Sequestros de prefixo: o que são, como acontecem, como se defender e o quê engenharia de tráfego tem a ver com isso?

Pedro Marcos, Renan Barreto
pbmarcos@furg.br

FURG
UNIVERSIDADE FEDERAL
DO RIO GRANDE

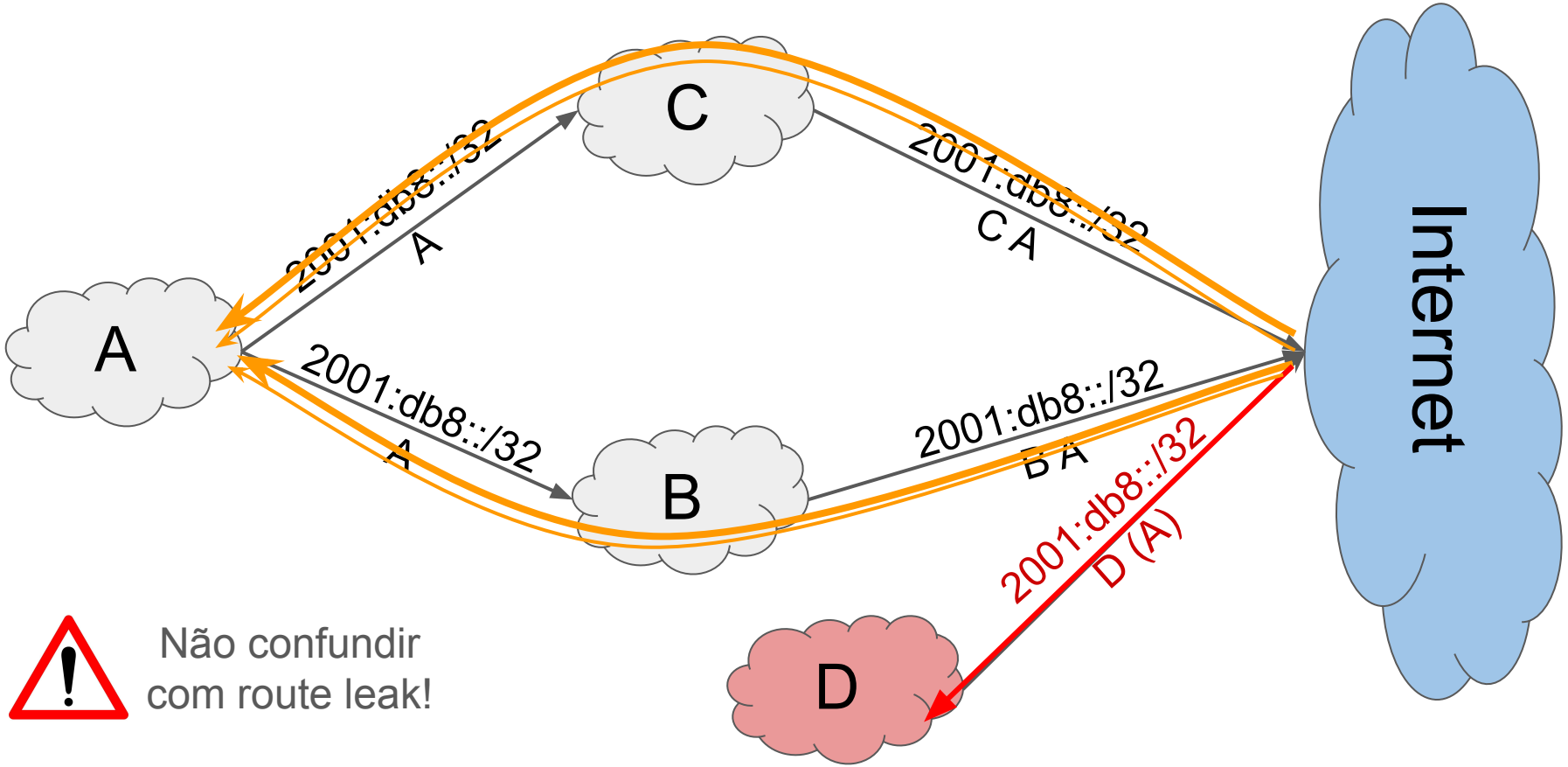
04 de julho de 2025

Você já deve ter visto alguma dessas notícias

Cerca de 10 sequestros por dia (Holterbach, 2024)

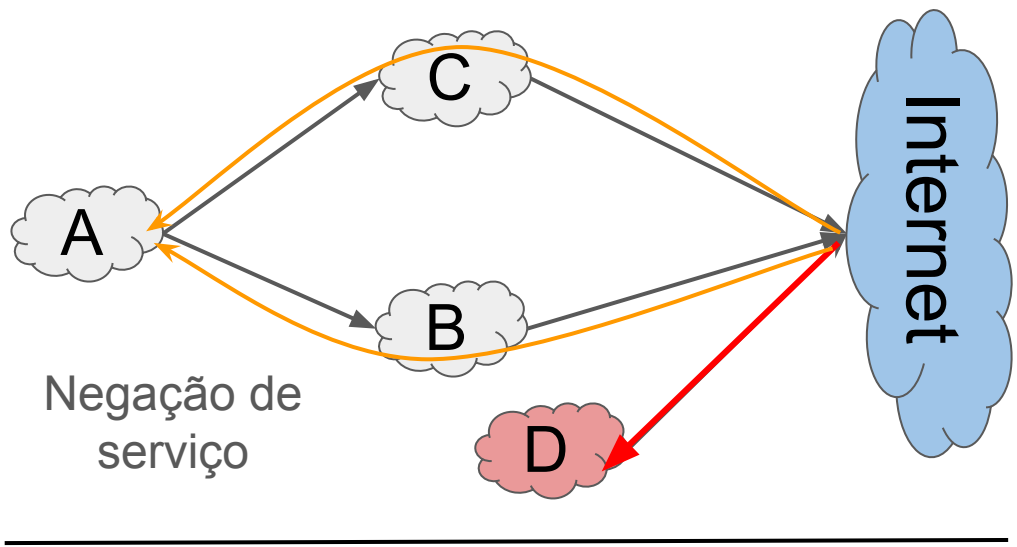
Thomas Holterbach, Thomas Alfroy, Amreesh Phokeer, Alberto Dainotti, and Cristel Pelsser. 2024. A system to detect forged-origin BGP hijacks. In Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI'24). USENIX Association, USA, Article 96, 1751–1770.

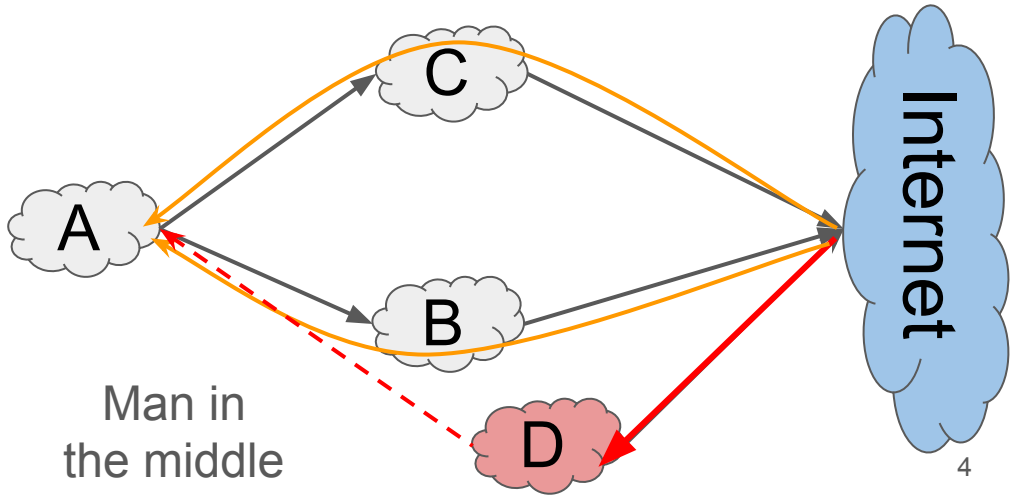
Mas afinal, o que é um sequestro de prefixo?

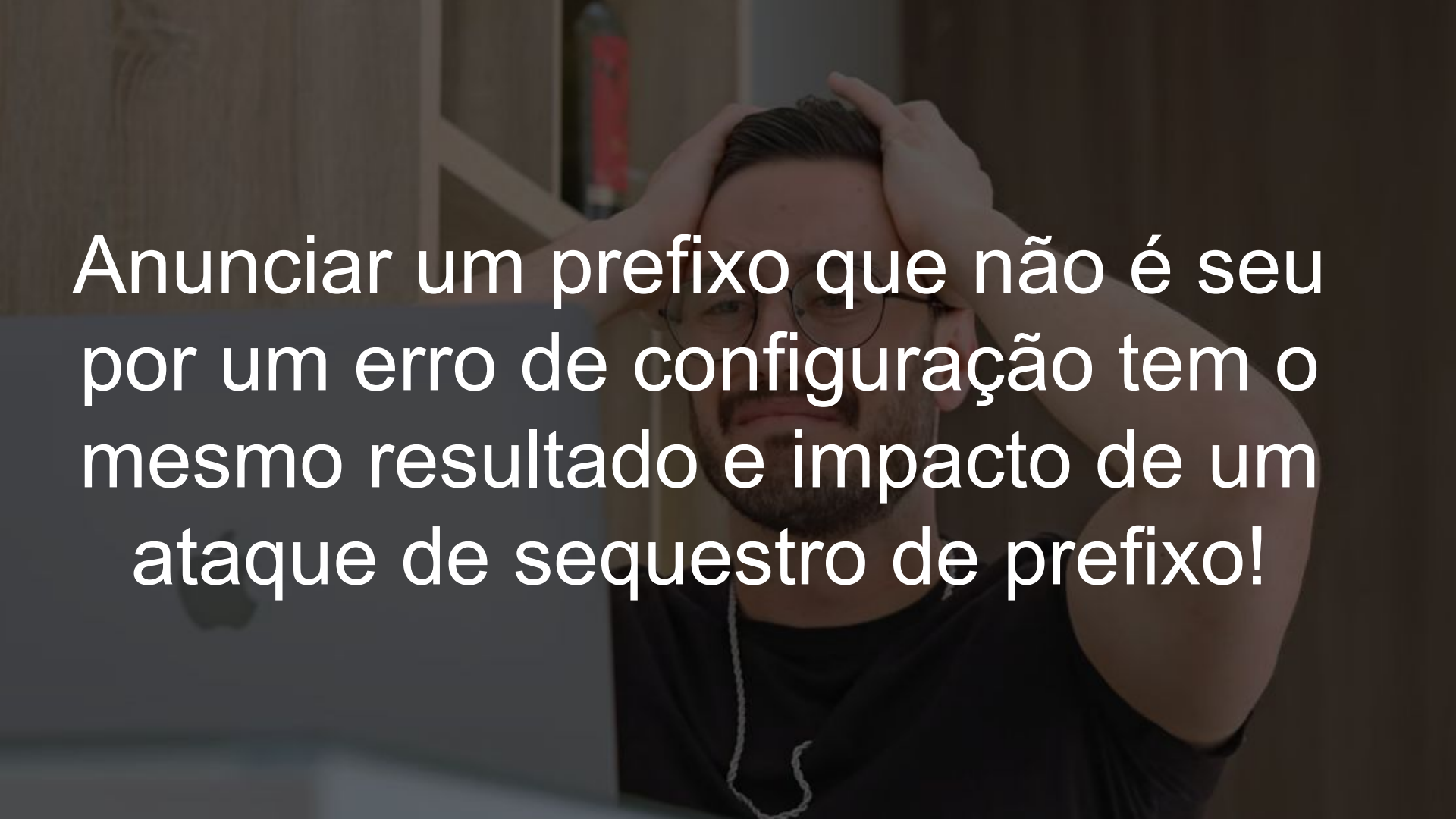


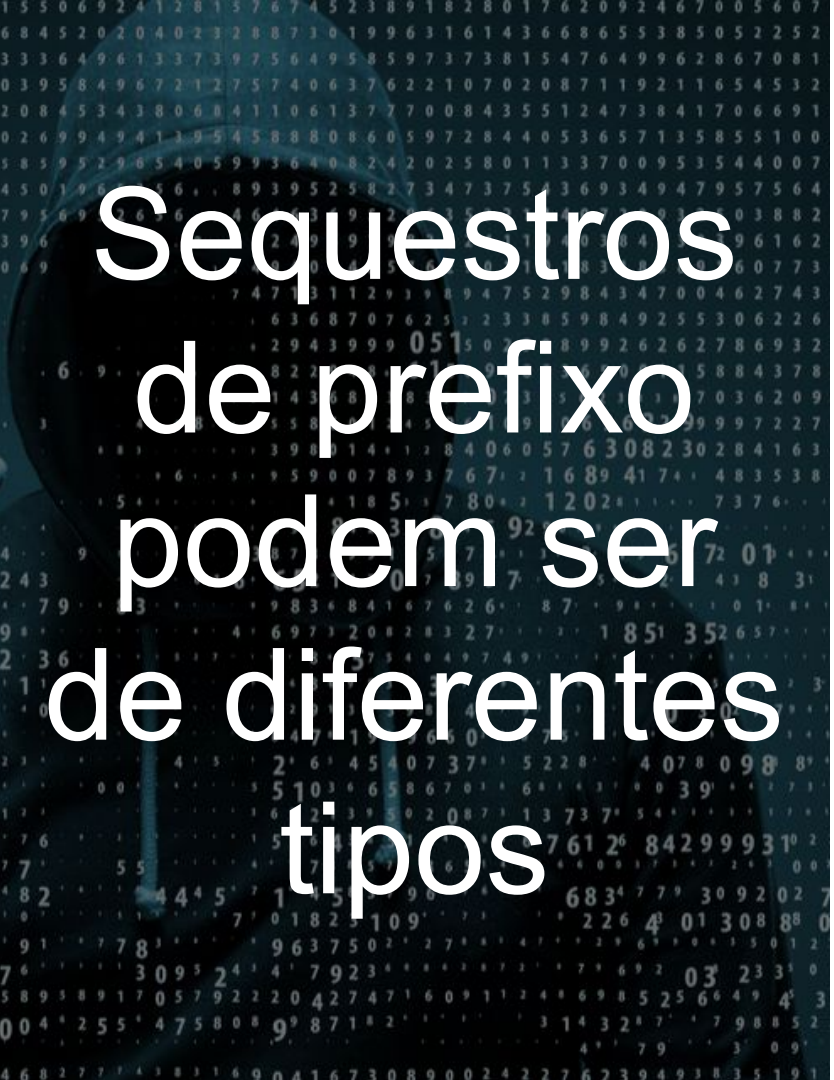
Não confundir
com route leak!

Sequestros de prefixo possuem dois objetivos principais






Anunciar um prefixo que não é seu por um erro de configuração tem o mesmo resultado e impacto de um ataque de sequestro de prefixo!



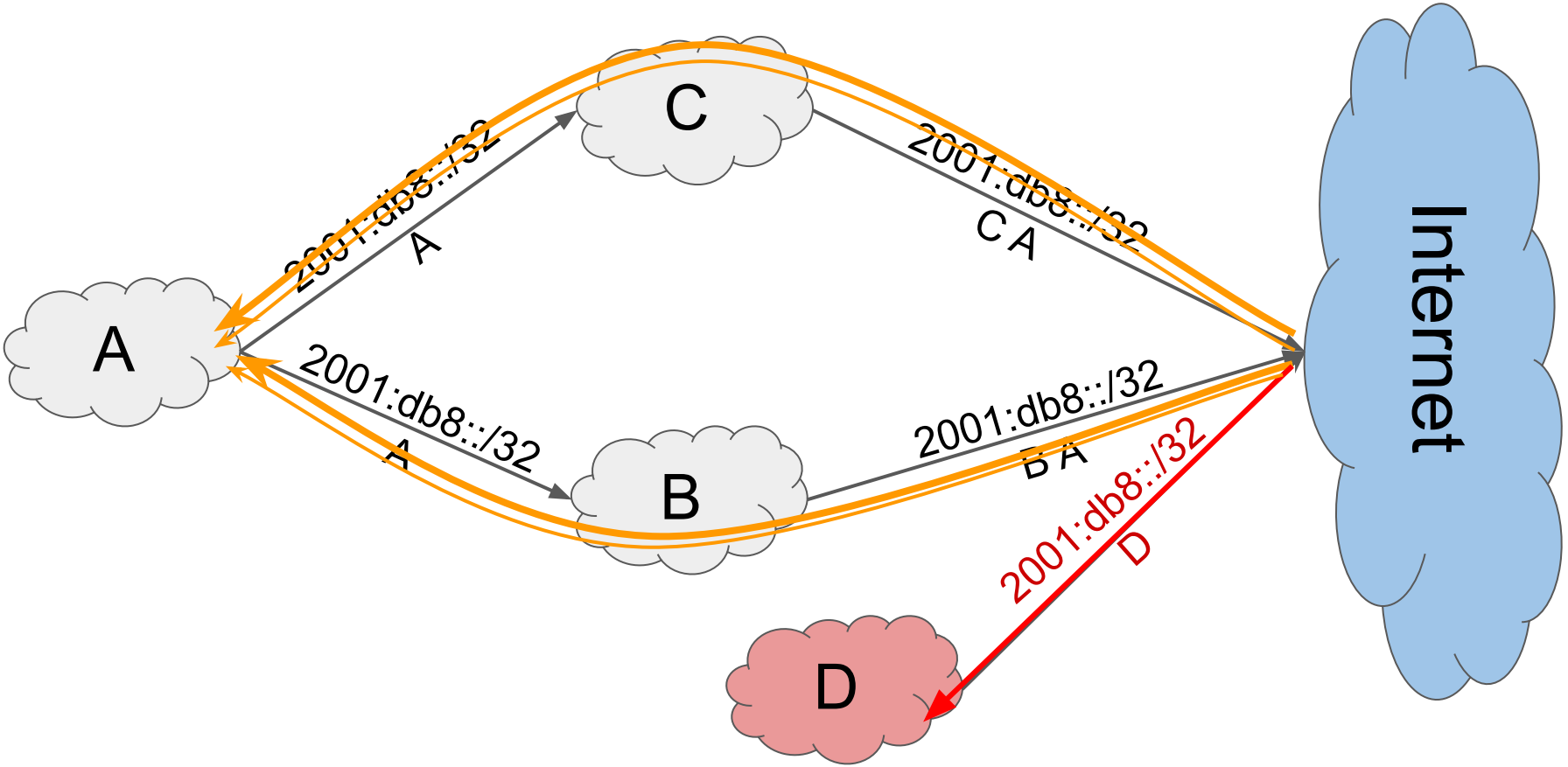
Sequestros de prefixo podem ser de diferentes tipos

Sequestro simples: anuncia o prefixo com um AS originador não legítimo

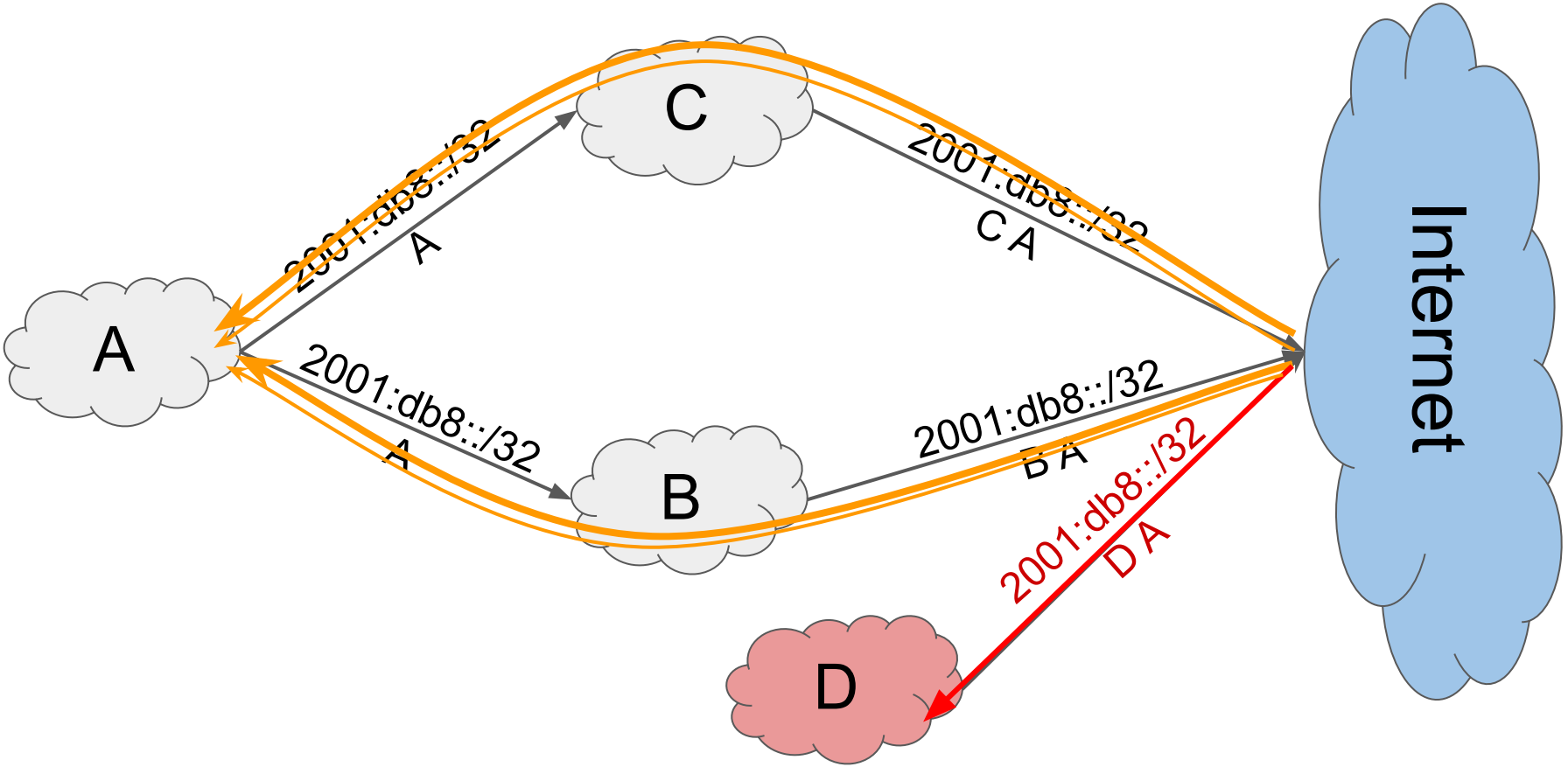
Sequestro com caminho forjado: anuncia o prefixo mantendo o originador legítimo

Sequestro parcial: anuncia um sub-prefixo da vítima

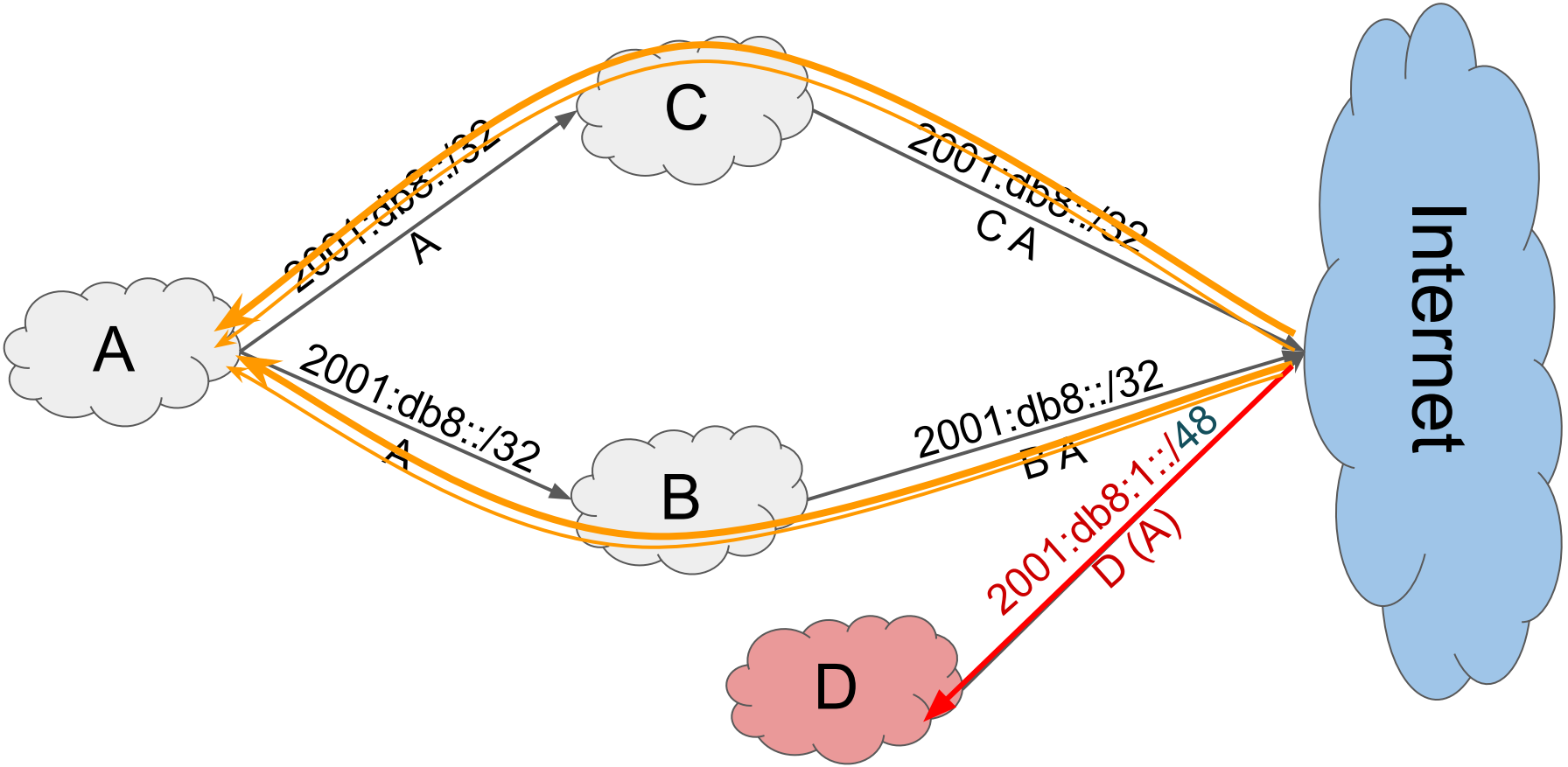
Sequestro simples

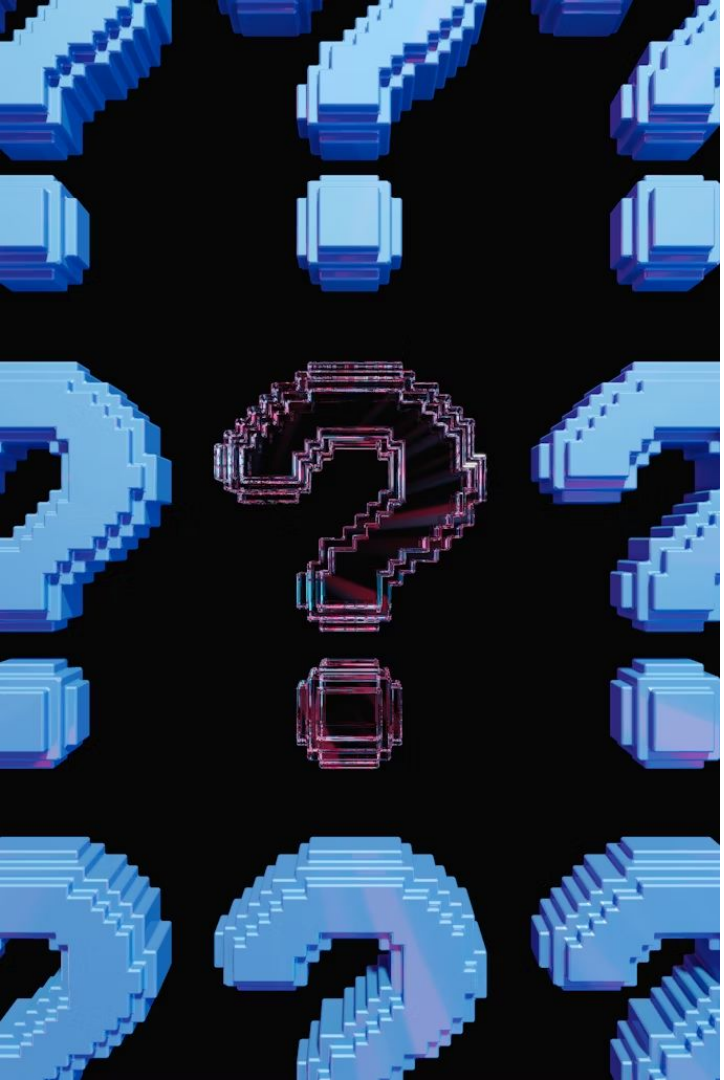


Sequestro com caminho forjado



Sequestro parcial (sub prefixo)

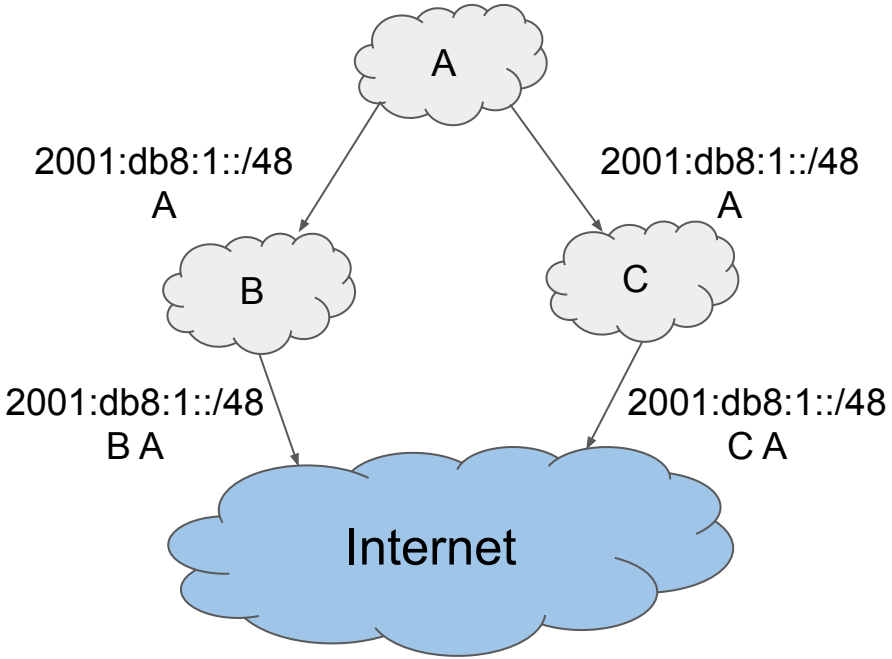




Por que os sequestros de prefixo funcionam?

O protocolo BGP não tem segurança?

O protocolo BGP, a “cola” que une a Internet, não tem mecanismos de segurança em sua concepção



Critérios para escolha da melhor rota

0. Prefixo mais específico (LPM protocolo IP)
1. Preferência local
2. Menor caminho
3. Menor tipo de origem (IGP < EGP < incompleto)
4. Menor MED
5. eBGP sobre iBGP
6. Menor IGP para o próximo hop BGP
7. Rota mais antiga
8. Menor ID do roteador BGP
9. Menor endereço do vizinho

Mas e agora, quem poderá nos defender?

Podemos lidar com sequestros de duas maneiras

Monitorando e reagindo

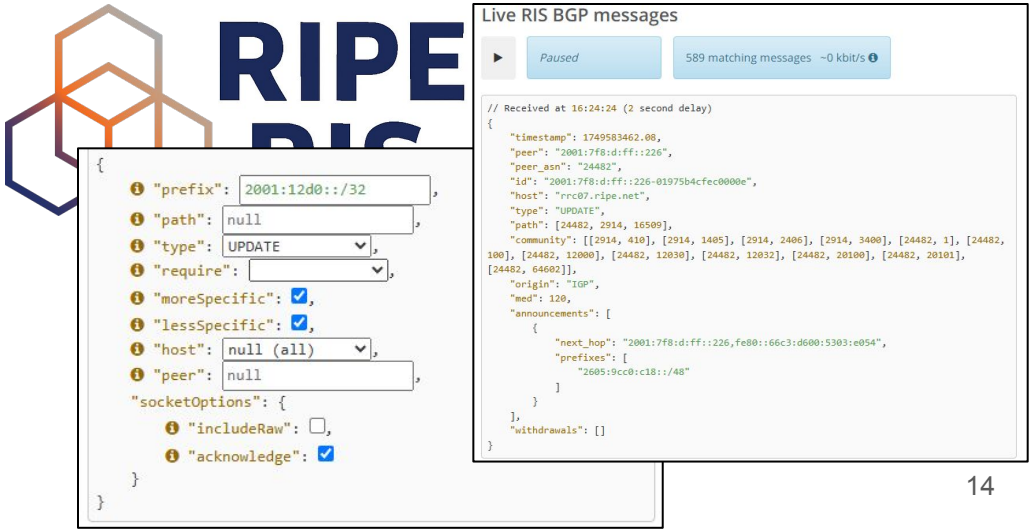
Prevenindo

Podemos monitorar os nossos prefixos em busca de anúncios suspeitos

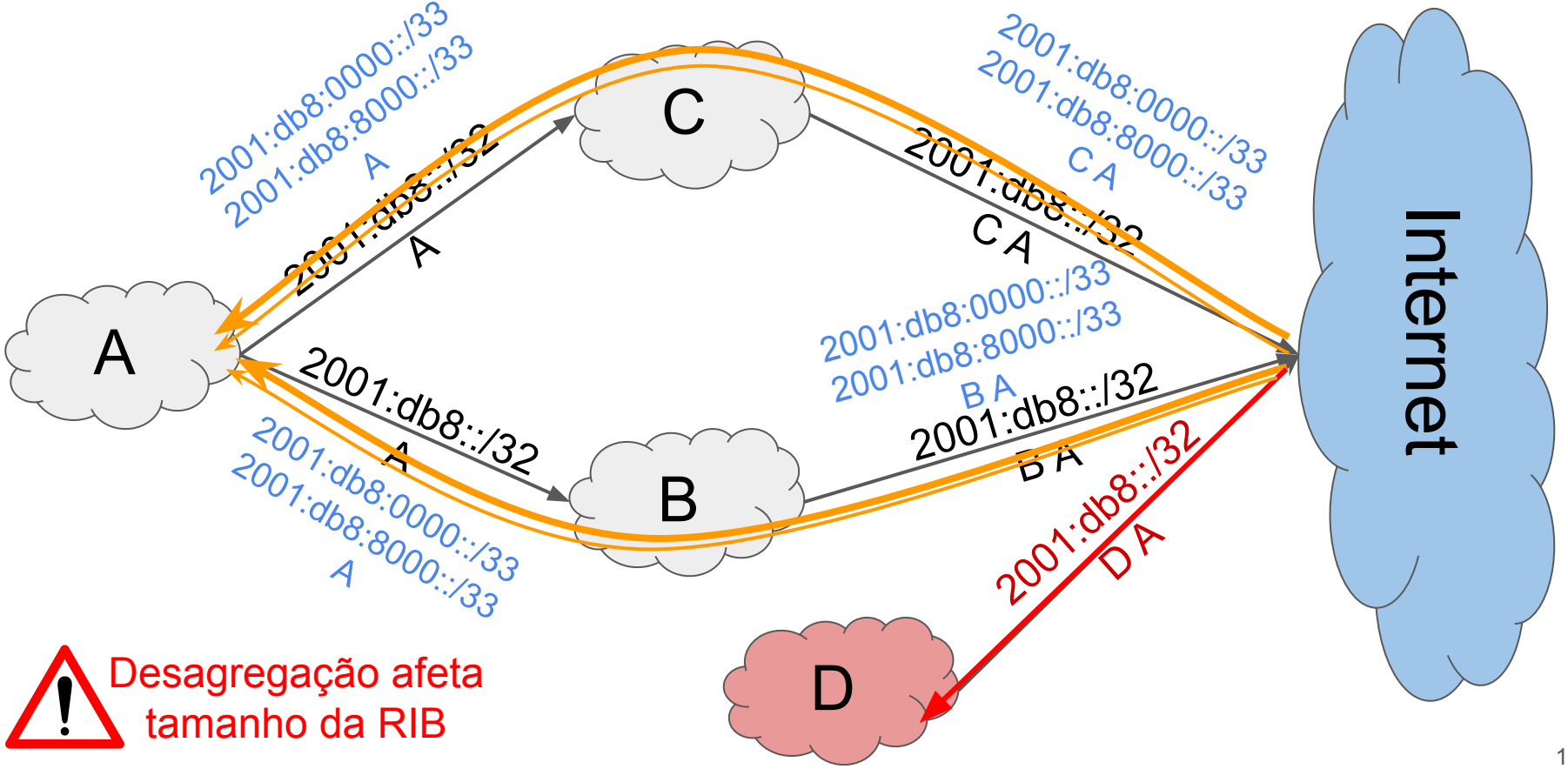
ARTEMIS

https://bgpartemis.readthedocs.io/en/latest/

Ferramenta *open-source* que monitora anúncios de prefixos, emite alertas permite configuração de ações de mitigação

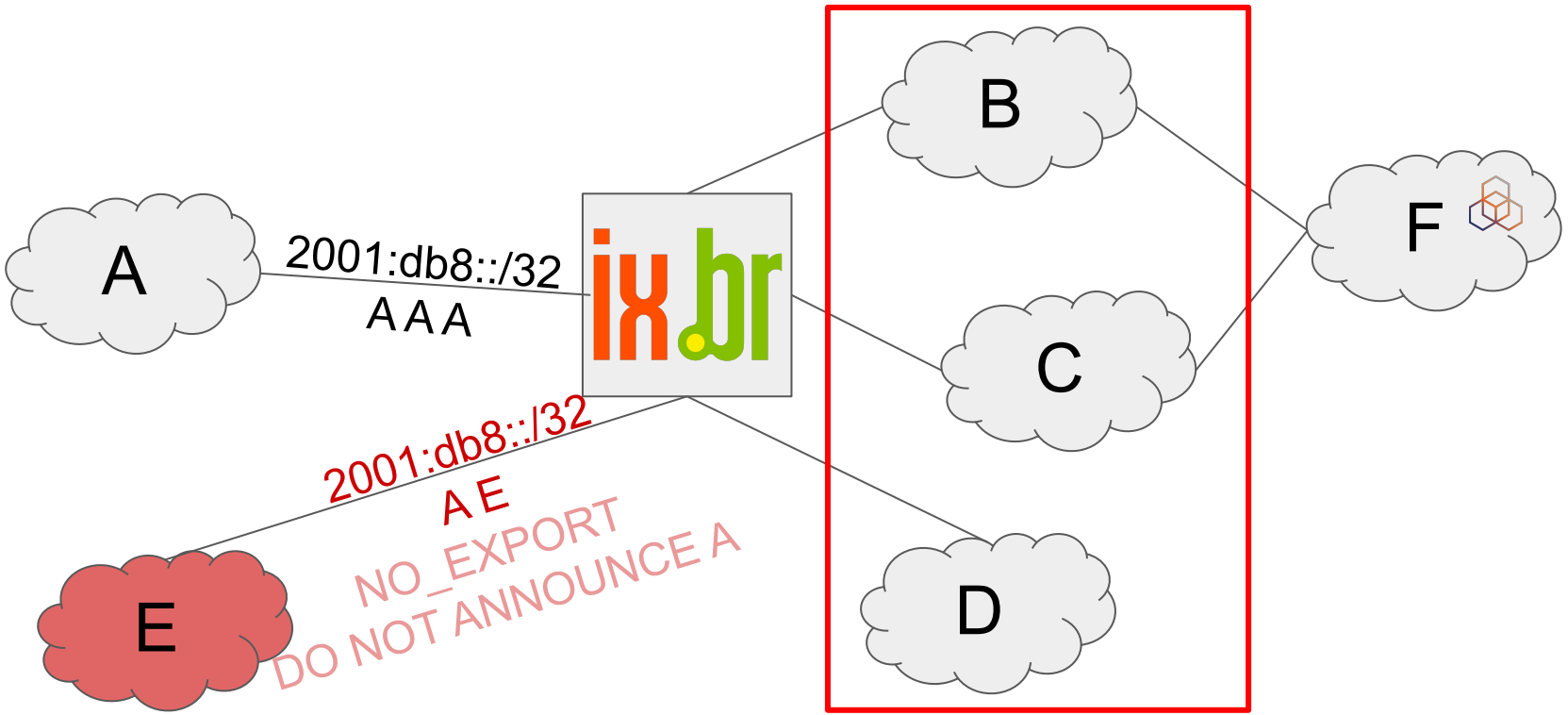


Mitigando com prefixos mais específicos



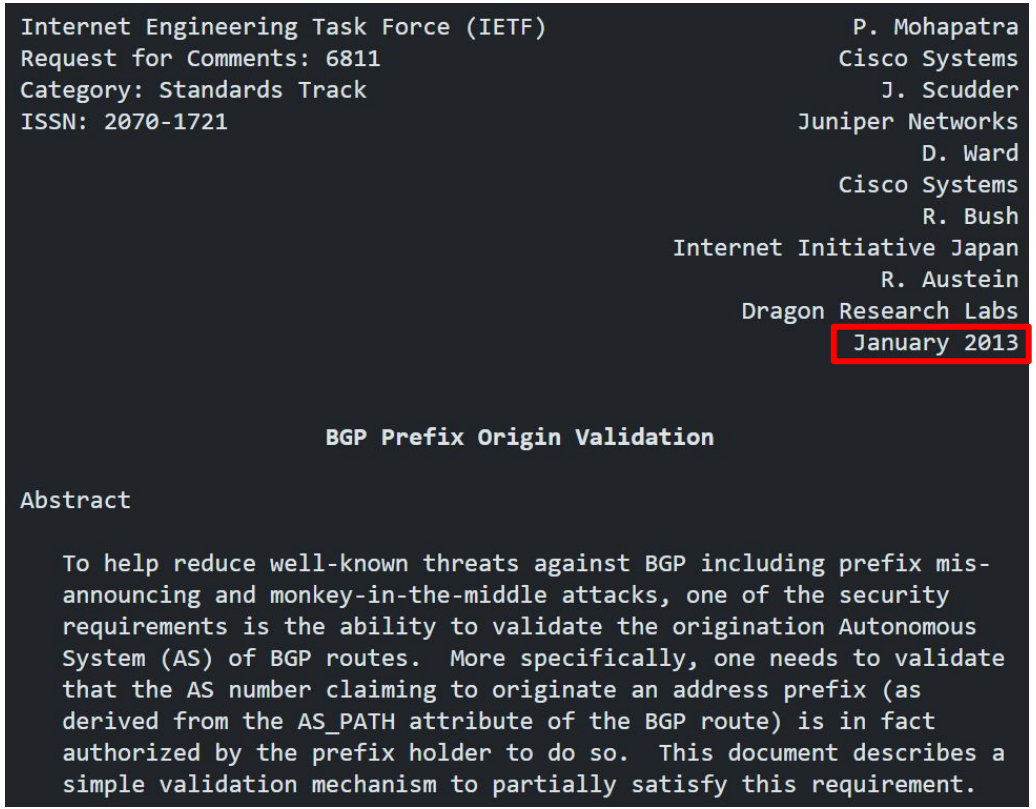
Desagregação afeta tamanho da RIB

Ao passo que as ferramentas de detecção evoluem, os ataques também tornam-se mais sofisticados e buscam evadir os sistemas de monitoramento



Existem diferentes técnicas para garantir a segurança do roteamento com BGP, nosso foco será em RPKI e ASPA

Validação de origem de prefixos com RPKI



Internet Engineering Task Force (IETF)
Request for Comments: 6811
Category: Standards Track
ISSN: 2070-1721

P. Mohapatra
Cisco Systems
J. Scudder
Juniper Networks
D. Ward
Cisco Systems
R. Bush
Internet Initiative Japan
R. Austein
Dragon Research Labs
January 2013

BGP Prefix Origin Validation

Abstract

To help reduce well-known threats against BGP including prefix mis-announcing and monkey-in-the-middle attacks, one of the security requirements is the ability to validate the origination Autonomous System (AS) of BGP routes. More specifically, one needs to validate that the AS number claiming to originate an address prefix (as derived from the AS_PATH attribute of the BGP route) is in fact authorized by the prefix holder to do so. This document describes a simple validation mechanism to partially satisfy this requirement.

Qual é o princípio do RPKI?

O RIR (i.e., LACNIC) gera um certificado digital atestando a alocação do prefixo para um determinado AS

O AS cria um objeto ROA (Route Origin Authorization) associado ao prefixo

Demais ASes validam os ROAs através de um processo chamado ROV (Route Origin Validation)

RPKI através de um exemplo

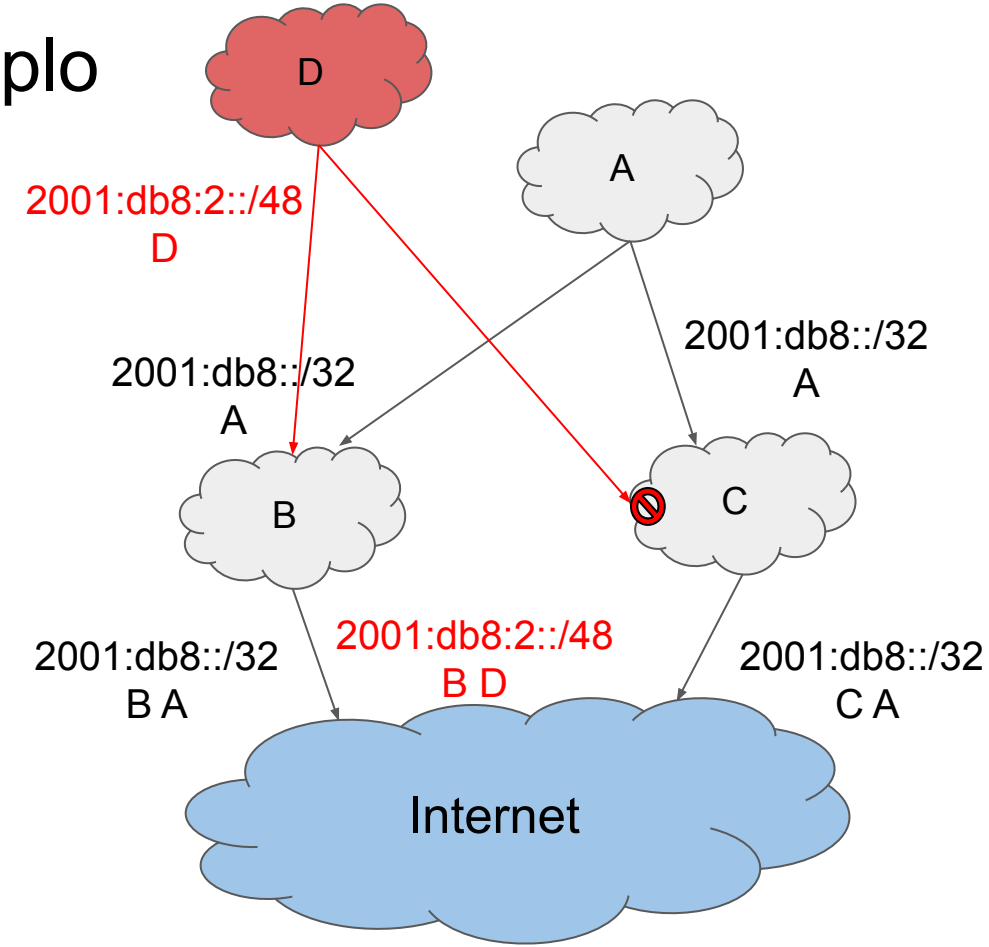
AS A recebeu do RIR o prefixo 2001:db8::/32 do seu RIR

AS A cria e publica o objeto ROA informando (entre outros):

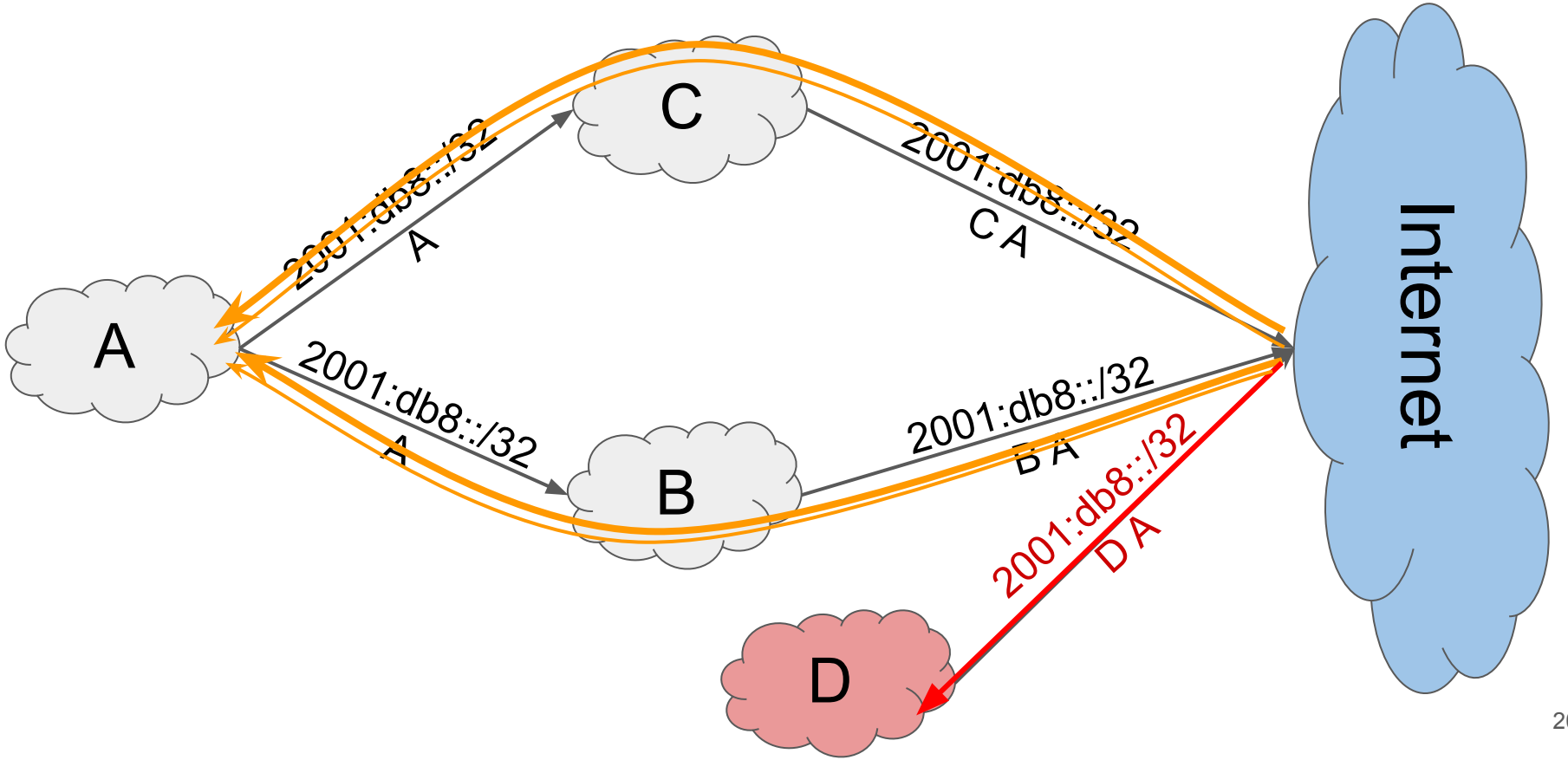
- ASN (i.e., A)
- Prefixo (2001:db8::/32)
- Max length (i.e, /32)
- Validade (2026-12-31)

AS A o anuncia o prefixo na Internet

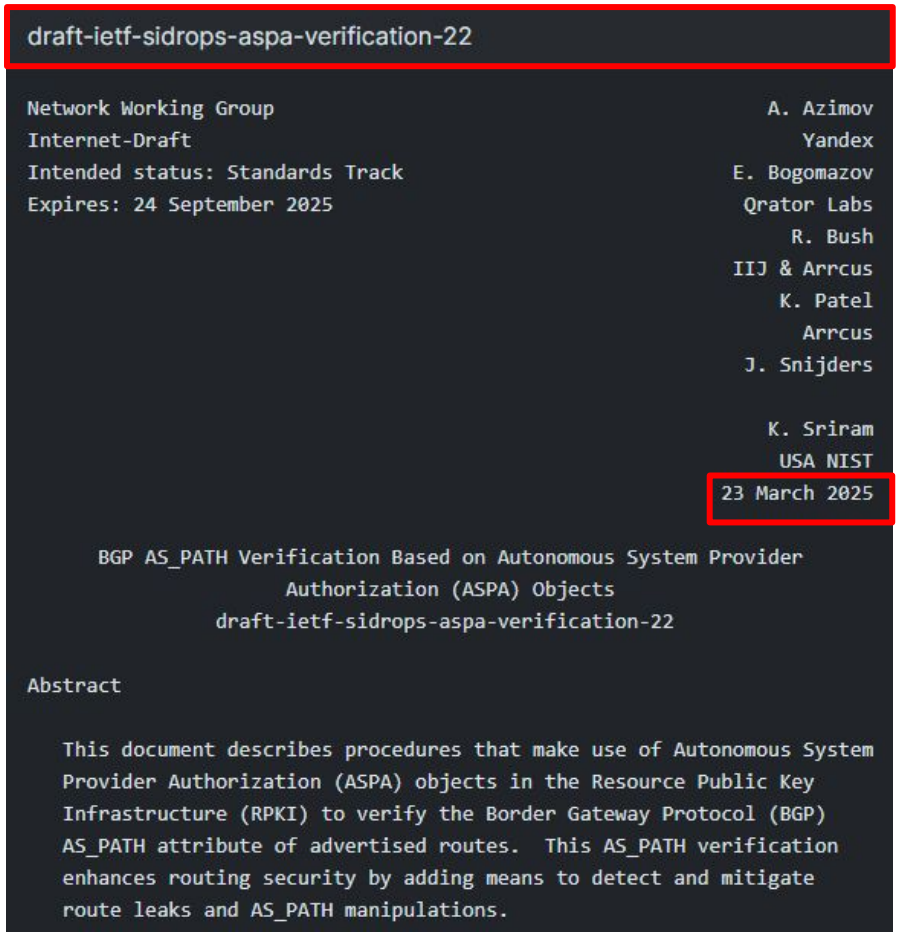
Outros ASes realizam (ou não) a validação



Como o RPKI pode ser burlado pelo atacante?



Validação de caminhos com ASPA



draft-ietf-sidrops-aspa-verification-22

Network Working Group — A. Azimov, Yandex
Internet-Draft — E. Bogomazov, Qrator Labs
Intended status: Standards Track — R. Bush, IIJ & Arrcus
Expires: 24 September 2025 — K. Patel, Arrcus
J. Snijders
K. Sriram, USA NIST
23 March 2025

BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects
draft-ietf-sidrops-aspa-verification-22

Abstract

This document describes procedures that make use of Autonomous System Provider Authorization (ASPA) objects in the Resource Public Key Infrastructure (RPKI) to verify the Border Gateway Protocol (BGP) AS_PATH attribute of advertised routes. This AS_PATH verification enhances routing security by adding means to detect and mitigate route leaks and AS_PATH manipulations.

Qual é o princípio do ASPA?

O AS cria um objeto ASPA (Autonomous System Provider Authorization) contendo a lista de ASes autorizados a propagar os seus prefixos

Os demais ASes verificam os objetos ASPA e validam se o prefixo foi propagado através de enlaces válidos

ASPA através de um exemplo

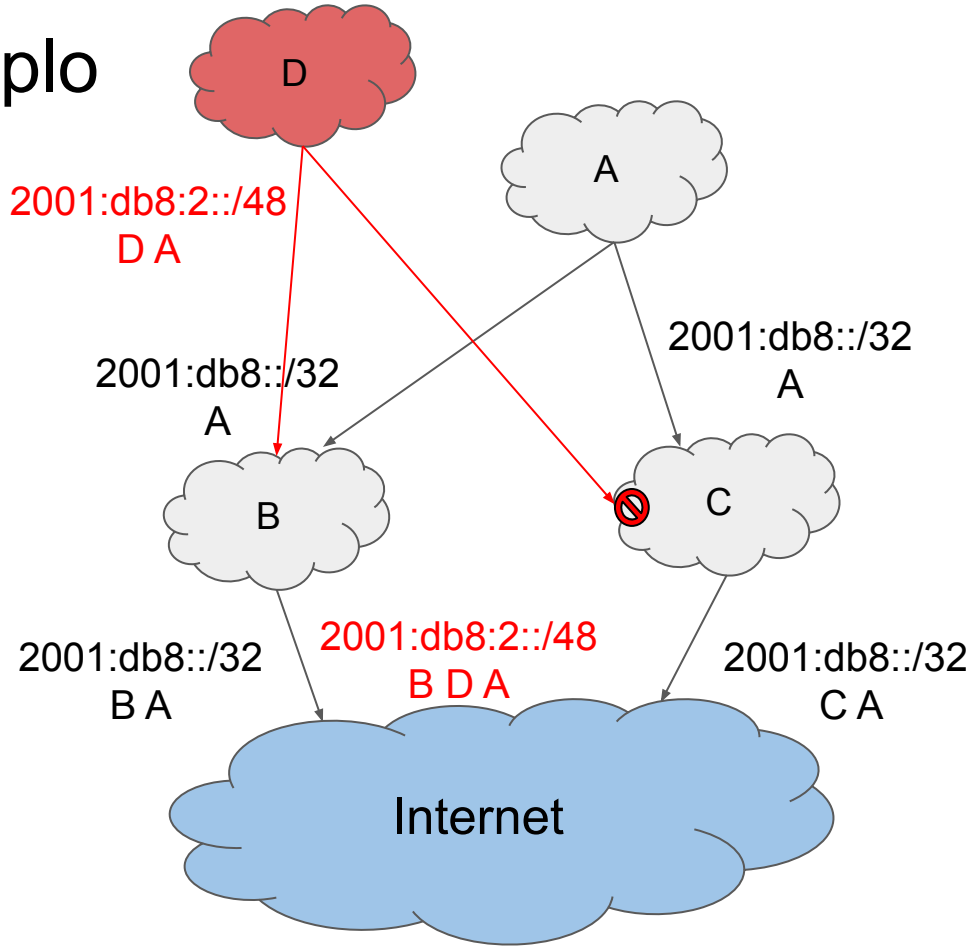
AS A está conectado aos ASes B e C

AS A cria e publica o objeto ASPA informando suas conexões:

- AS B
- AS C

AS A o anuncia o prefixo na Internet

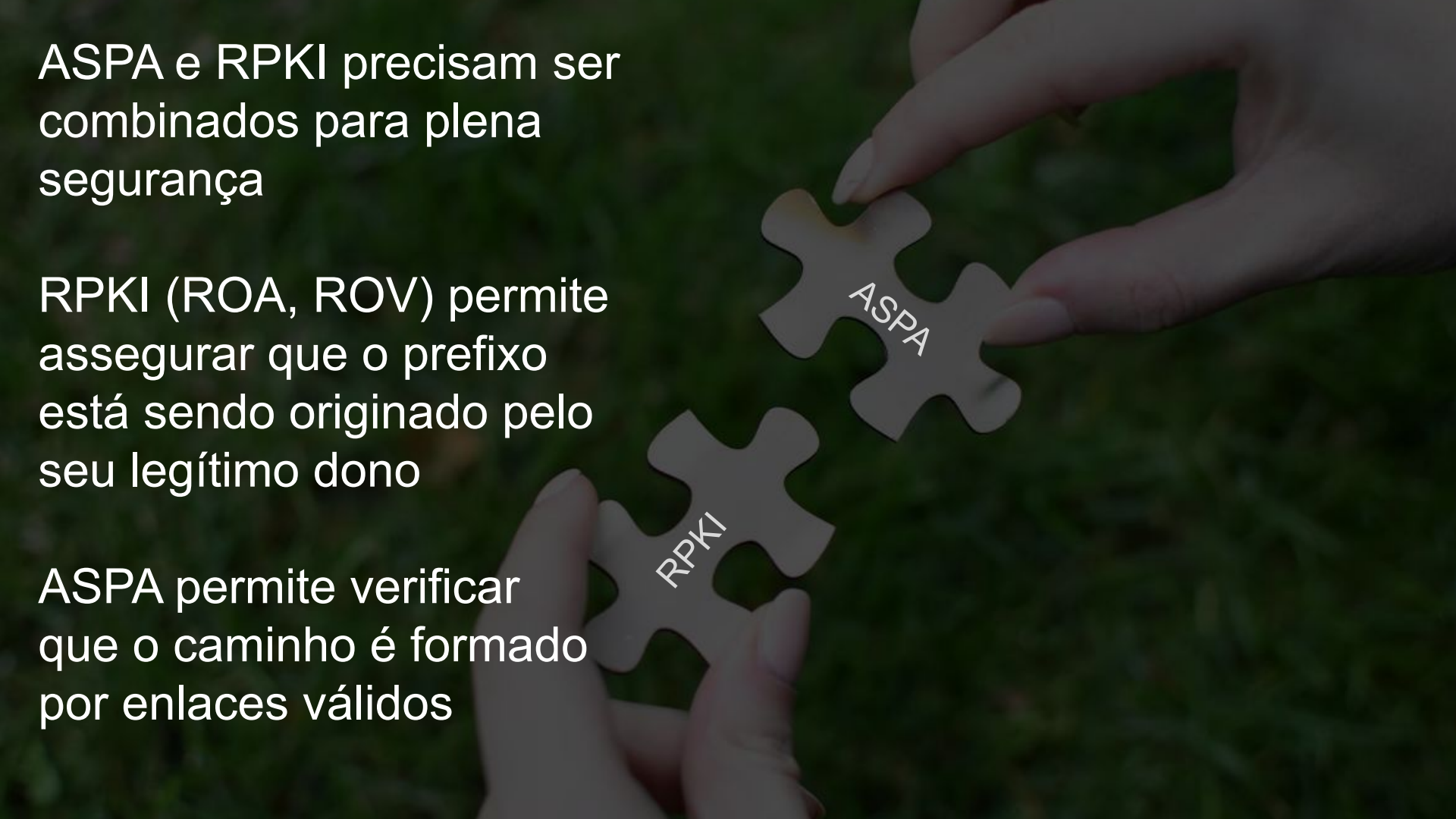
Outros ASes realizam (ou não) a validação



ASPA e RPKI precisam ser combinados para plena segurança

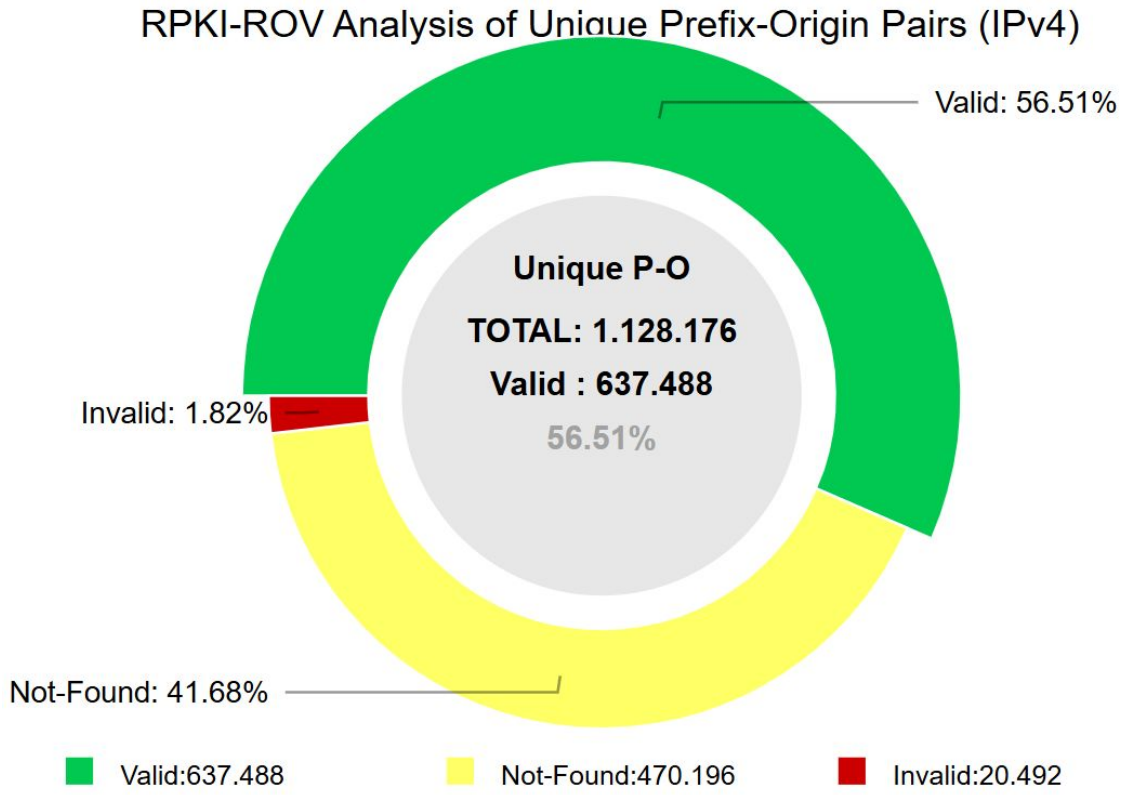
RPKI (ROA, ROV) permite assegurar que o prefixo está sendo originado pelo seu legítimo dono

ASPA permite verificar que o caminho é formado por enlaces válidos

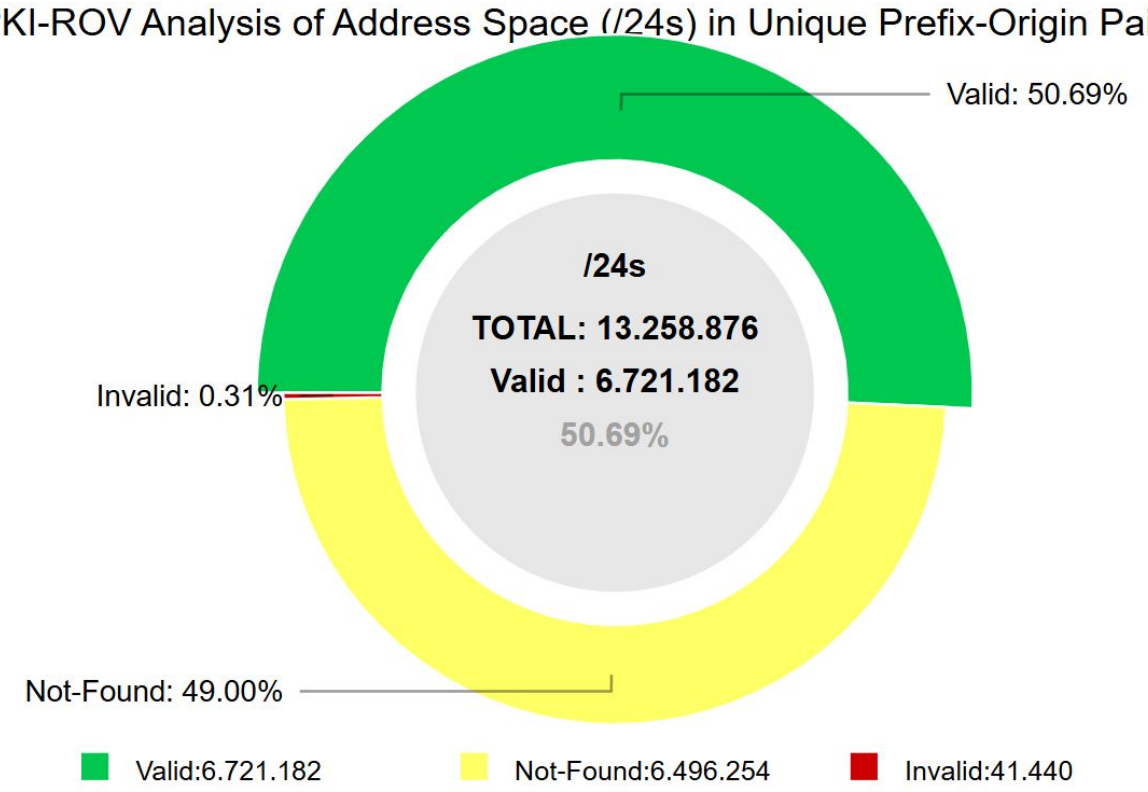


E como anda o processo de criação de objetos ROA e ASPA?

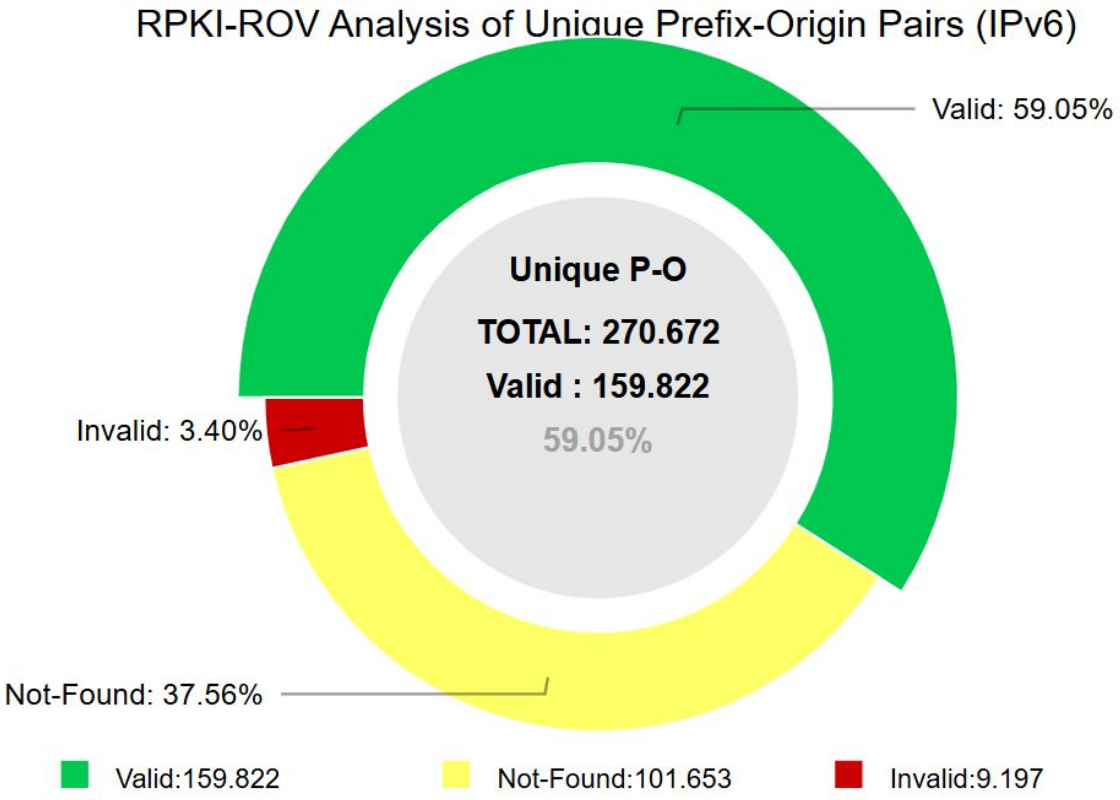
Validação de rotas IPv4 por par prefixo origem



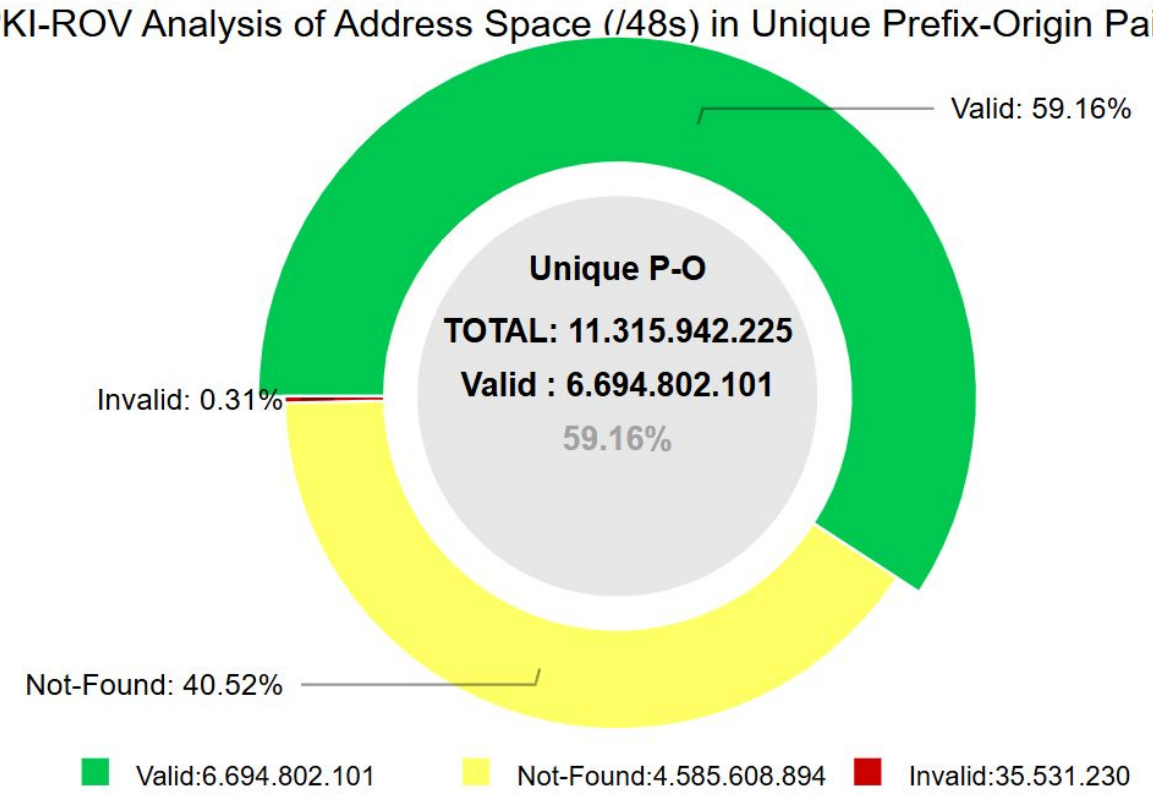
Validação de rotas IPv4 por par prefixo origem (/24)



Validação de rotas IPv6 por par prefixo origem



Validação de rotas IPv6 por par prefixo origem (/48)



E o ASPA? Bem…

No momento da gravação deste vídeo, apenas 86 ASes possuem objetos ASPA criados!

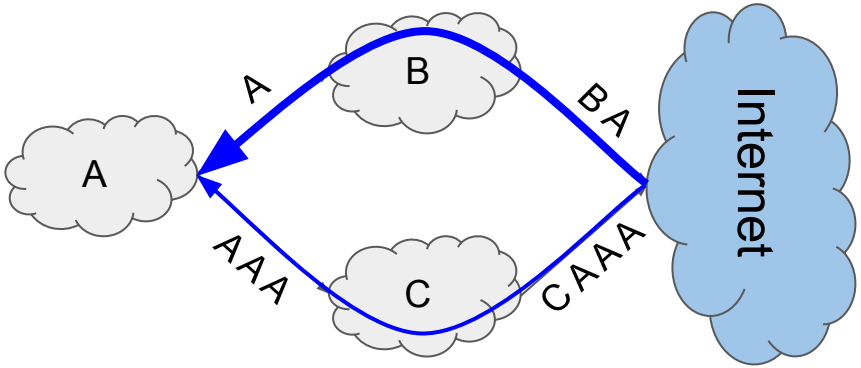
Os esforços de segurança somente terão sucesso se todos comprarem a ideia

Não adianta criar objetos ROA e objetos ASPA se não houver validação desses objetos pelos ASes

Ao validar os objetos estamos protegendo a nós e ao restante da Internet

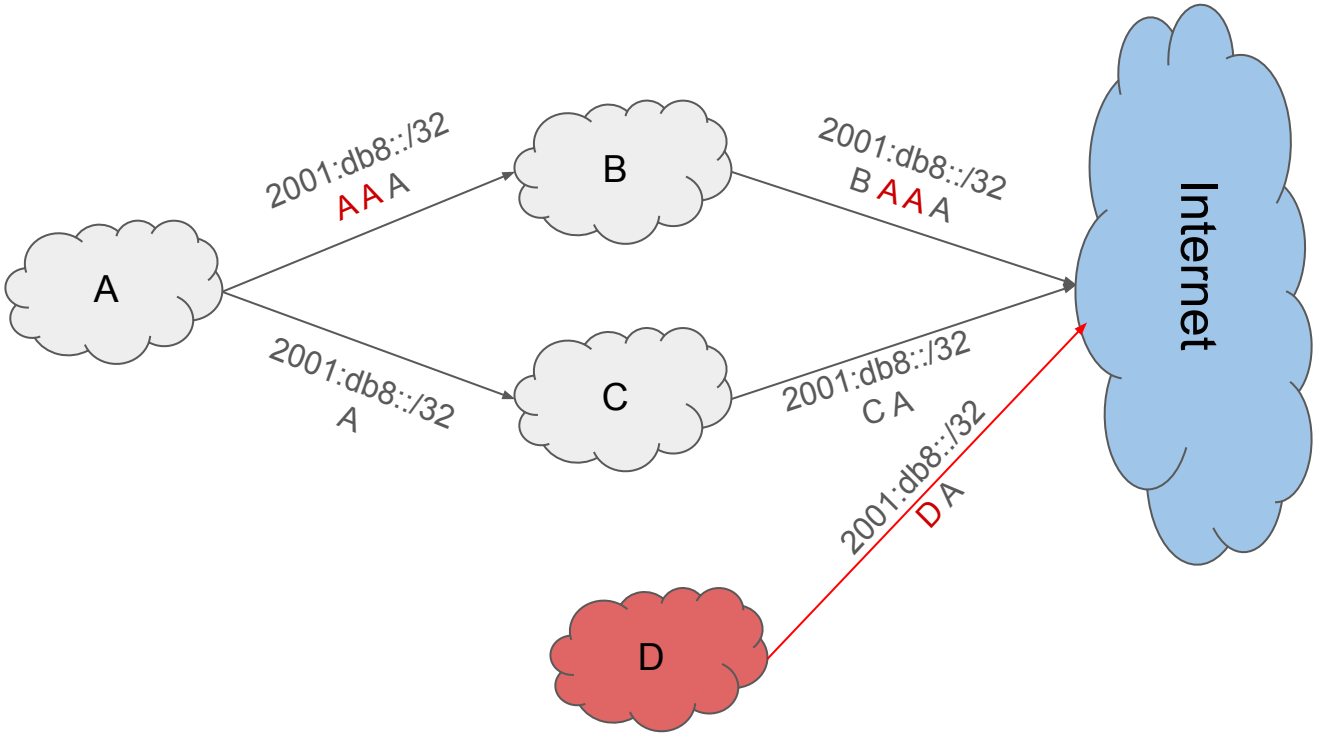
Engenharia de tráfego e riscos de exposição

ASes constantemente realizam engenharia de tráfego através da manipulação dos seus anúncios para reduzir **custos**, eliminar **congestionamentos** ou melhorar **desempenho** da troca de tráfego

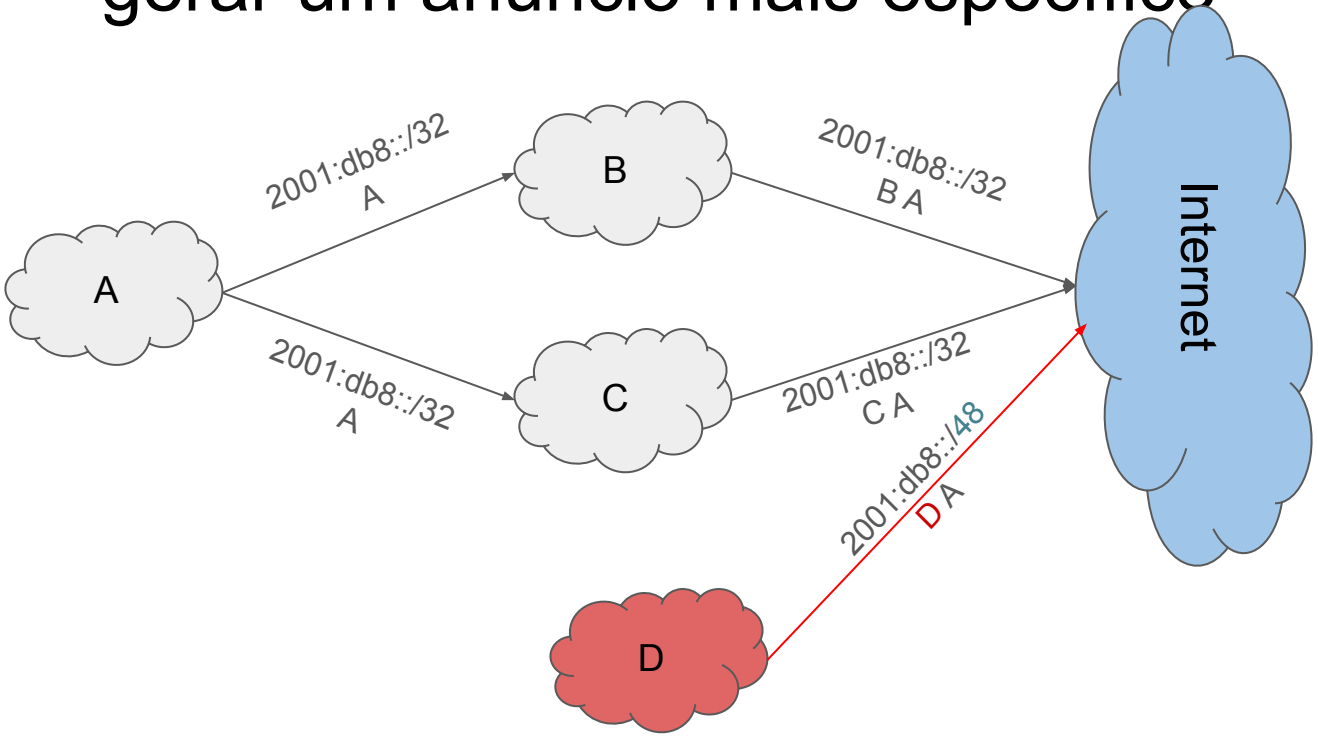


- ASes decidem por qual rota enviar o tráfego
- Buscam influenciar por onde receber o tráfego através de ASPP, anúncios seletivos ou anúncios mais específicos

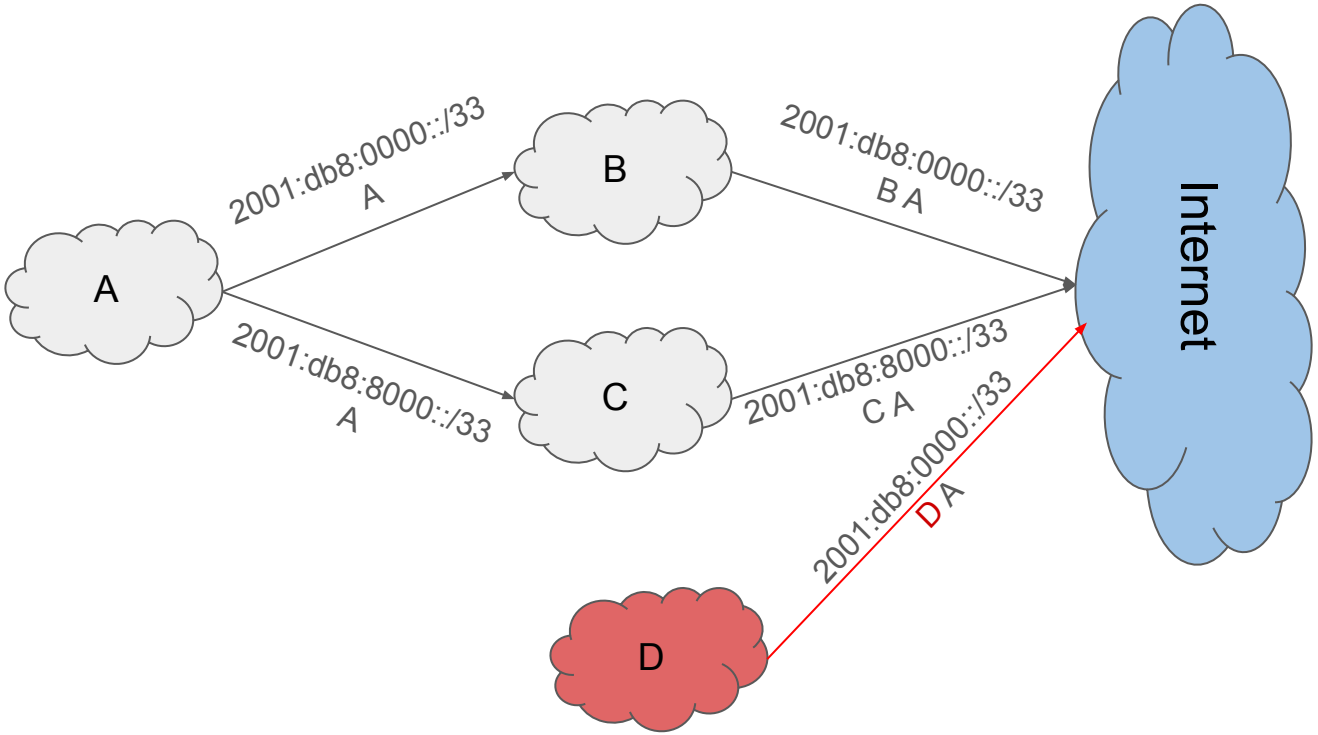
Ao inflar artificialmente o tamanho do caminho com AS-Path prepend aumentamos as chances do atacante ter sucesso no sequestro de prefixo



Prefixos menos específicos tem mais chance de serem sequestrados, uma vez que o atacante pode gerar um anúncio mais específico



Ao restringir a propagação de parte do espaço de endereçamento aumentamos as chances do ataque ter sucesso pela falta de diversidade de rotas



Mostrando na prática o que acabamos de falar!

Sumarizando…

Perguntas?

Pedro Marcos - pbmarcos@furg.br
Renan Barreto - renan.barreto@furg.br

Sequestros de prefixo ainda estão presentes na Internet, a única maneira de evitá-los e combinando o uso de RPKI e ASPA

É fundamental que seja realizada a validação de objetos RPKI e ASPA por todos os ASes e IXPs. Os benefícios são para todos!

Decisões de engenharia de tráfego podem afetar os riscos de você ser vítima de um sequestro de prefixo. Faça engenharia de tráfego, porém, com cuidado. E, por favor, não coloque mais do que dois prepends :)