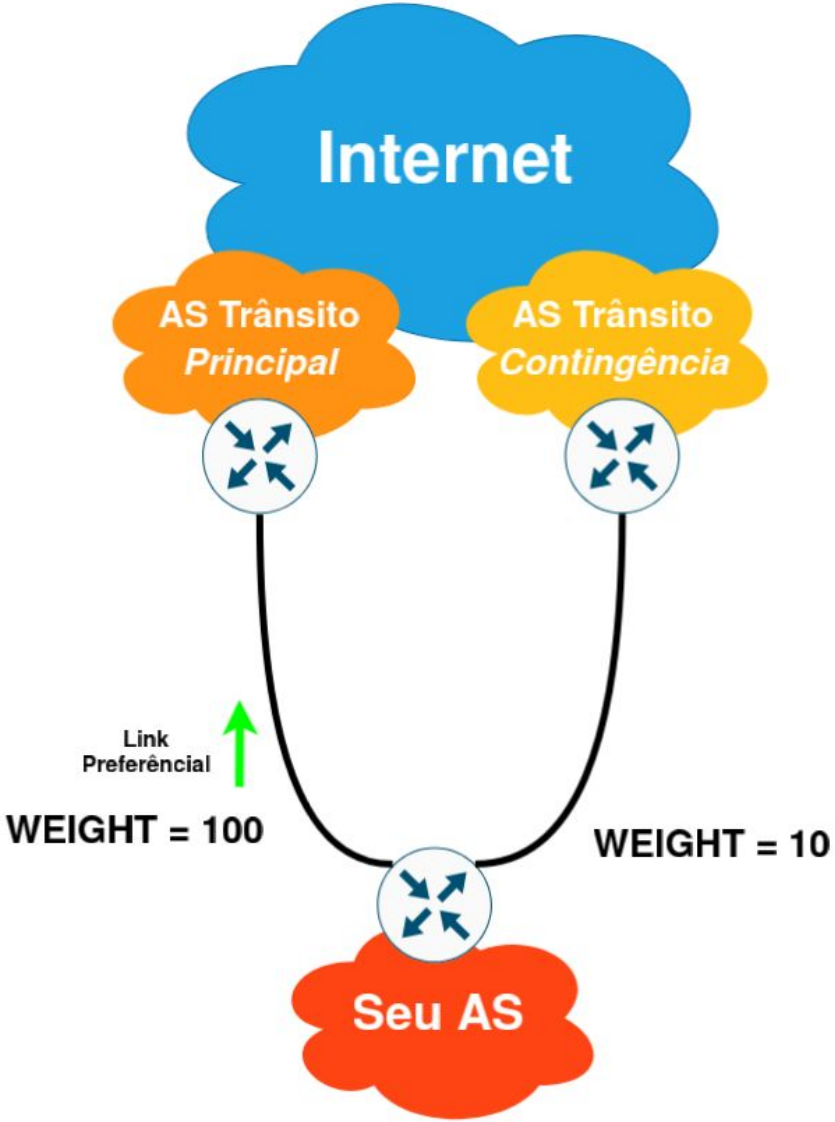
Atributos do BGP - Local Preference

- **Bem Conhecido** e **Discricionário**
- O valor pode ser associado a uma rota, indicando o caminho **preferencial de saída**.
- O caminho com a **maior Local Preference ganha.**
- Só vale **dentro do AS**



Atributos do BGP - Weight

- Não é um atributo (**é local para o roteador**)
  - **É um atributo proprietário da Cisco**
- O **maior** Weight **ganha**
- Pode ser aplicado as rotas aprendidas de um dado vizinho, ou por meio de filtros
- Influencia o **tráfego de saída**



Outros Atributos

- **Next-Hop (Bem Conhecido - Mandatório)**
  - Identifica o endereço IP de próximo salto para chegar ao prefixo
- **Origin (Bem Conhecido - Mandatório)**
  - Identifica a origem do prefixo.
    - i - IGP
    - e - EGP
    - ? - Incomplete
- **Atomic Aggregate (Bem Conhecido - Discricionário)**
  - Informa aos peers que o roteador está utilizando uma rota agregada
- **Aggregator (Opcional - Transitivo)**
  - Especifica o IP e ASN do roteador que agregou a rota

Outros Atributos

- **Community (Opcional - Transitivo)**
  - Funcionam como marcações em prefixos. Utilizados para criar políticas de roteamento
- **Originator (Opcional - Não Transitivo)**
  - Utilizado para identificar o primeiro Route Reflector que anunciou o prefixo no AS
- **Cluster ID (Opcional - Não Transitivo)**
  - Utilizado para identificar o roteador e prevenir loops em uma rede com Router Reflector.

Atributos novos no MP-BGP

- Necessário para suportar IPv6.
- Adiciona dois novos
  - **MP Reachable NLRI (Opcional - Não Transitivo)**
    - Carrega o conjunto de destinos alcançáveis junto com as informações do next-hop;
  - **MP Unreachable NLRI (Opcional - Não Transitivo)**
    - Carrega o conjunto de destinos inalcançáveis

Boas Práticas de BGP

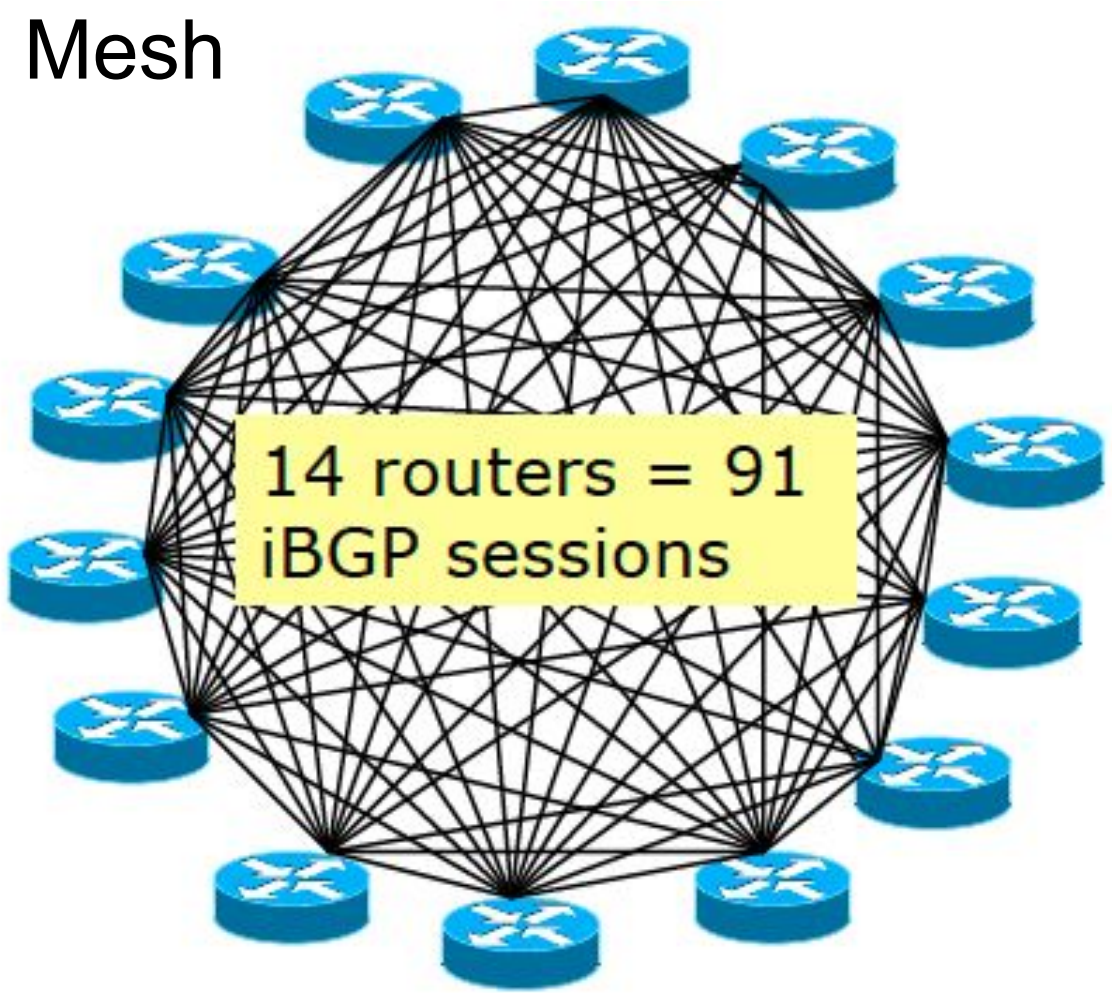
ceptro.br nic.br cgi.br

Loopback - iBGP

- No **iBGP** devemos **sempre usar interfaces loopback**
  - Usando **interfaces físicas**, se o **link for interrompido**, a **sessão BGP também será**
  - Usando **loopbacks** temos **uma estabilidade maior**.
    - Como as rotas para os IPs das **loopbacks** são aprendidos via **IGP**, se um **enlace for interrompido**, a **sessão contínua estabelecida**, com os pacotes fazendo um caminho alternativo.

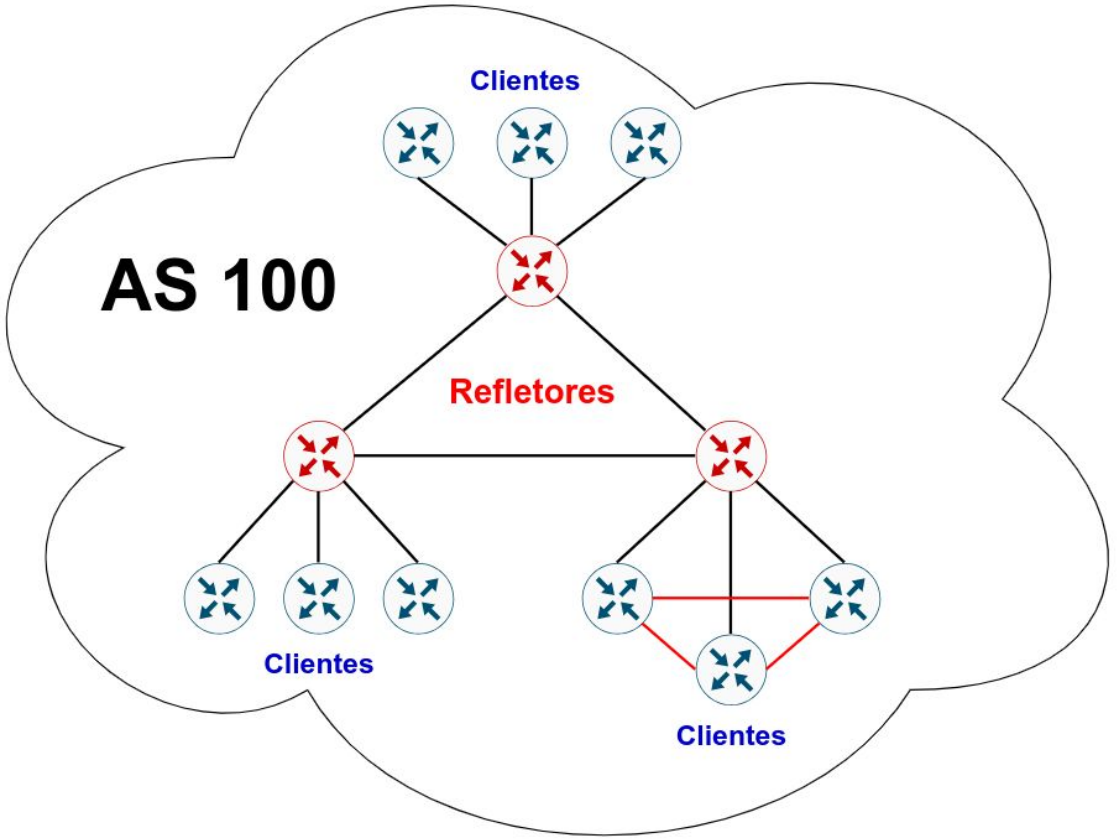
Escalando o iBGP

- iBGP deve operar em uma Rede Mesh
  - **Qtd. de Sessões** = **n**(**n**-1)/2
  - Onde **n** é nº de roteadores.
- **Alternativas**
  - Route Reflector
  - Confederation



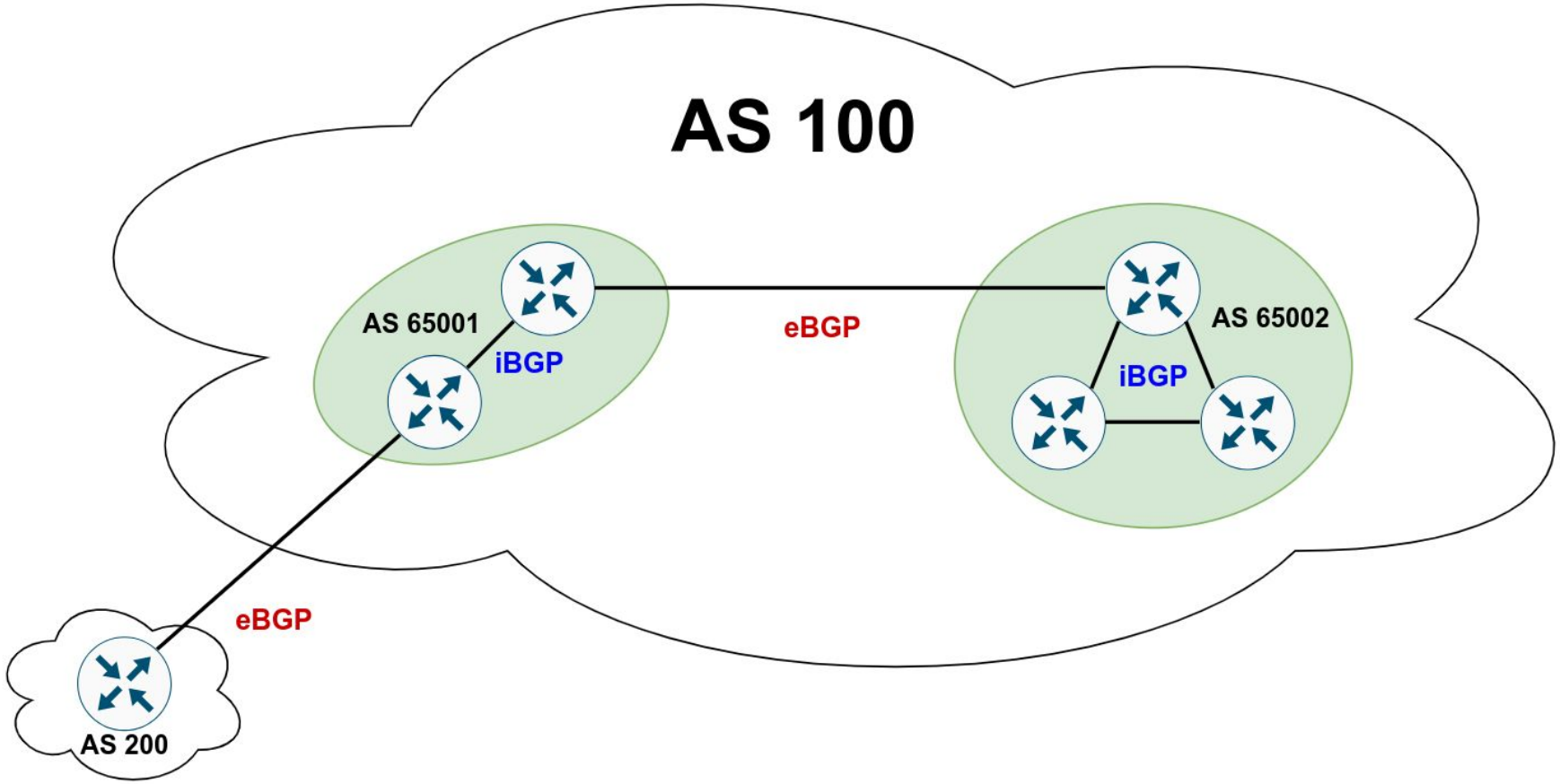
Escalando o iBGP - Router Reflector

- **Refletor** recebe rotas de todos
- Seleciona o melhor caminho
  - Se o **melhor caminho** for de um **cliente**, reflete para **todos**
  - Se o **melhor caminho** for de um **refletor**, reflete **somente para os clientes**



Escalando o iBGP - Confederation

- Aumenta a complexidade da rede.



Autenticando sessões BGP com MD5

- É recomendável usar **autenticação MD5** para as sessões BGP
- A configuração é simples
  - Os roteadores vizinhos compartilham uma mesma chave (uma senha)
- A cada pacote é adicionado um **checksum** codificado, que o outro roteador pode verificar utilizando **sua chave MD5**, ajudando a garantir sua autenticidade e integridade
- A técnica dificulta ataques.



TTL Security Check

- **Por padrão**
  - Os **pacotes** das sessões eBGP são enviados com valor de **TTL/Hop-Limit** igual a **1**
  - Garante que o **pacote** é um vizinho **diretamente conectado**.
  - Um atacante externo pode facilmente **forjar** um **pacote** com **TTL/Hop-Limit** igual a 1 no enlace.
- **Com TTL Security Check:**
  - O roteador envia pacotes com TTL/Hop-Limit igual a 255 (valor máximo desse campo).
  - No próximo roteador, o valor será decrementado
  - Ficará com o **TTL/Hop-Limit** igual a 254 (255-1)
  - Um atacante em outra rede não conseguirá inserir um pacote com TTL/Hop-Limit igual a 255 no enlace

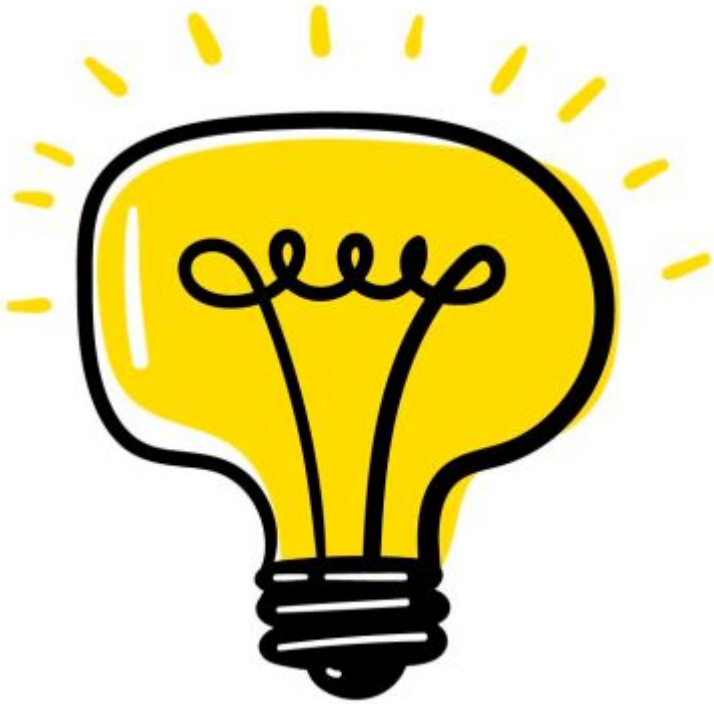


Image by Freepik

Desabilitando serviços e protocolos

- Nas **interfaces** onde são estabelecidas **sessões eBGP** é fundamentalmente que **todos os serviços e protocolos desnecessários estejam desabilitados,** de forma particular:
  - **IGP (OSPF / IS-IS)**
  - **Router Advertisement (RA) no IPv6**

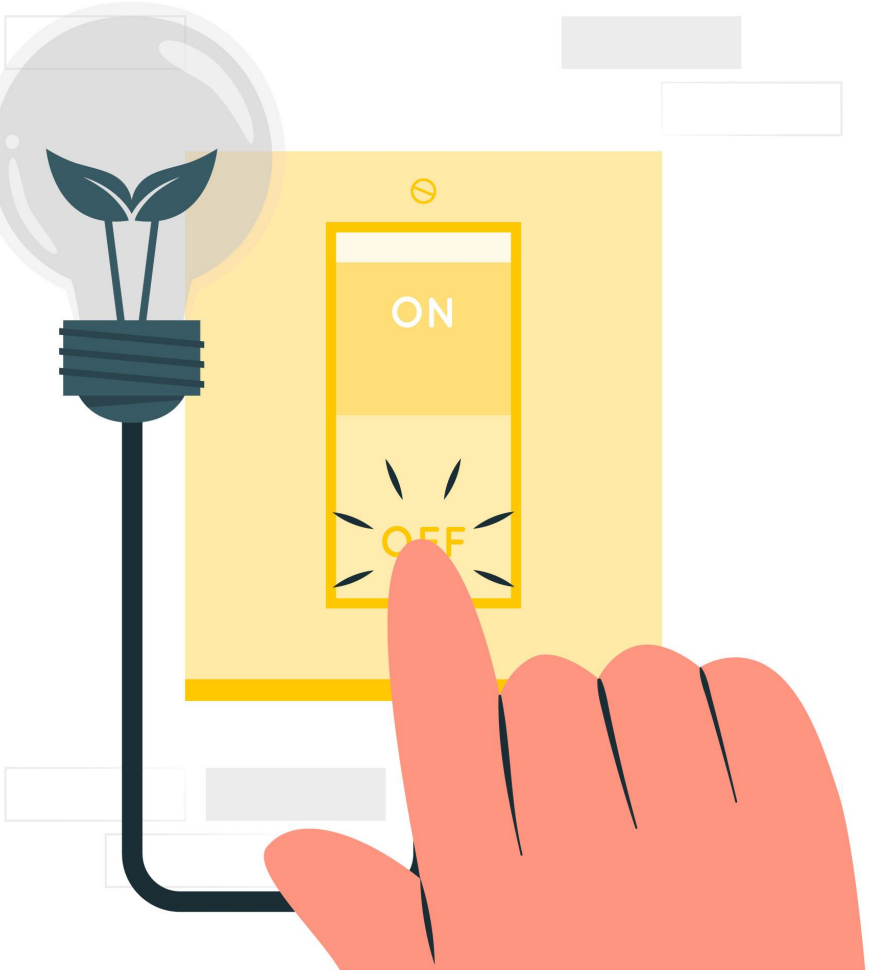


Image by storyset on Freepik

Route Refresh

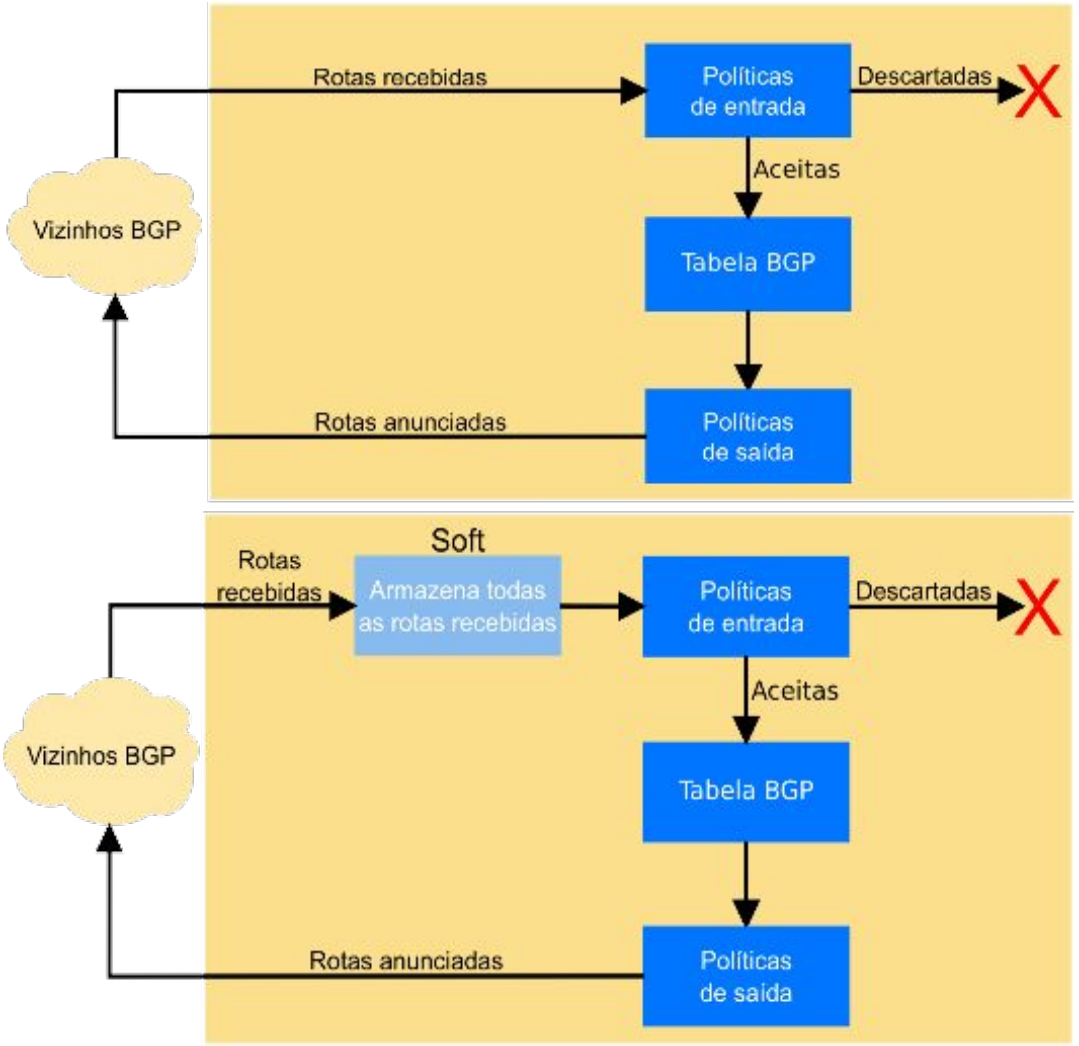
- Solicita que o **vizinho** cujas **rotas** são **afetadas** por uma **mudança de política**, **reenvie** toda a **informação pertinente**.
  - Isso se chama **Route Refresh**
  - Não usa memória
  - Não necessita de configuração extra
  - Maioria dos roteadores suportam
- Essa **capacidade** é informada no **estabelecimento de uma sessão BGP** e é possível verificá-la **olhando** as informações do **vizinho**.
- Após uma **mudança** em um **filtro** é preciso **solicitar o refresh para o roteador vizinho,** com um comando. **Isso não é automático!**



Image by rawpixel.com on Freepik

Soft Reconfiguration Inbound

- Antigamente era uma boa prática!
- Habilitando **“soft reconfiguration”**, é criada uma nova tabela, com a informação original.
  - Isso consome mais memória
  - Permite que filtros sejam modificados facilmente
- Serve para troubleshooting
  - É possível saber o que foi enviado antes de se aplicar os filtros



Filtros

Filtros

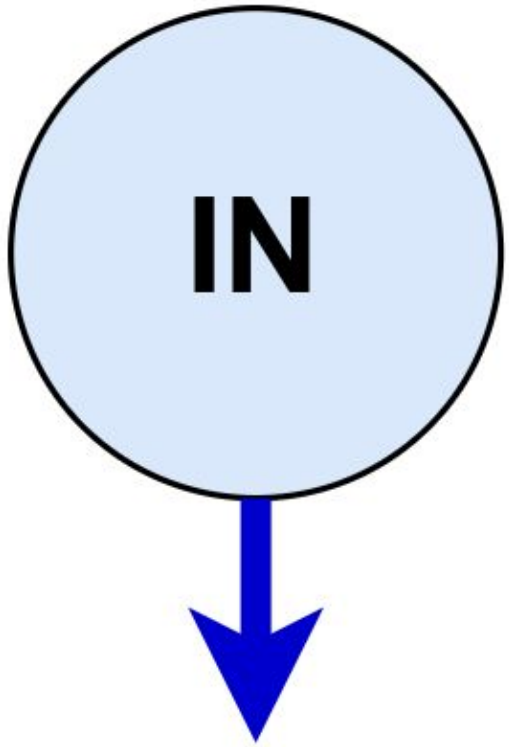
- Alguns **roteadores** são **permissivos**
- Se **nenhum filtro** for aplicado, aceitam **tudo** que os **vizinhos enviam**.
- É uma boa prática **aplicar filtros** de **entrada** e **saída** para cada vizinho, **ANTES** de estabelecer qualquer sessão eBGP.



Image by storyset on Freepik

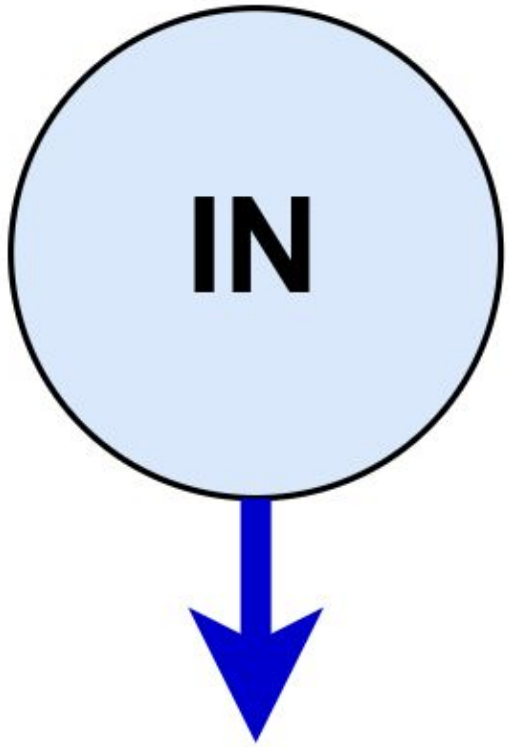
Filtros de Entrada

- **Clientes**
  - Apenas os prefixos que foram designados (por você mesmo) ao cliente
  - Ou alocados a ele pelo NIC.br ou por um RIR
- **Trânsito (Upstream)**
  - Full Routing
  - Rota Default



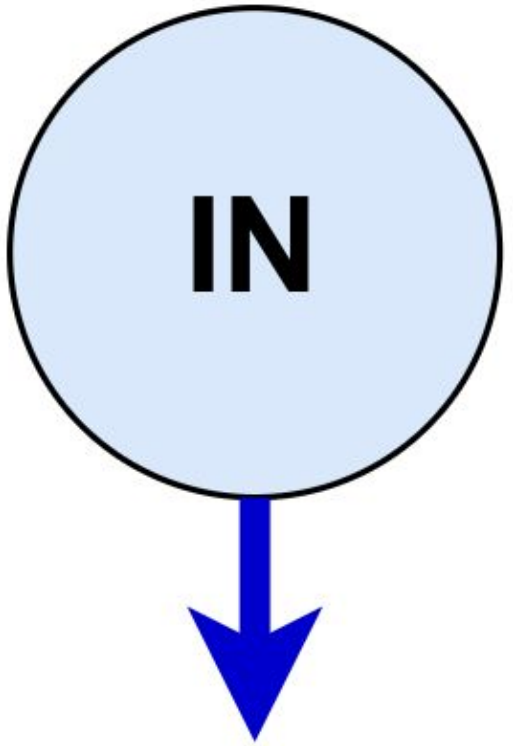
Filtros de Entrada

- **Peers (com quem realizamos troca de tráfego)**
  - Combinar os Prefixos que serão anunciados ou aceitos
  - Em caso de sessões em um acordo ATM no IX, deve-se receber todos os prefixos, com as seguintes exceções:
    - **Se você tem clientes de trânsito no IX**
      - Filtrar os prefixos dele, evitando que o tráfego para o cliente seja via IX
    - **Se você têm upstreams no IX**
      - Desejável filtrá-los forçando o tráfego a fluir pelo link de trânsito em ambas as direções
      - Evitar assimetrias.



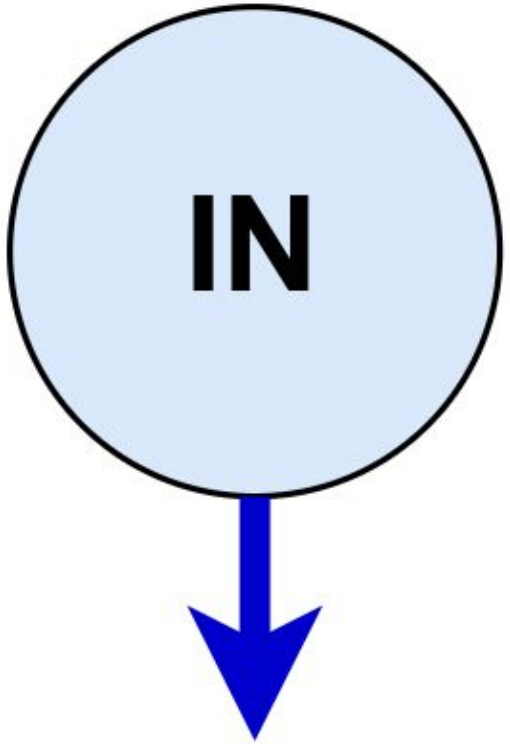
Filtros de Entrada

- Verifique a **lista do bogons** (prefixos que não deveriam aparecer no BGP), do **Team Cymru**
  - www.team-cymru.org/Services/Bogons/http.html
- **Para IPv4**
  - É preciso lembrar que **não há mais endereços reservados para alocações futuras.** Deve-se remover todos os filtros baseados no status dos blocos nos RIRs.
    - http://tools.ietf.org/html/rfc6441
- **Para IPv6**
  - Você pode **bloquear** tudo por **padrão** e **permitir** apenas o **2000::/3**, ou os prefixos mais específicos **/12 e /23** sob responsabilidade de cada **RIR**.
  - **Alguns bogons** podem estar **dentro do espaço dos RIRs**, então também **devem ser bloqueados explicitamente.**
- Feed automático de bogons:
  - http://www.team-cymru.org/Services/Bogons/routeserver.html



Filtros de Entrada

- Aplicando **corretamente os filtros**, você ajuda a:
  - *Garantir a integridade da sua própria rede*
  - *Garantir a integridade de toda a Internet*
- É **responsabilidade** de cada **Sistema Autônomos** ser um **bom cidadão da Internet!!!**

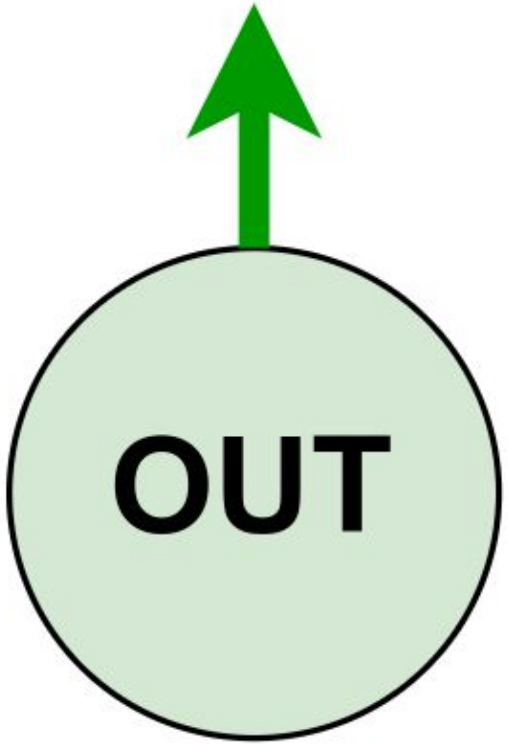


Prefixos no iBGP

- O **iBGP** deve ser usado para:
  - Transportar os **prefixos** de seus **clientes/usuários**.
  - Não use **OSPF** ou outro **IGP**.
- Crie uma rota estática para a interface do cliente (ou agregador).
- Use **“bgp network”** para originar o **prefixo** no **iBGP**
- O prefixo existirá enquanto a rota estática existir e a interface estiver ativa.
- Esses prefixos não são exportados no eBGP.

Prefixos no eBGP

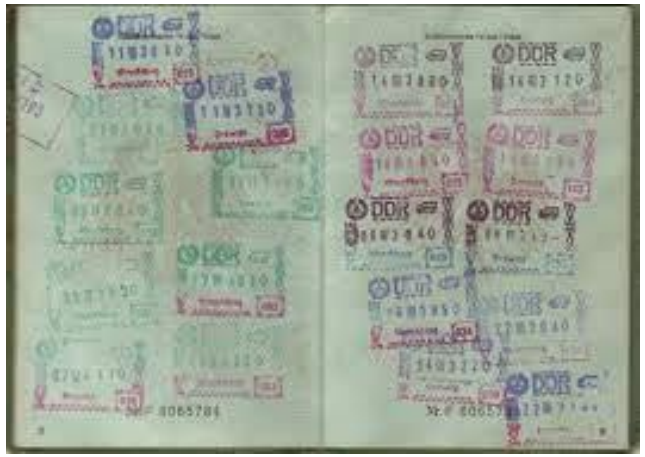
- No **eBGP** devem estar presentes:
  - Apenas os prefixos agregados,
  - Prefixos necessários para engenharia de tráfego.
- Os **prefixos** usados para **engenharia de tráfego** não **dependem** daqueles presentes no **iBGP**.
  - Os **prefixos** presentes no **iBGP** **não devem ser exportados para o eBGP.**
- Os prefixos usados para engenharia de tráfego devem ser gerados na **borda da rede**, com **rotas estáticas para null** e comandos do tipo **“bgp network”**.



Communities

- Descritas na **RFC 1997**
  - Cada community é um número inteiro de 32 bits, representada por dois inteiros de 16 bits (RFC 1998)
- **Communities** são usadas para agrupar destinos
  - Pode-se marcar um grupo de caminhos aprendidos, ou a exportar, com uma determinada community, de acordo com filtros
  - Pode-se filtrar rotas, ou modificar outros atributos, segundo às communities a qual a rota pertence
- São **úteis para aplicar políticas tanto dentro do AS, quanto entre diferentes ASes**







Dúvidas?



Patrocínio Terabyte







Apoio de Mídia





Obrigado!

CEPTRO.br Cursos: cursosceptro@nic.br
CEPTRO.br IPv6: ipv6@nic.br

@comunicbr
@nicbr
@NICbrvideos

nic.br cgi.br

www.nic.br | www.cgi.br