Default Route Analytics:
Um Sistema de Monitoramento de Rotas Padrão em Sistemas Autônomos

Pesquisa Tecnológica

Gabriel Alves Reis
Orientador: Prof. Ítalo Cunha

11 de dezembro de 2025

1 Introdução

A Internet é uma rede global responsável pela troca de dados entre processos, sendo o meio pelo qual diversas aplicações de uso cotidiano são disponibilizadas para usuários. Sua arquitetura é composta por uma rede de redes, denominadas Sistemas Autônomos (ASes), interconectadas para viabilizar a comunicação de dados em escala mundial. Quando um usuário envia um pacote, este percorre múltiplos ASes até alcançar seu destino, e uma resposta é retransmitida pela mesma cadeia.

Para garantir o roteamento eficiente, os ASes dependem de protocolos como o Border Gateway Protocol (BGP), que determina os caminhos mais adequados para a transmissão entre sistemas autônomos. O BGP mantém uma tabela dinâmica de rotas, atualizada constantemente com informações de acessibilidade e preferência de caminhos. No entanto, quando um AS recebe um pacote destinado a um prefixo IP não listado em sua tabela BGP, ele pode adotar duas abordagens: descartar o pacote ou recorrer ao uso de rotas padrão, encaminhando o pacote para um AS arbitrário na expectativa de que este o entregue corretamente.

Embora o uso de rotas padrão assegure a conectividade em alguns cenários de falhas ou rotas ausentes, seu uso no roteamento inter-domínio de pacotes viola princípios fundamentais da internet, como controle, transparência e responsabilidade [1]. No entanto, sua utilidade operacional introduz uma série de vulnerablidades para a infraestrutura da Internet. O principal problema reside na natureza manual de sua configuração, que frequentemente não acompanha a dinâmica das mudanças de topologia de rede. Quando um AS depende exclusivamente de rotas padrão, cria-se um ponto único de falha. Caso o roteador de saída padrão apresente problemas, todo o tráfego para destinos desconhecidos é imediatamente impactado, sem mecanismos automáticos de correção de falhas.

Além dos impactos na dependabilidade, o uso indiscriminado de rotas padrão compromete a eficiência do roteamento. Pacotes podem ser encaminhados por caminhos subóptimos, aumentando latência e consumo de recursos em enlaces desnecessários.

Este trabalho visa desenvolver um MVP de um sistema web que permite operadores de redes e pesquisadores da área pesquisarem e analisarem ASes que utilizam da política de roteamento padrão.

1.1 Objetivos Gerais e Específicos

O objetivo geral deste trabalho é fornecer uma plataforma de análise de uso de rota padrão por Sistemas Autônomos para pesquisadores e administradores de rede, que permita embasar decisões técnicas para mitigar riscos e promover rotas mais confiáveis. Ao centralizar e tornar públicos esses dados, a plataforma busca contribuir para uma infraestrutura de internet mais segura, transparente e alinhada aos princípios de responsabilidade do roteamento inter-domínio[1].

2 Referencial Teórico

Esta seção apresenta os conceitos fundamentais que embasam o desenvolvimento deste trabalho, estruturados da seguinte forma: a Seção 2.1 descreve o Border Gateway Protocol (BGP), detalhando seu papel essencial como protocolo de roteamento entre Sistemas Autônomos. Em seguida, a Seção 2.2 introduz a ferramenta de diagnóstico traceroute, cujo funcionamento é a base para a detecção de rotas padrão. Por fim, a Seção 2.3 apresenta o método de detecção por meio de prefixos não anunciados, explicando como sondagens traceroute podem identificar o uso de rotas padrão por um AS. Juntas, essas seções fornecem a base teórica e metodológica necessária para compreender o problema e a solução propostos.

2.1 Border Gateway Protocol

O BGP é o principal protocolo de roteamento que mantém a Internet conectada, permitindo a troca de informações de alcançabilidade entre ASes, ou seja, o BGP foi projetado para gerenciar o roteamento entre domínios administrativos distintos, garantindo que os pacotes trafeguem de forma eficiente através de múltiplas redes interconectadas.

Este protocolo funciona como um sistema de anúncios e decisões entre roteadores de borda (BGP peers). Cada AS anuncia aos seus vizinhos os prefixos de rede que possui, quando um roteador BGP recebe múltiplos anúncios para o mesmo destino, ele executa um algoritmo de seleção de rotas para escolher a melhor rota entre as demais.

Uma vez selecionada a melhor rota, o roteador a armazena em sua tabela de roteamento e a propaga para seus peers.

No entanto, quando um AS não possui uma entrada específica para um determinado prefixo na tabela BGP, ele pode recorrer a rota padrão, encaminhando o tráfego para um gateway genérico na esperança de que algum AS subsequente saiba como lidar com o pacote. Essa abordagem, embora útil para manter a conectividade em casos de falhas ou rotas ausentes, introduz desafios significativos em termos de eficiência, segurança e controle.

2.2 Traceroute

O traceroute é uma ferramenta essencial para diagnóstico de redes que revela o caminho percorrido por pacotes através da Internet. Seu funcionamento baseia-se no campo Time-to-Live (TTL) presente no cabeçalho de todo pacote IP. O TTL é um valor numérico que é decrementado a cada roteador por onde o pacote passa. Quando este valor atinge zero, o roteador descarta o pacote e envia uma mensagem de erro ICMP de volta ao remetente, indicando que o tempo de vida do pacote expirou naquele ponto específico da rede.

O traceroute aproveita esse comportamento de forma inteligente. Ele inicia enviando um primeiro pacote com TTL igual a 1, que será descartado pelo primeiro roteador no caminho, gerando uma mensagem de erro que revela o endereço desse roteador. Em seguida, envia um segundo pacote com TTL igual a 2, que chegará até o segundo roteador antes de expirar. Esse processo se repete sucessivamente, com o TTL sendo incrementado a cada nova tentativa, até que um dos pacotes finalmente atinja o destino final. Cada resposta recebida dos roteadores intermediários permite construir progressivamente o mapa completo do caminho percorrido desde a origem até o destino, mostrando todos os pontos de passagem e os tempos de resposta de cada salto na rede.

2.3 Detecção de rotas padrão utilizando prefixo não anunciado

O método utilizado para identificar a presença de rotas padrão em ASes baseia-se no princípio de que um AS só encaminhará pacotes para um destino não anunciado em sua tabela BGP se possuir uma rota padrão configurada. Essa abordagem, proposta por Randy Bush et al.[2], consiste em executar traceroute a partir do AS sob teste para um endereço IP pertencente a um prefixo não anunciado globalmente.

Se o *traceroute* revelar a existência de roteadores fora do AS testado, isso indica que o pacote foi encaminhado via rota padrão. Caso contrário, se o pacote for descartado, conclui-se que o AS não utiliza rota padrão para aquele destino.

Essa metodologia, também adotada pela ferramenta desenvolvida no artigo base deste trabalho [3], que permite classificar se um AS recorre a rotas padrão.

3 Metodologia

O sistema é composto por três módulos: ripe-atlas-measures, ferramenta responsável por gerar medições de traceroute e realizar a inferência do uso de rotas padrão; web-server, servidor web que disponibiliza rotas HTTP para acesso aos dados gerados pelo módulo ripe-atlas-measures; e web-client, cliente web responsável por disponibilizar uma interface intuitiva que permite uma busca fácil e eficiente por ASes que utilizam ou não a política de roteamento padrão. Toda a documentação técnica sobre como executar o sistema encontra-se no repositório GitHub deste trabalho [4].

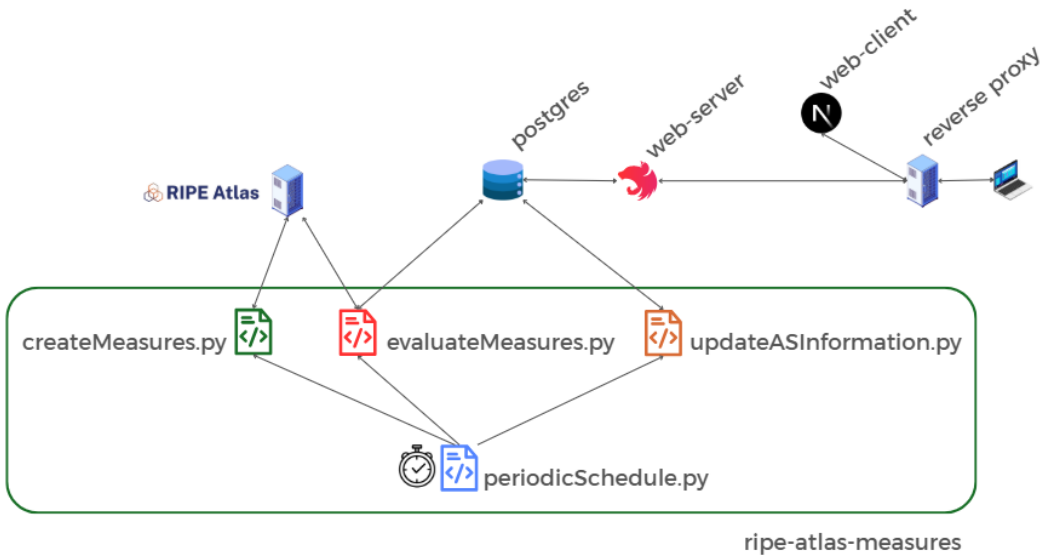

Figura 1: Diagrama da arquitetura do sistema.

3.1 Ripe Atlas Measures

Este módulo é responsável por gerar os dados de uso de rota padrão utilizados na plataforma. Para isso, foi utilizada como base a ferramenta implementada no artigo [5].

O módulo ripe-atlas-measures contém 4 scripts principais: createMeasures.py, evaluateMeasures.py, updateASInformation.py e periodicSchedule.py.

O periodicSchedule.py é responsável por executar os outros 3 scripts a cada 7 dias. Isso garante que o sistema se mantenha sempre atualizado e com dados que representam como o AS se comporta no presente.

O script createMeasures.py, primeiro na lista de execução, é responsável por listar todos os probes da plataforma RIPE Atlas e gerar medições de traceroute de cada probe para um prefixo não anunciado globalmente (detalhes na seção 2.3).

O segundo script na lista de execução é o evaluateMeasures.py, responsável por observar as medições de traceroute que foram geradas no script anterior utilizando uma estratégia de pooling. Quando uma medição é completada, os resultados são carregados e uma variação do algoritmo de detecção de rota padrão (seção 2.3) é executada. Nesta variação, ao invés de detectar rota padrão ao verificar a existência de um roteador fora do AS, modificamos para detectar ao verificar pelo menos 2 roteadores fora do AS testado. Ao finalizar, os resultados são salvos no banco de dados para consumo do próximo script.

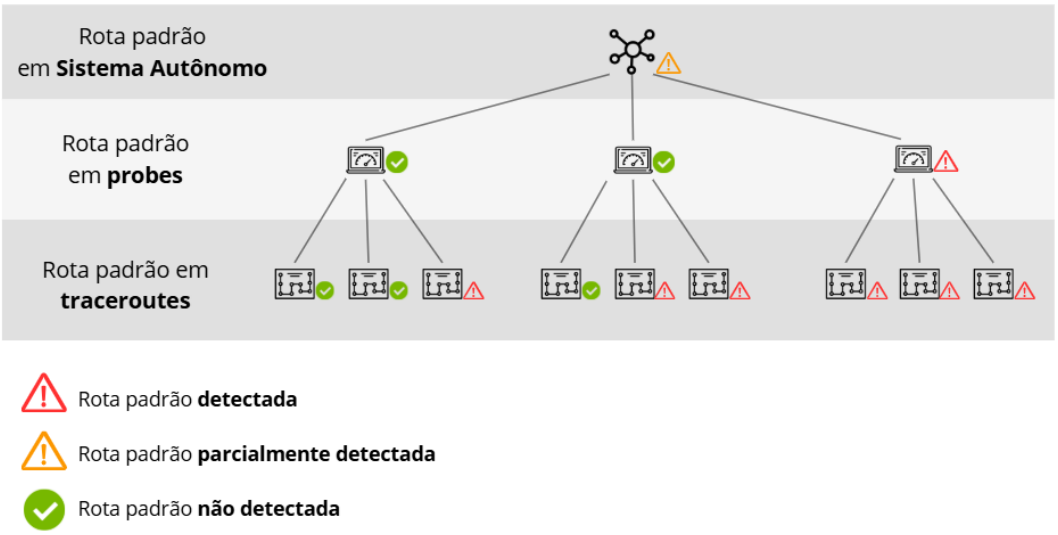

Figura 2: Esquema hierárquico de detecção de rota padrão

Por fim, o último script deste fluxo é o updateASInformation.py, responsável por gerar a classificação de uso de rota padrão para o AS, utilizando um esquema hierárquico para esta rotulação.

Um probe (ou sonda) terá rota padrão se as últimas 3 medições de traceroute realizadas a partir dele tiverem rota padrão. Já um AS terá o status "Detected"se todos os seus probes tiverem rota padrão, "Not Detected"se nenhum de seus probes tiver rota padrão e "Partial Detected"se apenas alguns probes forem classificados com rota padrão, mas não todos.

3.2 Back-end

O módulo web-server, back-end desta aplicação, é desenvolvido em Nest.js [6]. Sua principal responsabilidade é prover rotas HTTP para consulta dos dados de maneira eficiente, utilizando estratégias de paginação e filtros para disponibilizar esses dados da melhor forma. Atualmente, o único módulo que o utiliza é o web-client; no entanto, é possível acessar essas rotas utilizando qualquer aplicação que faça requisições HTTP.

3.3 Proxy Reverso

A arquitetura proposta prevê que o Nginx atue como intermediário entre os clientes e os serviços da aplicação, redirecionando as requisições para os respectivos módulos (front-end e back-end) conforme as regras de roteamento definidas. Esta abordagem permite ocultar a estrutura interna da aplicação, fornecer uma camada adicional de segurança através de SSL/TLS, além de possibilitar otimizações como compressão de conteúdo e balanceamento de carga, se necessário no futuro.

3.4 Front-end

O módulo *web-client* foi desenvolvido utilizando a biblioteca React [7]. Sua principal responsabilidade é prover uma interface de usuário amigável e intuitiva para gestores de redes e

pesquisadores interessados em analisar o uso de rota padrão em um dado sistema autônomo.

A Figura 3 apresenta a página inicial do sistema, que permite a visualização geral de todos os ASes monitorados com seus respectivos status de rota padrão, além de funcionalidades de busca e filtragem. A Figura 4 mostra a página de detalhes de um AS específico, onde são exibidas informações detalhadas sobre seus *probes*, medições e a classificação de uso de rota padrão.

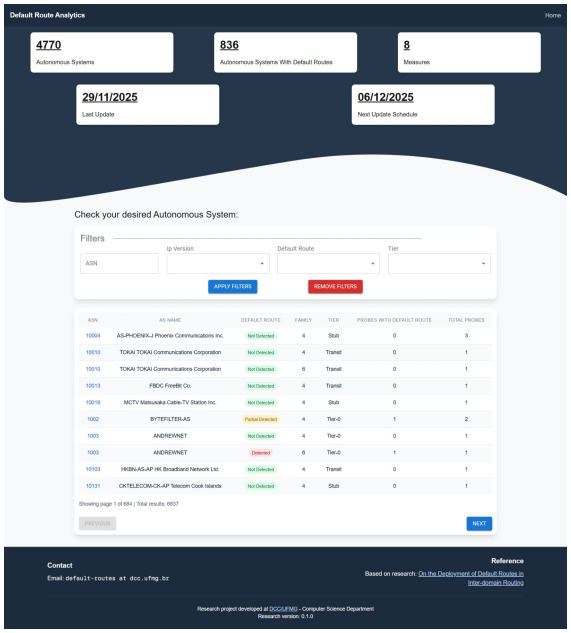

Figura 3: Página inicial do sistema.

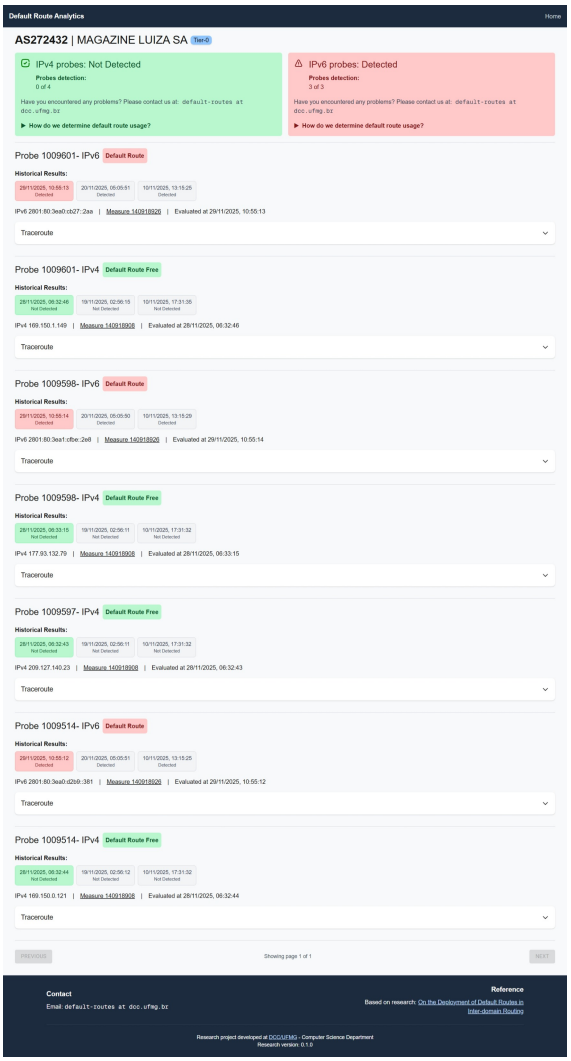

Figura 4: Página de detalhes de um AS.

4 Limitações e Melhorias Futuras

O MVP desenvolvido neste trabalho possui algumas limitações e pontos que são oportunidades claras para torná o sistema mais robusto e útil.

Uma limitação prática é que hoje coletamos dados apenas da plataforma RIPE Atlas. Para ter uma visão mais completa e diversa, seria interessante também integrar medições de outras redes, como o NLNOG Ring [8]. Essa expansão aumentaria nossa cobertura de

probes, especialmente em regiões onde o RIPE Atlas tem menos presença, e nos daria mais confiança nas classificações de rota padrão que geramos.

Para que os dados do sistema sejam mais facilmente aproveitados por outros projetos, é ideal criar SDKs em linguagens amplamente utilizadas (e.g. TypeScript e Python). Isso permitiria que desenvolvedores e pesquisadores integrem nossas métricas diretamente em suas próprias ferramentas e scripts, sem precisar interagir manualmente com a API.

No aspecto operacional, duas melhorias são prioritárias: containerizar toda a aplicação com Docker e implementar um pipeline de CI/CD. Com a containerização, o deploy ficará mais simples e consistente. Já o pipeline de CI/CD vai garantir que todo código seja automaticamente validado antes de ser aprovado e mergeado na branch main. Isso evita que alterações problemáticas entrem no código principal e aumenta a confiança no processo de desenvolvimento.

5 Resultados

Após a execução de oito ciclos de medição, realizados em intervalos regulares de sete dias, foi possível identificar um total de 836 Sistemas Autônomos (ASes) que empregam rotas padrão como política de roteamento. Esta amostra foi extraída de um conjunto de 4.770 ASes analizados, o que representa uma prevalência de aproximadamente 17.5% na utilização desse mecanismo para o encaminhamento de tráfego destinado a prefixos IP não anunciados em suas tabelas de roteamento BGP.

Além disso, assim como utilizado no artigo base deste trabalho [3] utilizamos o CAIDA AS relationship dataset [9] para mapear ASes e tiers. O Tier-1 são ASes que têm conectividade global e que não precisam comprar conectividade de outros ASes. Tier-2 (Trânsito) são ASes que estabelecem peering gratuito com alguns ASes, mas necessitam comprar trânsito de outros para alcançar todas as porções da Internet. Tier-3 (Borda) são ASes de redes stub que dependem exclusivamente da compra de conectividade de outros ASes para obter acesso à Internet. Tier-0 (Desconhecido) são aqueles que não foi possível realizar o mapeamento pelo dataset CAIDA (consideramos como stub).

Tabela 1: Resultados de detecção de rota padrão por tier de AS

	IPv4				**IPv6**			
Tier	**Total**	**Detec.**	**Não Detec.**	**Parcial**	**Total**	**Detec.**	**Não Detec.**	**Parcial**
Tier-1	11	0	8	3	10	0	8	2
Trânsito	1.971	149	1.732	90	1.006	87	870	49
Borda	1.897	336	1.515	46	737	128	589	20
Desconhecido	699	144	518	37	506	121	356	29
Total	**4.578**	**629**	**3.773**	**176**	**2.259**	**336**	**1.823**	**100**

Analisando a tabela acima percebe-se que nenhum AS de Tier-1 adotou a rota padrão como política de roteamento. Paralelamente, chama atenção a prevalência da prática nos ASes de borda, que lideram as detecções com 336 casos em IPv4.

Outra análise realizada focou na presença de rotas padrão em Sistemas Autônomos que não são stubs. Dentre os 4.770 ASes analisados, 2.009 foram classificados como não stubs

(i.e. Tier-1 e Trânsito), dentre esses, apenas 201 apresentaram rota padrão, o que corresponde a uma prevalência de 10% do uso dessa política em ASes não stubs.

Além disso, ao analisar todos os 16.763 traceroutes com rota padrão gerados ao longo de oito ciclos de medição, observa-se uma preferência por ASes de trânsito como destino final da rota padrão. Do total, 11.844 traceroutes alcançaram um AS de trânsito, enquanto 1.857 alcançaram ASes de Tier desconhecido, 1.785 alcançaram Tier-1 e 1.277 alcançaram AS de borda.

Em resumo, os resultados obtidos demonstraram a ocorrência do uso de rotas padrão em uma parcela significativa dos Sistemas Autônomos analisados, com uma prevalência observada de aproximadamente 17,5%. A distribuição desse comportamento variou entre os diferentes tiers de ASes, sendo mais frequente em redes de borda e ausente nos ASes Tier-1. Além disso, a análise dos traceroutes revelou que, quando a rota padrão é empregada, ASes de trânsito atua como o principal destino final para o tráfego.

6 Conclusão

O desenvolvimento deste trabalho resultou em uma aplicação web para monitoramento do uso de rotas padrão no roteamento interdomínio de pacotes. O objetivo desta plataforma é servir como base para operadores de rede e pesquisadores que buscam realizar análises sobre a adoção dessa prática de roteamento em ASes.

Do ponto de vista teórico, o desenvolvimento desta ferramenta proporcionou um melhor entendimento acerca do protocolo BGP e da lógica de roteamento de pacotes, especialmente sobre as implicações operacionais do uso de rotas padrão. Este processo foi marcado por alguns desafios, particularmente na integração com a API do RIPE Atlas, que exigiu a criação de mecanismos robustos para lidar com suas limitações, como a assincronia das medições e a necessidade de pooling eficiente para coleta de dados. Além disso, um dos grandes desafios e aprendizados deste projeto foi organizar a arquitetura do sistema visando separar as responsabilidades entre os módulos e fazer com que estes interajam entre si com harmonia, desde a geração do traceroute, passando pela inferência hierárquica de rota padrão até a disponibilização dos dados no front-end.

Os potenciais impactos deste trabalho estão alinhados à promoção de uma Internet mais responsável. Ao monitorar e expor uma prática que compromete o princípio da responsabilidade no roteamento, a ferramenta contribui para aumentar a transparência sobre a configuração das redes. A longo prazo, a disponibilização contínua desses dados pode incentivar operadores a revisarem suas configurações, reduzindo pontos únicos de falha e roteamentos subótimos. Assim, este projeto apoia a evolução da Internet em direção a uma infraestrutura mais segura, eficiente e confiável.

Referências

[1] Ralph Holz Fernando Kuipers Janet Hui Xue Mattijs Jonker Joeri de Ruiter Anna Sperotto Roland van Rijswijk-Deij Giovane CM Moura et al Cristian Hesselman, Paola Grosso. A responsible internet to increase trust in the digital world. In *Journal of Network and Systems Management*, 2020.

[2] R. Bush, O. Maennel, M. Roughan, and S. Uhlig. Internet Optometry: Assessing the Broken Glasses in Internet Reachability. 2009.

[3] I. Cunha R. Bush E. Katz-Bassett G. D.Rodosek et al. N. Rodday, L. Kaltenbach. On the deployment of default routes in inter-domainrouting. In *Proceedings of the ACM Sigcomm 2021 Workshop on Technol-ogies, Applications, and Uses of a Responsible Internet, TAURIN'21*, 2021.

[4] Gabriel Alves Reis. Default Route Analytics: Um sistema de monitoramento de rotas padrão em sistemas autônomos. https://github.com/Ga-Alves/default_routes/blob/master/README.md, 2025. Acessado: 2025-12-07.

[5] Haya Shulman Tomas Hlavacek, Amir Herzberg and Michael Waidner. Practical experience: Methodologies for measuring route origin validation. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 634–641*, 2018.

[6] Kamil Myśliwiec and contributors. Nestjs - a progressive node.js framework. https://nestjs.com/, 2023. Acessado em: 11 de dezembro de 2025.

[7] Meta and contributors. React - a javascript library for building user interfaces. https://react.dev/, 2023. Acessado em: 11 de dezembro de 2025.

[8] NLNOG Foundation. Nlnog ring. https://ring.nlnog.net/, 2023. Acesso em: 11 de dezembro de 2025.

[9] Center for Applied Internet Data Analysis (CAIDA). CAIDA AS Relationships Dataset. https://publicdata.caida.org/datasets/as-relationships/serial-2/, 2021. Accessed: 2021-01-16.