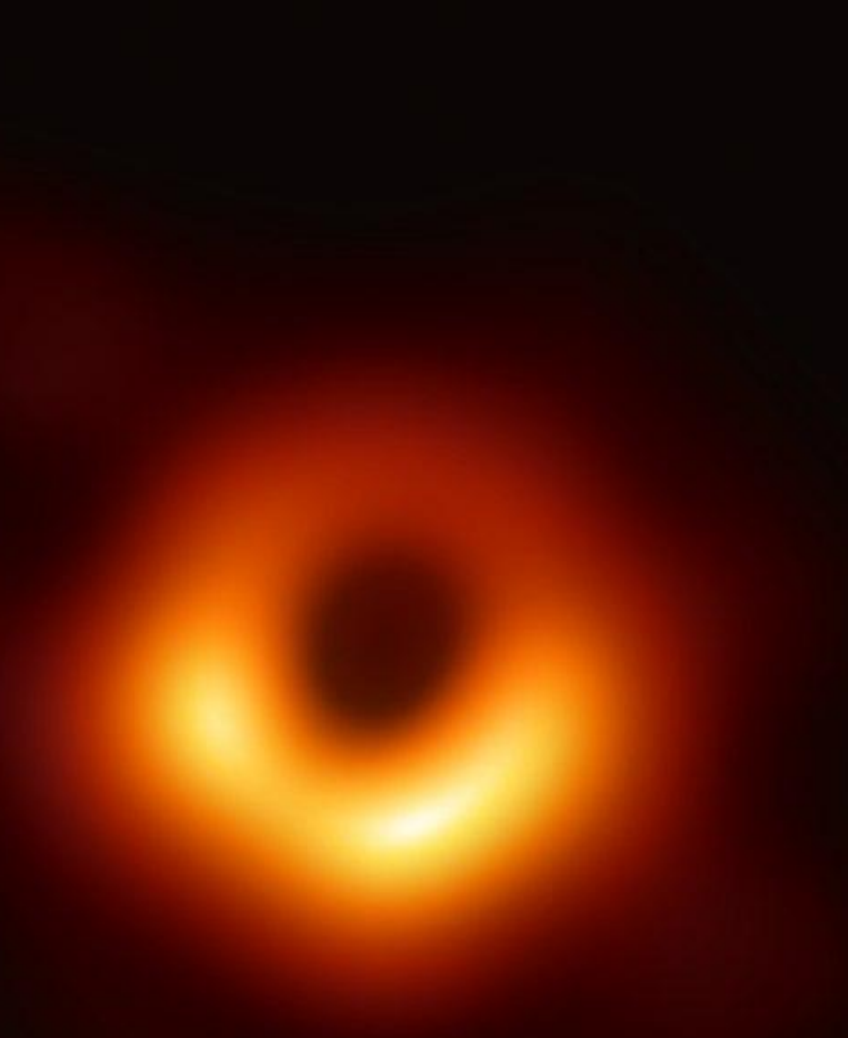
IX FÓRUM 15 - DEZEMBRO DE 2021

Blackhole no IX.br

Antonio M. Moreiras
Julio Sirota

Blackhole, previsto pela relatividade geral, é uma região do espaço-tempo em que o campo gravitacional é tão intenso que nada, nenhuma partícula ou radiação eletromagnética como a luz, pode escapar dela.

Esta é a foto do buraco negro supermassivo no centro da galáxia elíptica supergigante Messier 87, com uma massa de 7 bilhões de vezes a do Sol, obtida pelo telescópio Event Horizon em 2019.



O **blackhole no IX** atrai **todo o tráfego** destinado aos **prefixos selecionados**, de forma que esse tráfego não chega ao destino.

Pode ser ativado para participantes individuais com anúncio específico e communities adicionais.

Benefício ao usar um blackhole durante um ataque:
- o tráfego é interrompido

Problema em usar um blackhole durante um ataque:
- o tráfego é interrompido

Singularidade: no centro de um buraco negro está uma singularidade gravitacional, uma região onde a curvatura do espaço-tempo se torna infinita. As leis da física como as conhecemos não se aplicam ali.

Singularidade do blackhole do IX: algumas regras nos filtros do roteamento BGP têm que ser alteradas na rede do IX e dos participantes. As boas práticas convencionais colapsam e precisamos de algo diferente.

Os participantes DEVEM aceitar os prefixos **/128 IPv6** e **/32 IPv4** anunciados pelos RS com a **community de blackhole**, sem fazer validação de RPKI

O **Servidor de Rotas** (RS) do IX.br aceita os prefixos **/128 IPv6** e **/32 IPv4** anunciados com a **community de blackhole** e os repassa para os participantes, trocando o IP de NEXT HOP por um IP da rede do IX.br.

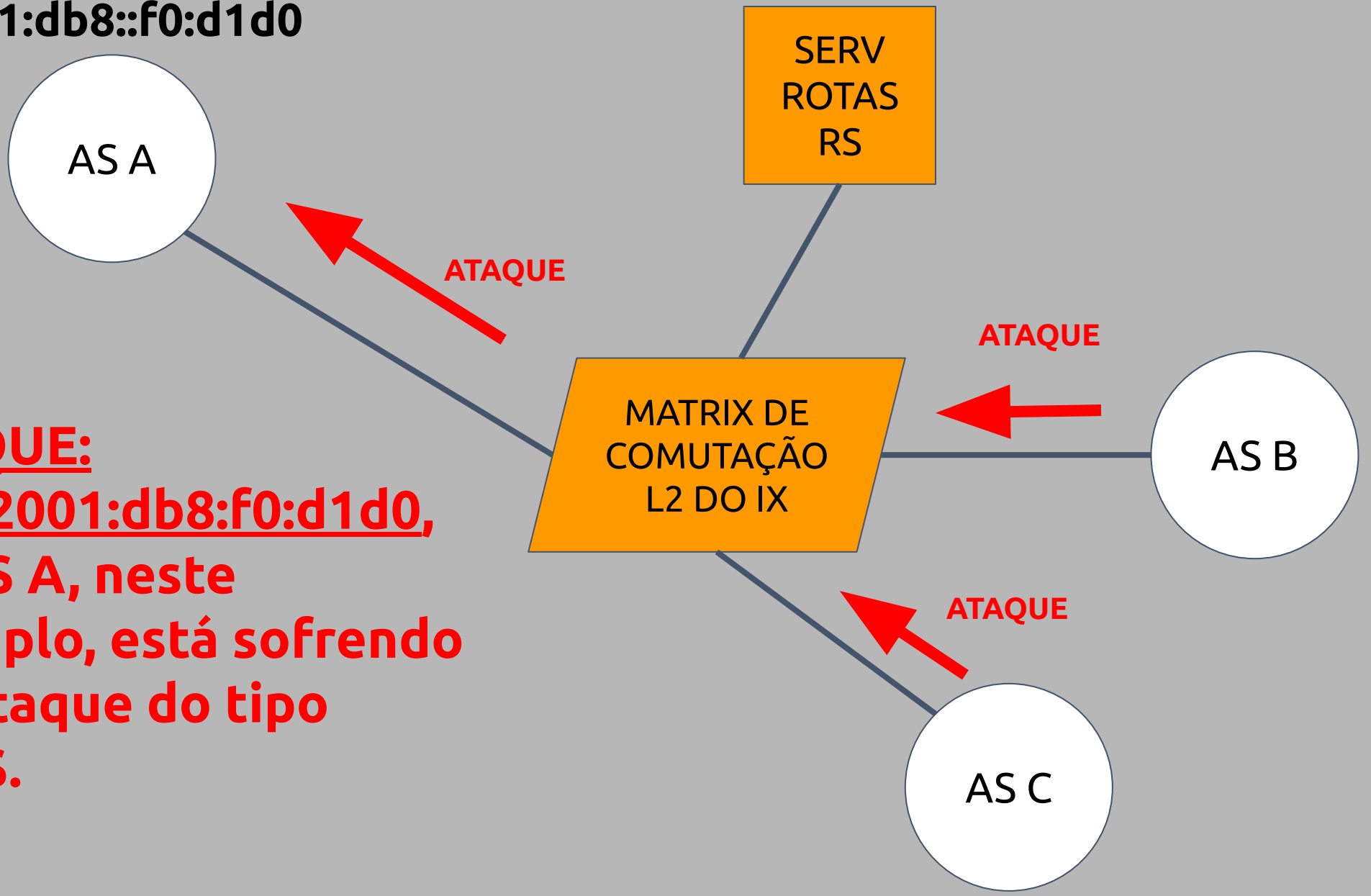
Os RS aceitam **apenas**
prefixos /128 IPv6 e
/32 IPv4 **pertencentes aos blocos de IP alocados pelo Registro.br**
aos AS participantes.

Os RS aceitam **apenas** prefixos /128 IPv6 e /32 IPv4 **pertencentes aos AS diretamente conectados ao IX**, onde o AS de origem é igual ao neighbour.

O **IP de NEXT HOP** repassado para os participantes pelo RS em um blackhole é **resolvido para um MAC ADDRESS** registrado para o IX.br e que é **bloqueado por uma ACL** em todos os switches.

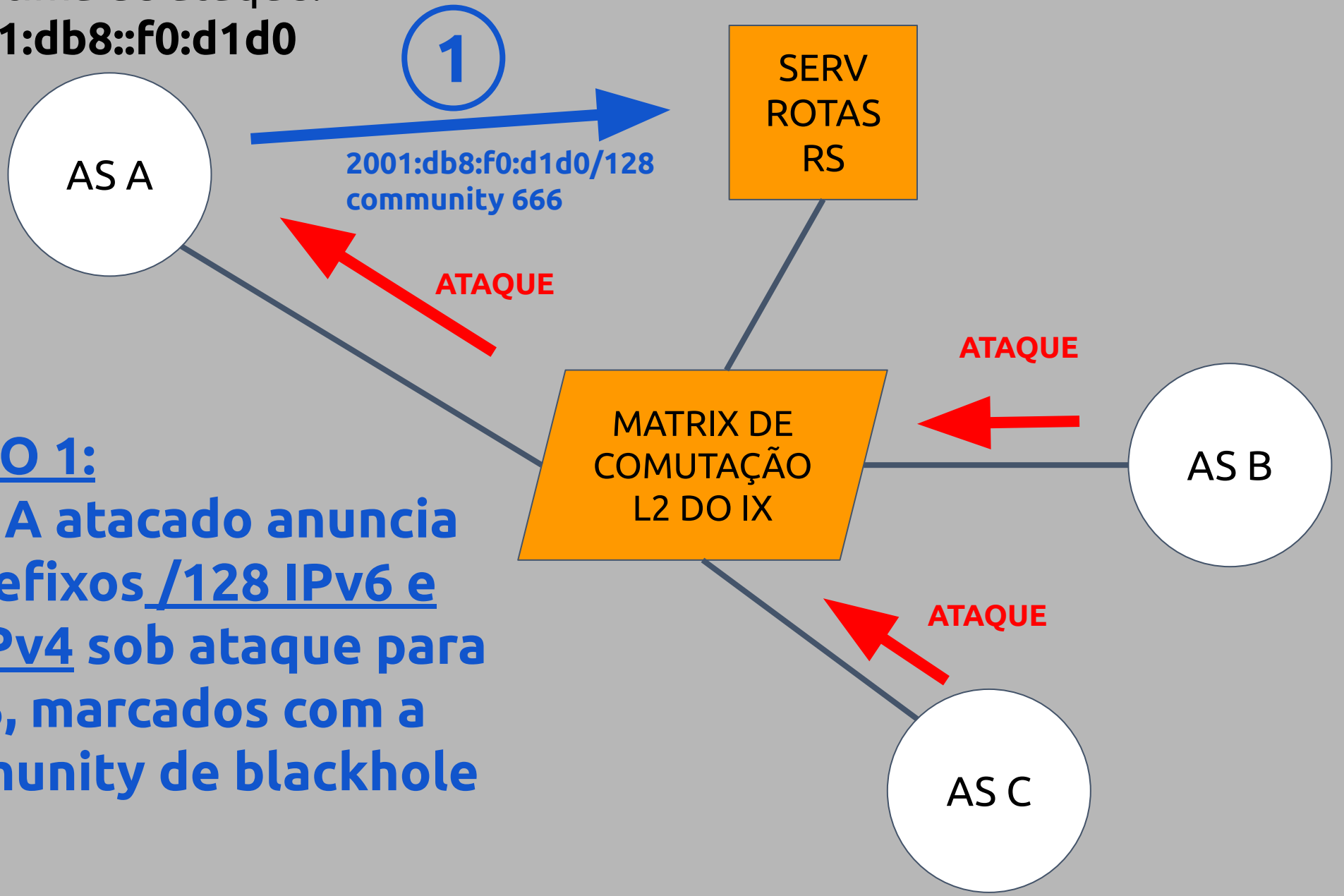
O tráfego é descartado na borda.

IP vítima de ataque:
2001:db8::f0:d1d0



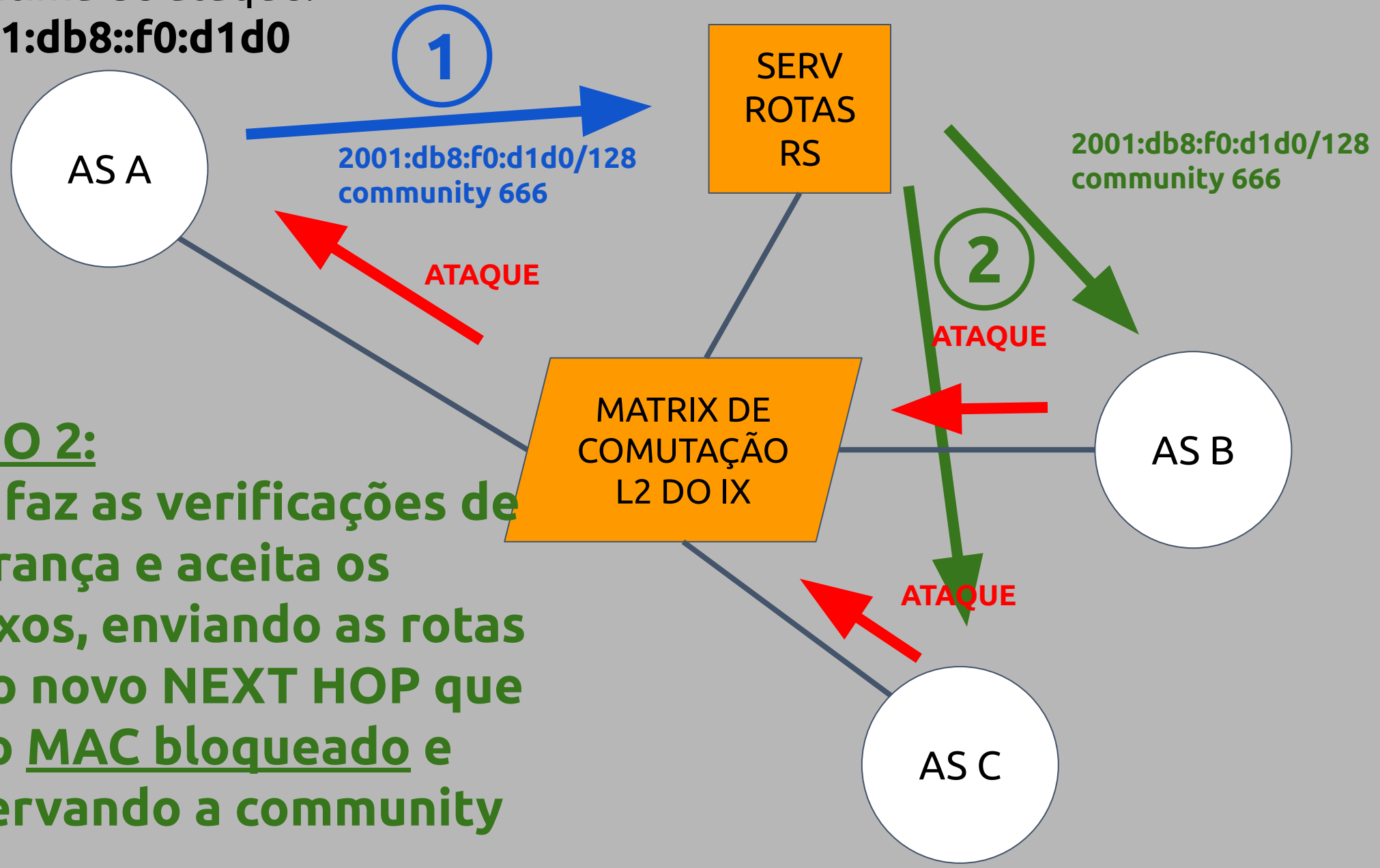
ATAQUE:
O IP 2001:db8:f0:d1d0, do AS A, neste exemplo, está sofrendo um ataque do tipo DDoS.

IP vítima de ataque:
2001:db8::f0:d1d0



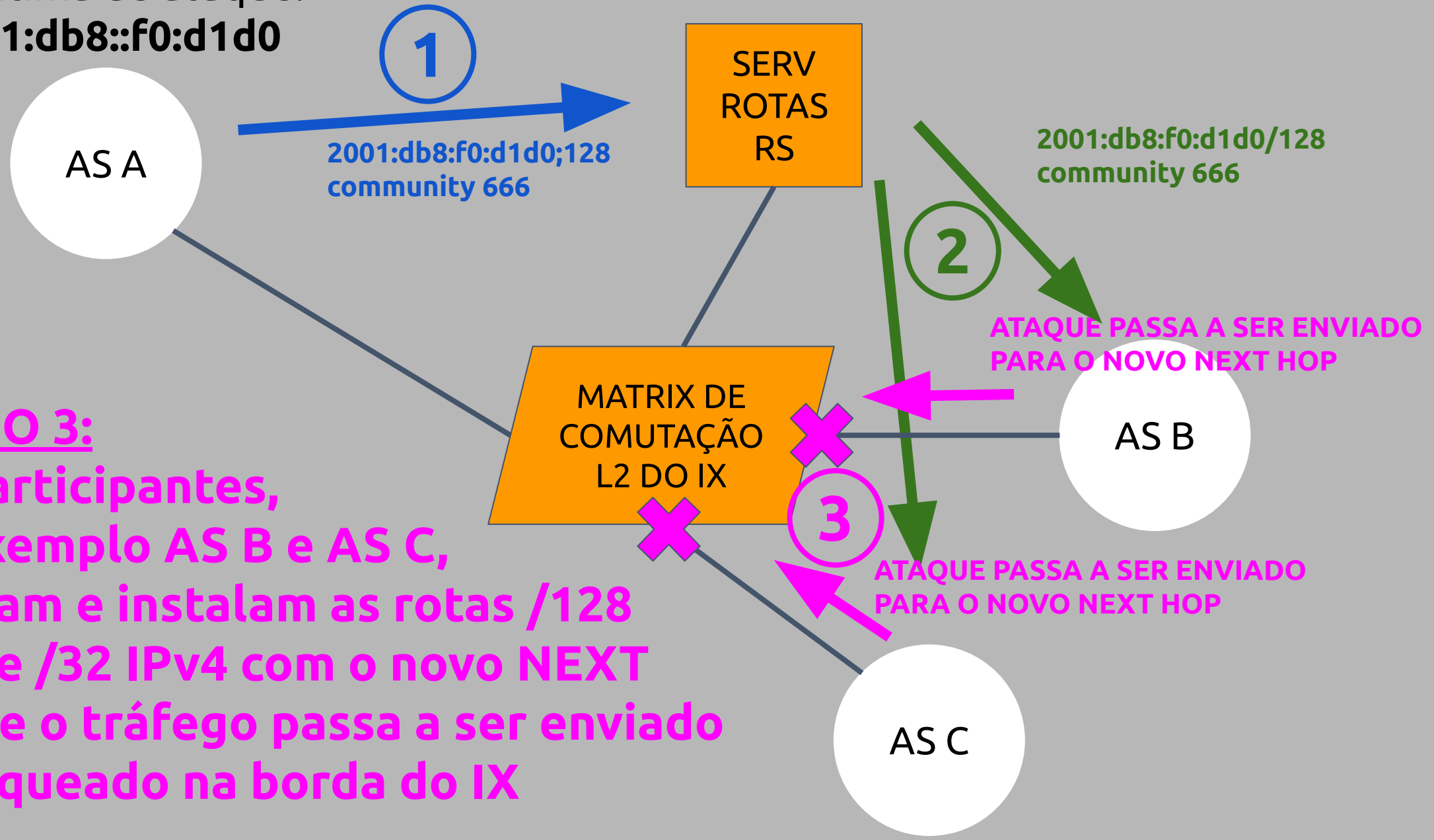
PASSO 1:
O AS A atacado anuncia os prefixos /128 IPv6 e /32 IPv4 sob ataque para os RS, marcados com a community de blackhole

IP vítima de ataque:
2001:db8::f0:d1d0



PASSO 2:
O RS faz as verificações de segurança e aceita os prefixos, enviando as rotas com o novo NEXT HOP que tem o MAC bloqueado e preservando a community

IP vítima de ataque:
2001:db8::f0:d1d0



PASSO 3:

Os participantes, no exemplo AS B e AS C, aceitam e instalam as rotas /128 IPv6 e /32 IPv4 com o novo NEXT HOP e o tráfego passa a ser enviado e bloqueado na borda do IX

Já funciona em CAMPINAS e VITÓRIA. No início de 2022 estará habilitado em todas as localidades.

Os participantes **PRECISAM ALTERAR** as configurações para aceitar os prefixos /128 e /32 com a community de blackhole dos RS.

DÚVIDAS?

jsirota@nic.br
moreiras@nic.br