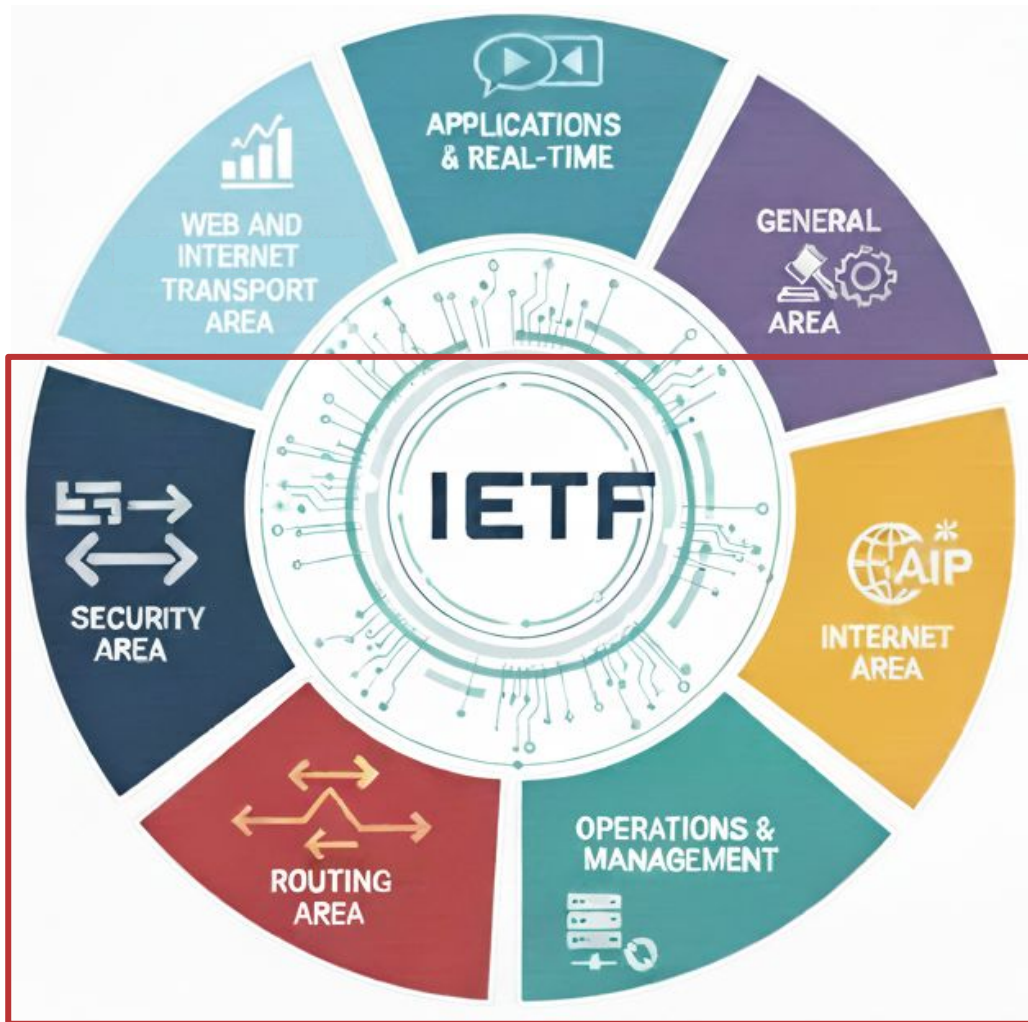


LIVE **INTRAREDE** 2025 — 5 ANOS

Construindo padrões e boas práticas para
engenharia de tráfego, medições de rotas reversas
e transparência do roteamento da Internet

Pedro Marcos, Italo Cunha, Ronaldo Ferreira, Sthefany Duquini

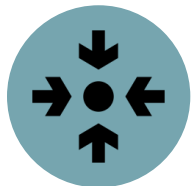


Foco do grupo de pesquisa está alinhado com quatro principais áreas do IETF

Objetivo é a submissão de *drafts* de diferentes tipos



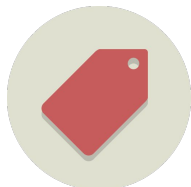
Foco em aspectos fundamentais da operação da Internet



Boas práticas de engenharia de tráfego e peering remoto na Internet



Padronização e suporte de medições de rotas reversas

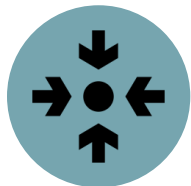


Inferência, validação e padronização de comunidades BGP para engenharia de tráfego e transparência operacional



Monitoramento de adoção e implantação de validação de rotas

Foco em aspectos fundamentais da operação da Internet



Boas práticas de engenharia de tráfego e peering remoto na Internet



Padronização e suporte de medições de rotas reversas



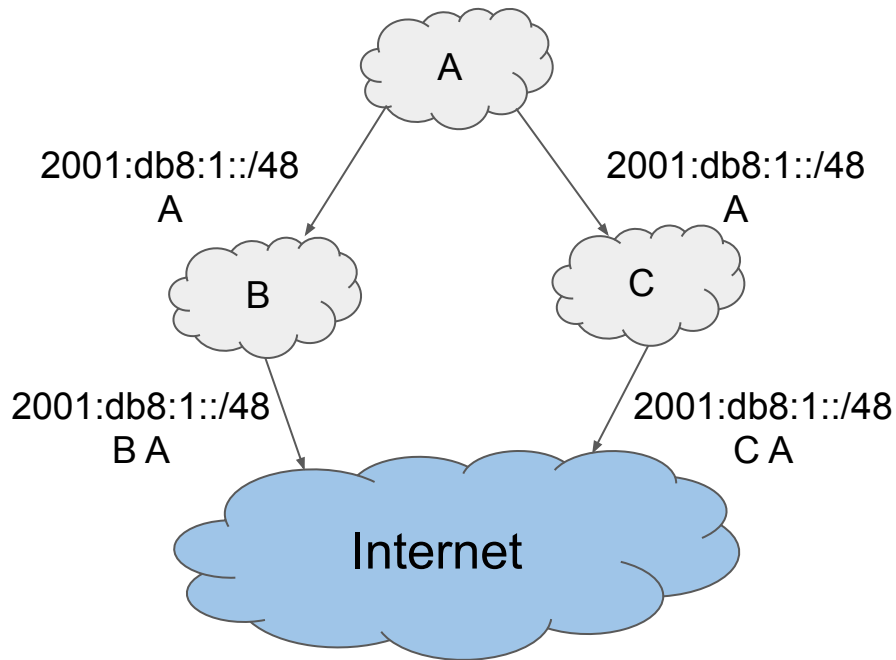
Inferência, validação e padronização de comunidades BGP para engenharia de tráfego e transparência operacional



Monitoramento de adoção e implantação de validação de rotas

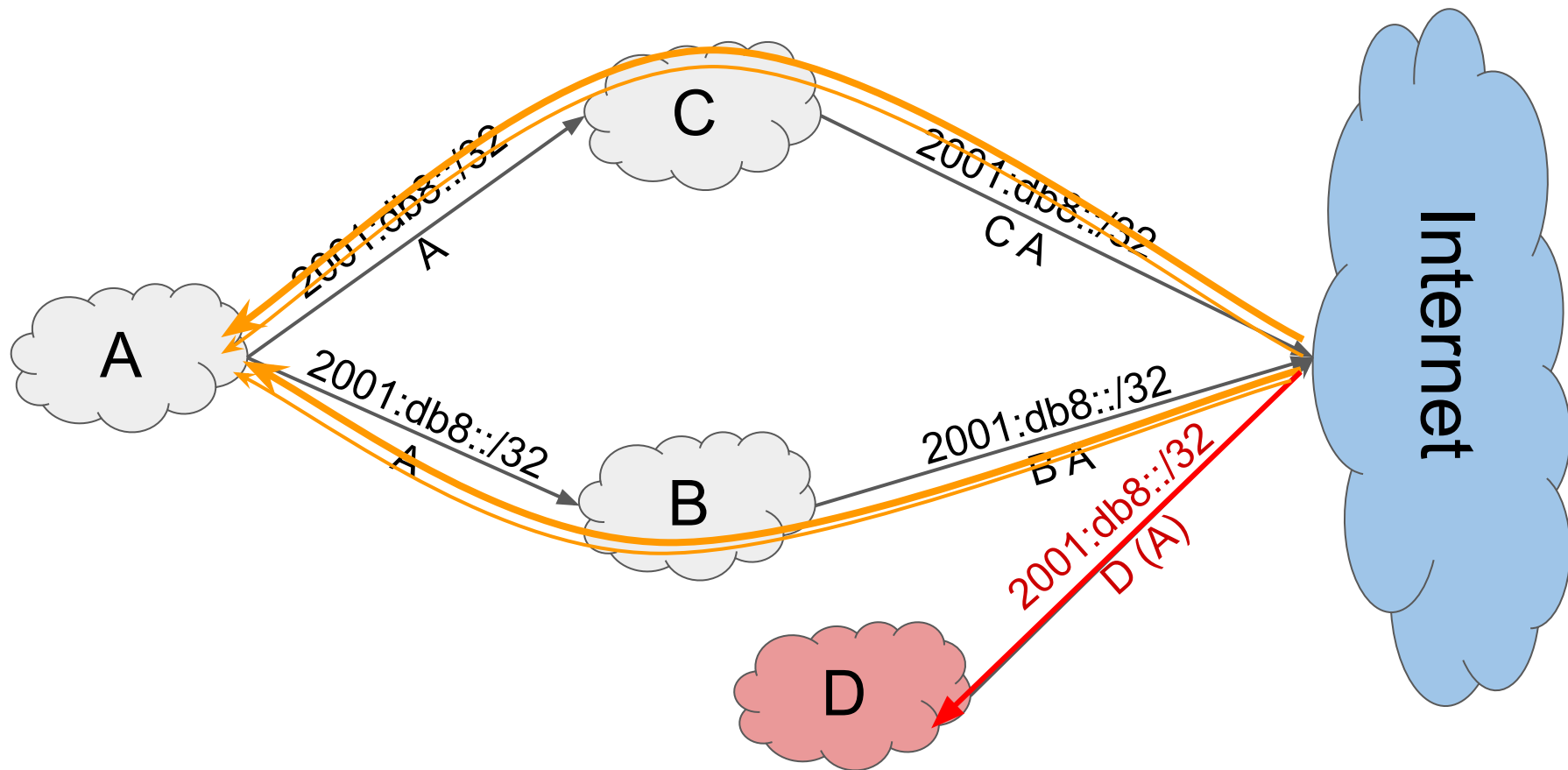
O protocolo **BGP**, a “cola” que une a Internet, **não tem** mecanismos de **segurança** em sua concepção

Critérios para escolha da melhor rota

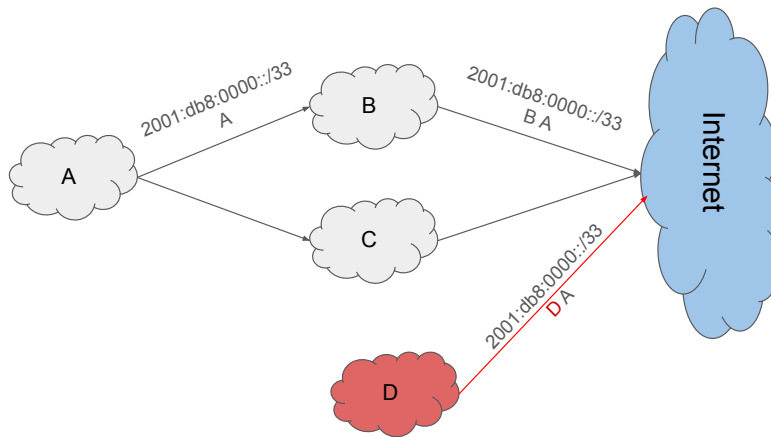
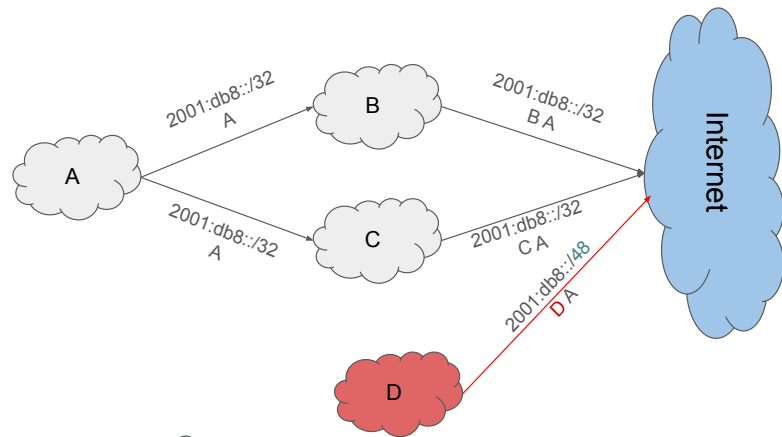
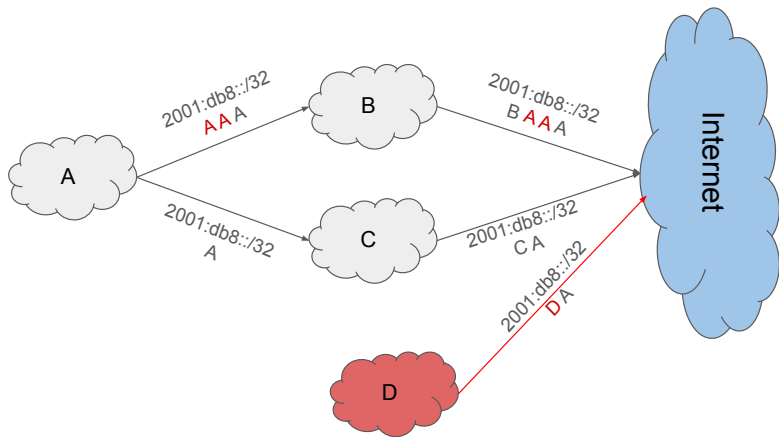


0. Prefixo mais específico (LPM protocolo IP)
1. Preferência local
2. Menor caminho
3. Menor tipo de origem (IGP < EGP < incompleto)
4. Menor MED
5. eBGP sobre iBGP
6. Menor IGP para o próximo hop BGP
7. Rota mais antiga
8. Menor ID do roteador BGP
9. Menor endereço do vizinho

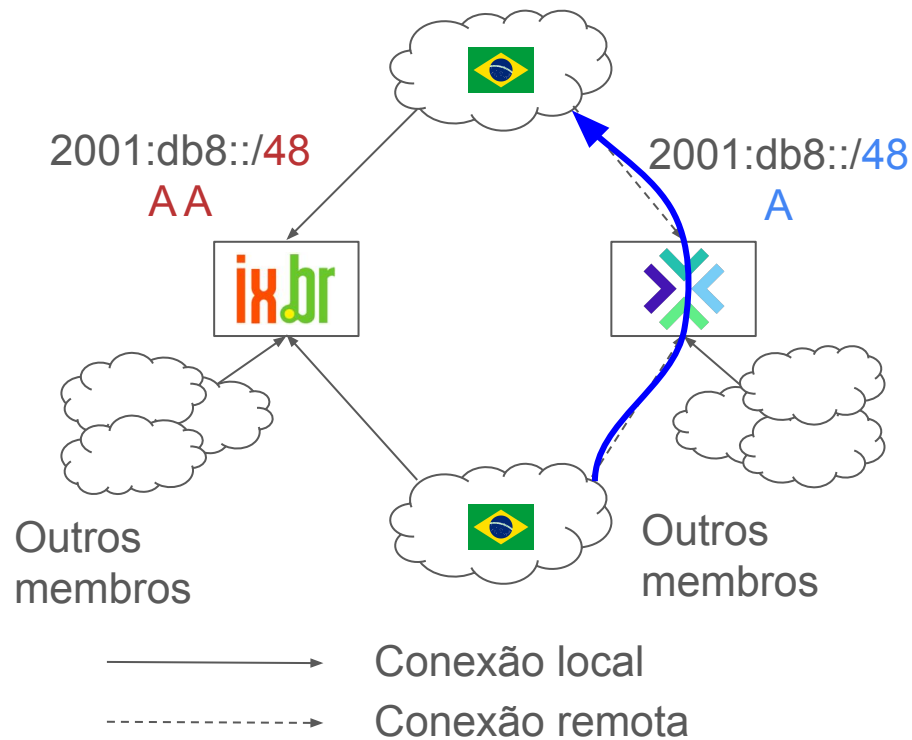
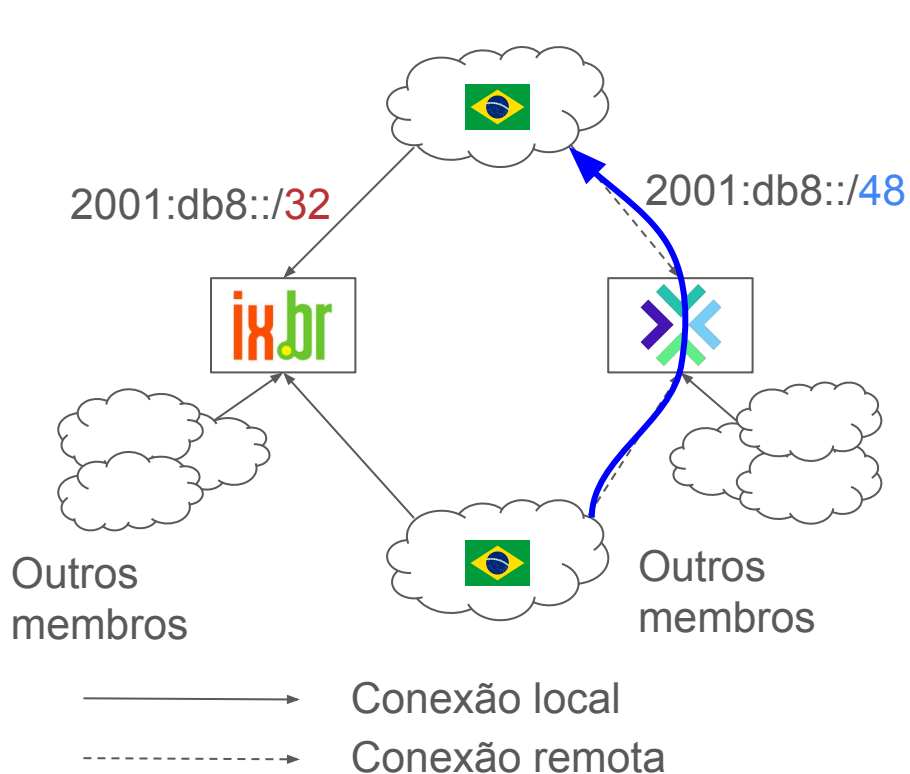
O que é um sequestro de prefixo?



Decisões de engenharia de tráfego influenciam riscos



IXPs surgiram para manter tráfego local, local, porém, *peering* remoto pode “complicar” engenharia de tráfego



Propor boas práticas de engenharia de tráfego para

Segurança e resiliência

- Como fazer engenharia de tráfego de forma **segura e resiliente**?
- Como a escolha da **técnica de engenharia de tráfego** influencia o risco de sofrer um sequestro de prefixo?
- Como a **conectividade** do AS influencia a sua resiliência?

Peering remoto

- Como fazer engenharia de tráfego quando o **AS está remotamente conectado** ao IXP?
- Como fazer engenharia de tráfego quando os **outros ASes estão remotamente conectados** ao IXP?
- Como o **IXP pode auxiliar**?

Foco em aspectos fundamentais da operação da Internet



Boas práticas de engenharia de tráfego e peering remoto na Internet



Padronização e suporte de medições de rotas reversas

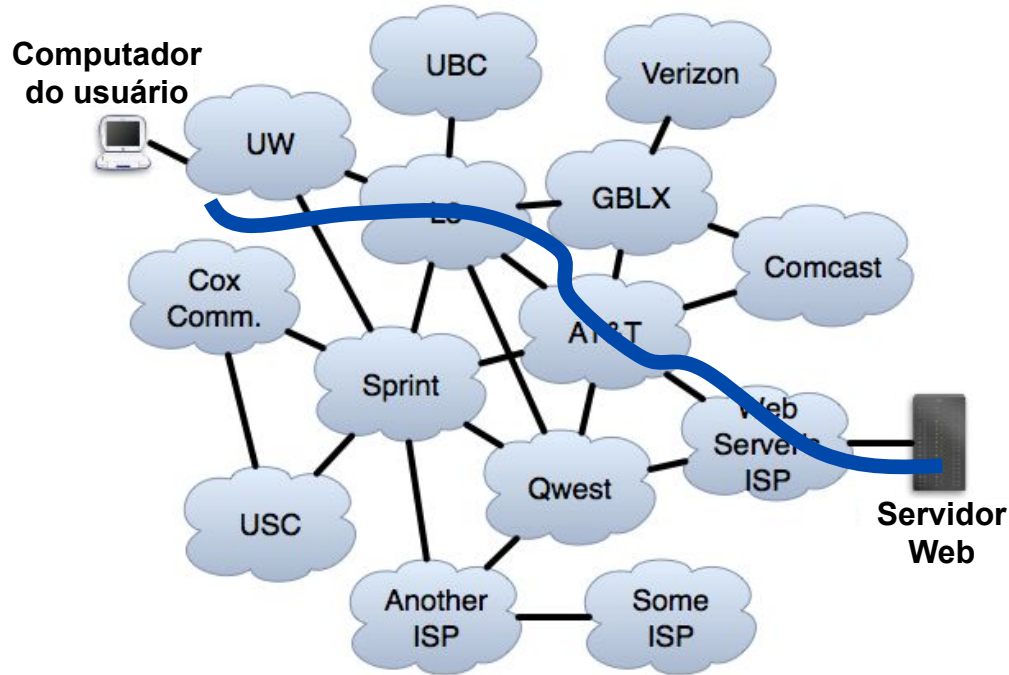


Inferência, validação e padronização de comunidades BGP para engenharia de tráfego e transparência operacional

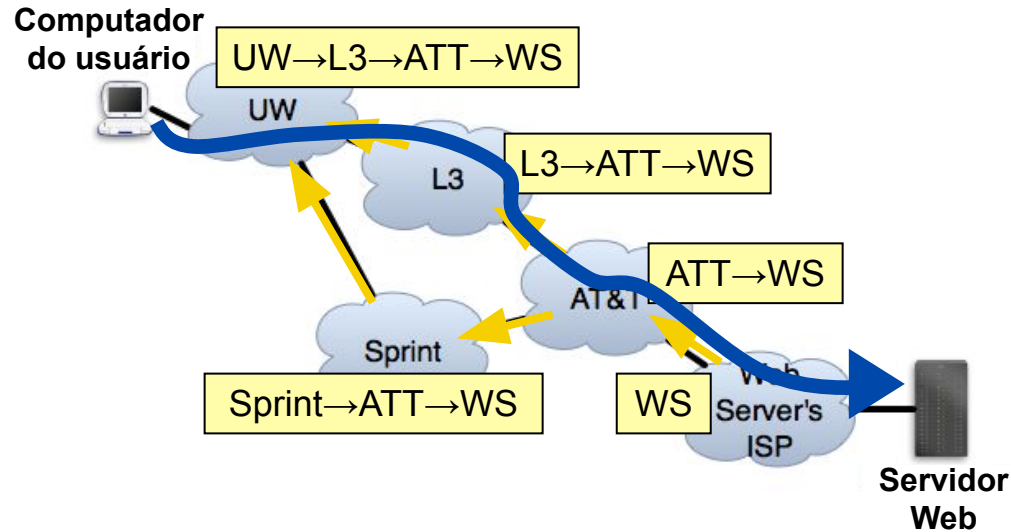


Monitoramento de adoção e implantação de validação de rotas

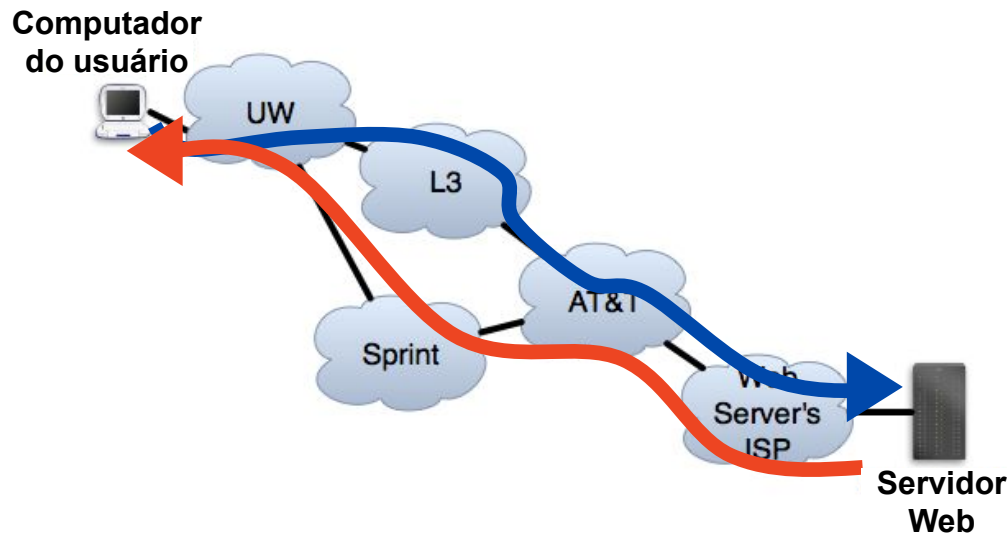
A Internet é uma federação de redes (sistemas autônomos)



Estabelecimento de rotas interdomínio



Caminhos são frequentemente assimétricos

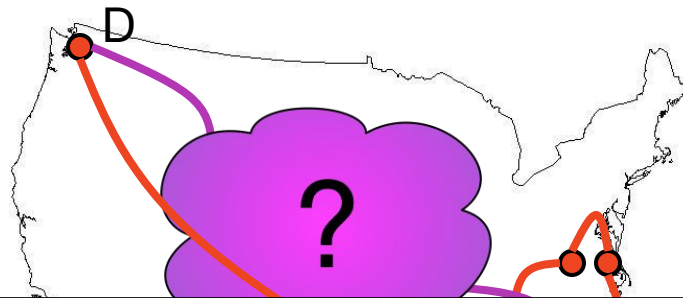


47% dos caminhos são assimétricos na granularidade de provedores, muito mais na granularidade de roteadores

Exemplo de depuração de caminho com baixo desempenho

- Latência de 150ms entre Orlando e Seattle, 3x o esperado
 - Por exemplo, CDN detecta desempenho ruim de usuários
- *Abordagem atual*: Disparar traceroute, verificar se indireto

Hop no.	DNS name / IP address
1	132.170.3.1
2	198.32.155.89
3	JAX-FL... net.flrnet.org
4	ATLANTA ix.cox.com
5	ASH... as.cox.net
6	core2... WDC .pnap.
7	cr1. WDC ...internap.
8	cr2-cr1. WDC ...internap.
9	cr1. MIA ...internap.
10	cr1. SEA ...internap.



*“To more precisely troubleshoot problems, [Google] needs the ability to gather information about **the reverse path** back from clients to Google.”*

- Indireção: Flórida → NY
Mas só explica *metade* do

Artigo do Google no ACM IMC, 2009

Limitações e desafios do Reverse Traceroute

- Roteadores precisam suportar a opção Record Route
 - 55% dos sistemas autônomos suportam

Avaliar o custo em suportar o Record Route e motivar sua configuração a operadores.

- Atualmente só funciona para IPv4

Padronizar suporte para Record Route no IPv6.

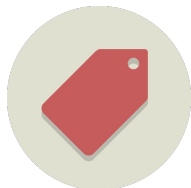
Foco em aspectos fundamentais da operação da Internet



Boas práticas de engenharia de tráfego e peering remoto na Internet



Padronização e suporte de medições de rotas reversas



Inferência, validação e padronização de comunidades BGP para engenharia de tráfego e transparência operacional



Monitoramento de adoção e implantação de validação de rotas

Comunidades BGP são fundamentais para engenharia de tráfego

Network Working Group
Request for Comments: 1997
Category: Standards Track

R. Chandra
P. Traina
Cisco Systems
T. Li
August 1996

BGP Communities Attribute

Status of This Memo

Well-known Communities

This document specifies Internet community, and improvements. Please refer to the Official Protocol Standard and status of this protocol.

The following communities have global significance. Operations shall be implemented in any community speaker.

Abstract

Border Gateway Protocol (BGP) is a protocol designed for Internet routing.

This document describes additional information.

The intention of the protocol is to provide administration and reduce the Internet.

NO_EXPORT (0xFFFFF01)

All routes received carrying a community containing this value MUST NOT be advertised across a confederation boundary (a stand-alone autonomous system is not part of a confederation should be confederation itself).

NO_ADVERTISE (0xFFFFF02)

All routes received carrying a community containing this value MUST NOT be advertised to peers.

NO_EXPORT_SUBCONFED (0xFFFFF03)

All routes received carrying a communities attribute containing this value MUST NOT be advertised to external BGP peers (this includes peers in other members autonomous systems inside a BGP confederation).

Internet Engineering Task Force (IETF)
Request for Comments: 7999
Category: Informational
ISSN: 2070-1721

T. King
C. Dietzel
DE-CIX
J. Snijders
NTT
G. Doering
SpaceNet AG
G. Hankins
Nokia
October 2016

BLACKHOLE Community

Abstract

This document describes the use of a well-known Border Gateway Protocol (BGP) community for destination-based blackholing in IP networks. This well-known advisory transitive BGP community named "BLACKHOLE" allows an origin Autonomous System (AS) to specify that a neighboring network should discard any traffic destined towards the tagged IP prefix.

Porém, a falta de uma padronização dificulta a operação dos ASes e a engenharia de tráfego

Traffic engineering			
function	standard	extended	large
not announce to ASN	65000:dest-asn	(ro rt):65000:dest-asn	65000:0:dest-asn
export only to ASN	65001:dest-asn	(ro rt):65001:dest-asn	65001:0:dest-asn
add one prepend	64601:dest-asn	(ro rt):64601:dest-asn	64601:0:dest-asn
add two prepend	64602:dest-asn	(ro rt):64602:dest-asn	64602:0:dest-asn
add three prepend	64603:dest-asn	(ro rt):64603:dest-asn	64603:0:dest-asn
graceful shutdown	65535:0	-	-
do not announce to Afrinic (ASNs)	65002:0	(ro rt):65002:0	65002:0:0
do not announce to Apnic (ASNs)	65002:1	(ro rt):65002:1	65002:0:1
do not announce to Arin (ASNs)	65002:2	(ro rt):65002:2	65002:0:2
do not announce to Lacnic (ASNs)	65002:3	(ro rt):65002:3	65002:0:3
do not announce to Ripe (ASNs)	65002:4	(ro rt):65002:4	65002:0:4
do not announce to Brasil (ASNs)	65002:5	(ro rt):65002:5	65002:0:5
export to Afrinic (ASNs)	65003:0	(ro rt):65003:0	65003:0:0
export to Apnic (ASNs)	65003:1	(ro rt):65003:1	65003:0:1
export to Arin (ASNs)	65003:2	(ro rt):65003:2	65003:0:2
export to Lacnic (ASNs)	65003:3	(ro rt):65003:3	65003:0:3
export to Ripe (ASNs)	65003:4	(ro rt):65003:4	65003:0:4
export to Brasil (ASNs)	65003:5	(ro rt):65003:5	65003:0:5
do not announce to IXP	65004:65XXX	(ro rt):65004:65XXX	65004:0:65XXX

customer traffic engineering communities - Prepending

65001:0 - prepend once to all peers

65001:XXX - prepend once at peerings to AS XXX

65002:0 - prepend twice to all peers

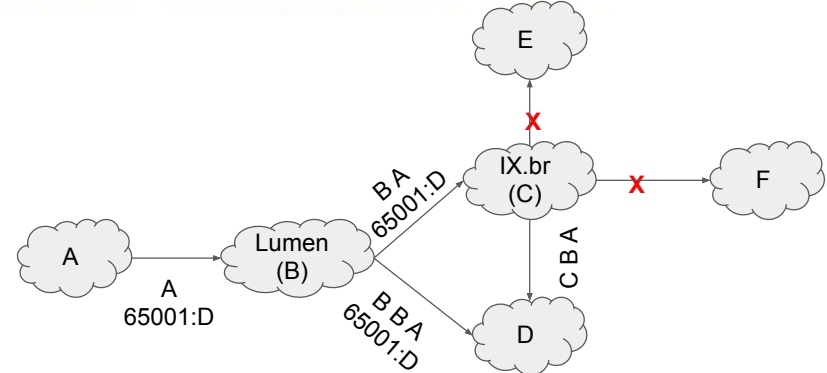
65002:XXX - prepend twice at peerings to AS XXX

65003:0 - prepend 3x to all peers

65003:XXX - prepend 3x at peerings to AS XXX

65004:0 - prepend 4x to all peers

65004:XXX - prepend 4x at peerings to AS XXX



Propor mecanismos para facilitar o uso de comunidades de BGP para engenharia de tráfego

Inferência e validação de semântica

- Como LLMs podem extrair a semântica de comunidades BGP a partir de documentações?
- Como inferir a semântica de comunidades BGP a partir de dados de roteamento?
- Criar base de dados sobre semântica de comunidades BGP

YANG para semântica

- Quais requisitos são necessários para capturar semântica de uma comunidade BGP?
- Como estender RPSL para permitir a especificação da semântica de comunidades BGP?
- Propor extensões ao modelo YANG de comunidades BGP para capturar a semântica

Foco em aspectos fundamentais da operação da Internet



Boas práticas de engenharia de tráfego e peering remoto na Internet



Padronização e suporte de medições de rotas reversas



Inferência, validação e padronização de comunidades BGP para engenharia de tráfego e transparência operacional



Monitoramento de adoção e implantação de validação de rotas

Evolução da Segurança de Roteamento



RPKI

“Quem anuncia?”

Validação da **origem**
Garante a autenticidade do **emissor**



ASPA

“Por onde passou?”

Validação de **caminho**
Garante a integridade da **rota**

ASPA através de um exemplo

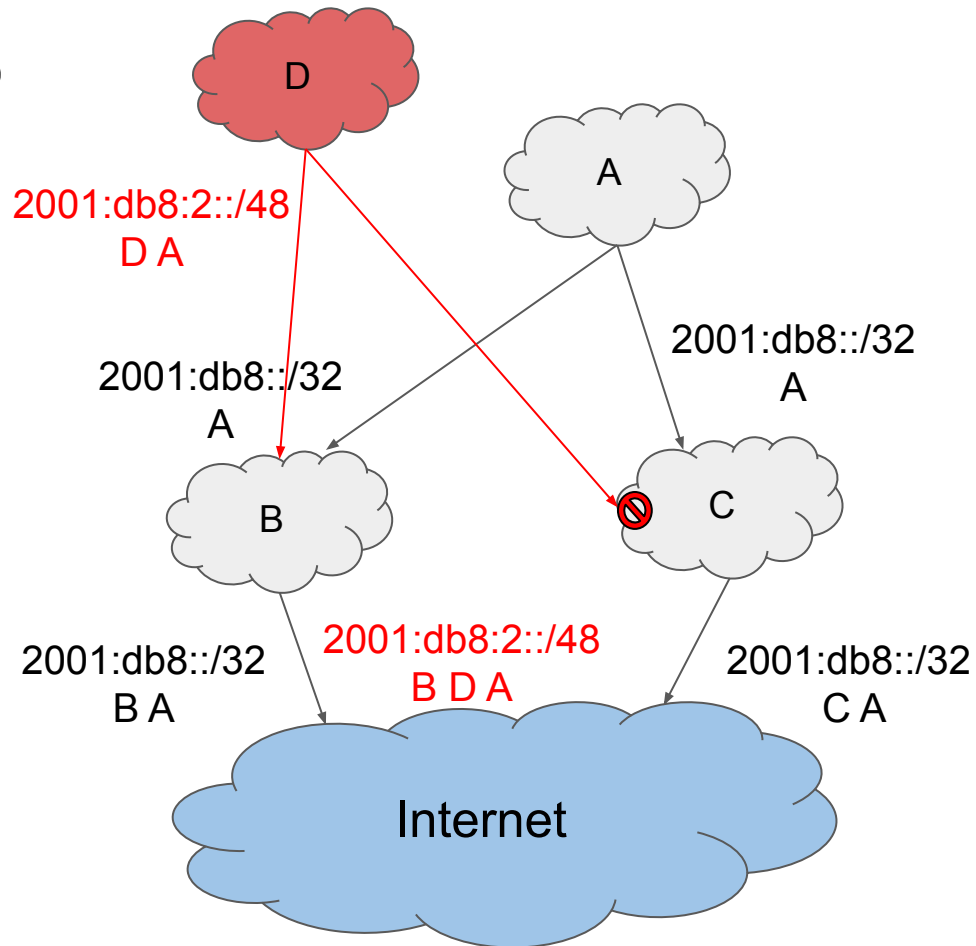
AS A está conectado aos ASes B e C

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



Monitoramento de Adoção

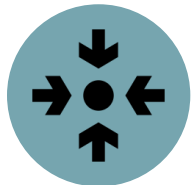
Quais ASes estão adotando ASPA?

- Quem está publicando objetos ASPA?
- Quem está validando: Não basta publicar SPAs, é preciso validar!

Quais as consequências de SPAs desatualizados?

- Rotas legítimas podem ser descartadas devido a erros de configuração.

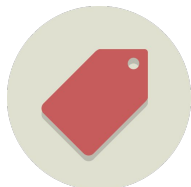
Em resumo...



Propor boas práticas de engenharia de tráfego com foco em segurança e resiliência



Aprimorar e propor mecanismos de medição para permitir um melhor *troubleshooting* de rede



Estabelecer um modelo para especificação de comunidades BGP e desenvolver métodos para inferência de sua semântica



Compreender o uso de mecanismos de segurança para o roteamento da Internet e qualificar suas especificações