UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

MARCELO ALMEIDA DA SILVA

PerfResolv: Analisando o Desempenho de Resolvedores DNS Públicos em Relação à Popularidade de Domínios

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação

Orientador: Prof. Dr. Lisandro Zambenedetti Granville

Porto Alegre
2024

CIP — CATALOGAÇÃO NA PUBLICAÇÃO

Silva, Marcelo Almeida da

PerfResolv: Analisando o Desempenho de Resolvedores DNS Públicos em Relação à Popularidade de Domínios / Marcelo Almeida da Silva. – Porto Alegre: PPGC da UFRGS, 2024.

58 f.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR–RS, 2024. Orientador: Lisandro Zambenedetti Granville.

1. DNS. 2. Popularidade. 3. Medição. 4. Resolvedores. I. Zambenedetti Granville, Lisandro. II. Título.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito, Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”

MARTIN LUTHER KING JR.

AGRADECIMENTOS

Agradeço a Deus, autor de toda sabedoria, juntamente com Oxalá e meus orixás, por me permitirem iniciar e concluir este trabalho. Sua orientação e inspiração foram fundamentais para superar os obstáculos neste curto prazo.

Ao porto seguro que é minha família, meus pais Sandra, Jurandir, minha irmã Bárbara e meu Tio Paulo por terem me dado uma base solida de amor e educação.

A minha esposa Clarice e meus filhos Miguel e Rafael pela paciência nas horas em que estava ausente de seu convívio e por me mostrarem que o amor incondicional é o maior sentimento que existe no mundo, não havendo limites nem regras para a sua compreensão.

Ao professor e orientador Lisandro, pois sua cooperação permanentemente convicta e decidida foi essencial para o desenvolvimento deste mestrado. Mostrou o empenho e dedicação de um verdadeiro amigo, pelos valiosos e convenientes auxílios. É difícil expressar, em linguagem escrita, toda a minha gratidão.

Aos pós-doc e amigos, Muriel e Eder, expresso minha gratidão pelo apoio caloroso durante o desenvolvimento deste mestrado. Agradeço profundamente pelo incentivo e orientação que ofereceram em momentos de dúvida. Sua generosidade, dedicação e atenção foram fundamentais em todas as etapas deste processo. Agradeço especialmente pela orientação exemplar e pela busca contínua de soluções para os desafios enfrentados. Vocês são verdadeiros modelos de orientadores e pessoas, demonstrando um compromisso genuíno com o sucesso do aluno. Muito obrigado por tudo.

Agradeço imensamente ao doutorando e amigo Luciano por seu apoio crucial e ideias valiosas durante meu mestrado. Sua dedicação contagiosa e inspiradora, aliada à nossa parceria, foram fundamentais para o sucesso. Admiro sua história, valores e profissionalismo exemplares. Você é um verdadeiro exemplo de ser humano e educador. Obrigado por tudo.

Aos Professores Jefferson, Luciano e Juliano, Sempre muito pacientes e solícitos, foram peça primordial no bom andamento de todo o mestrado e pela dedicação ao meu crescimento intelectual e as explicações diversas sobre dúvidas muitas vezes simplesmente desconectas sobre o tema.

Finalmente, agradeço aos funcionários do Instituto de Informática, em especial ao Luis Otavio e ao Leandro, pelo apoio crucial nesta fase da minha vida acadêmica. Suas orientações foram inestimáveis, tornando minha jornada mais suave e enriquecedora.

PerfResolv: Analyzing the Performance of Public DNS Resolvers in Relation to Domain Popularity

ABSTRACT

The Domain Name System (DNS) represents one of the pillars of the World Wide Web and plays an indispensable role in its operation. DNS is an extensive-distributed database structured to resolve readable domain names for people, companies and institutions into corresponding and reliable IP addresses. This dissertation presents PerfResolv, an approach for analyzing the performance of public DNS resolver servers (*e.g.*, Google, Cloudflare, OpenDNS, Quad9 and ComodoDNS) with different domain name popularity. The analysis was carried out with PerfResolv located at geographically distributed points in three different countries: Brazil, Switzerland and Australia. The results were obtained by considering the response time for resolving domain names with different levels of popularity to see if and how geolocation, domain name popularity, week, day and time affect the performance of DNS resolver servers. The results show considerable fluctuations in the response time of some DNS resolvers, with a variation of up to 40% in response time at different times of the day. In addition, there are differences between the resolution time of popular and unpopular domains, which are also influenced by the geolocation of the measurement monitors.

Keywords: DNS. Popularity. Measurement. Resolvers.

RESUMO

O Sistema de Nomes de Domínio (DNS, Domain Name System) representa um dos pilares da rede mundial de computares e desempenha um papel indispensável no seu funcionamento. DNS é um extenso banco de dados distribuído estruturado para resolver nomes de domínio legíveis para pessoas, empresas e instituições em endereços IP correspondentes e confiáveis. Esta dissertação apresenta PerfResolv, uma abordagem para análise de desempenho em servidores resolvedores DNS públicos (*e.g.*, Google, Cloudflare, OpenDNS, Quad9 e ComodoDNS) com diferentes popularidades de nomes de domínios. A análise foi realizada com PerfResolv localizado em pontos distribuídos geograficamente em três países diferentes: Brasil, Suíça e Austrália. Os resultados foram obtidos considerando o tempo de resposta para resolução de nomes de domínio com diferentes níveis de popularidade para verificar se e como a geolocalização, popularidade do nome de domínio, semana, dia e hora afetam o desempenho dos servidores resolvedores de DNS. Os resultados mostram flutuações consideráveis no tempo de resposta de alguns resolvedores DNS, com uma variação de até 40% no tempo de resposta em diferentes horas do dia. Além disso, existem diferenças entre o tempo de resolução de domínios populares e impopulares, que também são influenciados pela geolocalização dos monitores de medição.

Palavras-chave: DNS. Popularidade. Medição. Resolvedores.

LISTA DE ABREVIATURAS E SIGLAS

IP	Protocolo de Internet
DNS	Sistema de Nome de Domínio
SRI	Instituto de Pesquisa de Stanford
ISI	Instituto de Ciências da Informação
USC	Universidade do Sul da Califórnia
TLD	Domínio de Nível Superior
ISO	Organização Internacional de Normalização
DCA	Agência de Comunicações de Defesa
CSV	Valores Separados por Vírgulas
RFC	Pedido de Comentários
UDP	Protocolo de Data gramas do Usuário
TCP	Protocolo de Controle de Transmissão
SDN	Rede Definida pelo Software
PPs	Perguntas de pesquisa
IETF	Força tarefa de engenharia de Internet
IANA	Autoridade para Atribuição de Números da Internet
IDNs	Serviço DNS Interno
FTP	Protocolo de Transferência de Arquivos
EDNS	Mecanismos de Extensão para DNS
TSIG	Ãssinatura de Transação
FQDN	Nome de Domínio Totalmente Qualificado
UFRGS	Universidade Federal do Rio Grande do Sul
ICANN	Corporação da Internet para Atribuição de Nomes e Números
ASCII	Código Padrão Americano para Intercâmbio de Informações

MILNET Rede Militar

COMSAT Corporação de Satélites de Comunicações

ARPANET Rede de Agências e Projetos Pesquisas Avançadas

DDN-NIC Centro de informações de rede de dados de defesa

NSFNET Rede Nacional de Fundação Científica

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A Internet tornou-se indispensável devido à importância de suas aplicações e possibilidades de uso em diferentes setores da indústria, governo e entretenimento. O Sistema de Nomes de Domínio (DNS, do Inglês Domain Name System) representa um dos alicerces da Internet, desempenhando um papel indispensável para o seu funcionamento. O DNS funciona como um grande banco de dados distribuído e estruturado para resolução de nomes de domínio legíveis (*e.g.*, *www.ufrgs.br*) em endereços de Protocolos de Internet (IP, do Inglês Internet Protocol) correspondentes e válidos (PARK et al., 2019). A criação do DNS se iniciou na década de 80, com o surgimento da Rede de Agências para Projetos de Pesquisas Avançadas (ARPANET, do Inglês Advanced Research Projects Agency Network) (LEINER et al., 2009). Com o advento dos avanços de automatização das plataformas computacionais, melhorias foram realizadas no DNS, tendo em novembro de 1983 os critérios e normativas do DNS publicadas na Request for Comments (RFC) 882 (MOCKAPETRIS, 1983a) e RFC 883 (MOCKAPETRIS, 1983b) e atualizadas em novembro de 1997 nas RFCs 1034 (MOCKAPETRIS, 1987a) e 1035 (MOCKAPETRIS, 1987b). Tais normativas são, ainda hoje, relevantes e amplamente utilizadas para a comunicação entre dispositivos e acesso a serviços (LAI; TSAI, 2021).

Diferentes abordagens e implementações do protocolo DNS permitem oferecer aos usuários variáveis níveis de desempenho e segurança (YAN et al., 2019). O DNS também é utilizado como um meio de negócios, com diversas organizações (*i.e.*, resolvedores DNS) oferecendo a resolução de domínio como serviço com o foco em prover melhor desempenho ou segurança para os usuários e serviços. Tais serviços podem ser oferecidos por servidores de DNS privados, os quais oferecem serviços que garantem a segurança, privacidade e desempenho para usuários dispostos a pagar por tais serviços (HOUNSEL et al., 2019). Além disso, existe também a possibilidade de servidores de DNS locais, os quais podem ser instalados na infraestrutura do usuário (*e.g.*, empresas de grande porte) e fornecem mais agilidade na resolução de nomes. Porém, em ambos os cenários, existem contrapartidas entre custos, complexidade de operação e segurança (HAO et al., 2015).

Para suprir tal demanda de forma eficiente, confiável e sem custos, os servidores de DNS públicos surgem como uma opção. Tais servidores podem ser descritos como resolvedores DNS gratuitos e relativamente confiáveis, pois são ofertados por grandes empresas mantenedoras de serviços na Internet (*e.g.*, Google, Cloudflare e Cisco) que adotam

medidas efetivas de segurança. Os servidores DNS públicos podem também prover recursos relacionados à segurança e, especificamente, para identificação de domínios maliciosos (AFFINITO; BOTTA; VENTRE, 2022). Porém, os servidores DNS públicos vem representando uma crescente preocupação na academia e indústria devido à centralização de serviços, fluxos de rede e infraestrutura (ZEMBRUZKI; JACOBS; GRANVILLE, 2022). Além disso, a terceirização de serviços para empresas de resolução de DNS públicos que não adotem medidas efetivas de segurança pode gerar riscos para os usuários do serviço, visto que a resolução de nomes pode ser afetada negativamente em casos de ataque maliciosos (*e.g.*, Amplificação, *Spoofing* e Negação de Serviço) (ZEMBRUZKI et al., 2020; FRANCO et al., 2021).

Nesse contexto, a literatura atual foca em abordagens relacionadas a identificar e quantificar a centralização dos DNS (MOURA et al., 2020). Entretanto, a maioria das pesquisas não analisa o desempenho de servidores resolvedores DNS públicos de maneira profunda (*e.g.*, considerando a popularidade de domínios e dias da semana), nem dão a ênfase necessária nos passos para definir abordagens que medem tal desempenho (DOAN; FRIES; BAJPAI, 2021). Logo, existe uma oportunidade e a motivação necessária para abordagens que analisam o desempenho de resolvedores de DNS públicos em tais contextos não explorados.

1.1 Objetivos e Contribuições

O objetivo desta dissertação é propor uma abordagem inédita para análise do desempenho de resolvedores DNS públicos realizada sob a perspectiva da popularidade de domínios e de resolvedores. Para tal, a abordagem proposta deverá ser capaz de realizar a medição de métricas de desempenho utilizando nomes de domínios considerando, diferentes características, como a popularidade e geolocalização distintas dos resolvedores DNS públicos. A definição de servidores resolvedores DNS públicos a serem utilizados deverá levar em conta sua representatividade e confiabilidade, a qual será verificada através da análise da literatura.

Portanto, propomos e implementamos uma abordagem, chamada PerfResolv, para análise detalhada do desempenho de servidores DNS públicos utilizando diferentes listas de domínios com diferentes características (*e.g.*, popularidade e geolocalização). Para isso, uma abordagem de monitoramento geo-distribuída e baseada em diferentes critérios de seleção de domínios foi definida e avaliada. Assim, é possível obter dados para um

melhor entendimento do desempenho da resolução de domínios sob diferentes perspectivas e critérios. Os resultados deste trabalho permitem avançar o estado da arte com uma abordagem inédita e também com discussões pertinentes para auxiliar trabalhos futuros na área de monitoramento de DNS.

A abordagem proposta é utilizada para coletar informações de diferentes resolvedores DNS públicos de modo a possibilitar a análise da infraestrutura DNS sob diferentes perspectivas, como se o dia da semana ou o tipo de domínio impacta no tempo de resposta. As Pergunta de Pesquisa (PP) que serão respondidas utilizando o PerfResolv são:

- **PP1**: Qual é o tempo médio de resolução para cada servidor resolvedor DNS público?
- **PP2**: O tempo médio é impactado pelo dia e hora da semana?
- **PP3**: Os servidores possuem tempo de respostas diferentes para nomes de domínio populares, médios ou novos?
- **PP4**: A geolocalização das consultas é um fator que impacta no tempo de resposta?

Baseado nos resultados das análises realizadas nesta dissertação, será possível ter uma visão mais clara sobre o desempenho, em termos de tempo médio de resolução de domínio, de servidores resolvedores DNS públicos utilizando nomes de domínios de diferentes popularidades e de acordo com diferentes dias da semana. Portanto, espera-se que este trabalho possa contribuir para o debate sobre a importância dos servidores resolvedores DNS públicos, bem como para o desenvolvimento de soluções que possam garantir desempenho e segurança para usuários finais.

1.2 Organização

Esta dissertação está organizado da seguinte forma: No Capítulo 2 apresentamos a fundamentação teórica necessária para o entendimento de conceitos-chave desta dissertação. Tais conceitos incluem o funcionamento do protocolo DNS, bem como a apresentação das diferentes implementações e evoluções do protocolo. Além disso, os principais resolvedores DNS são apresentados, bem como uma discussão sobre as diferenças entre resolvedores públicos e privados.

No Capítulo 3, é apresentado uma análise dos trabalhos relacionados focados em desempenho de resolvedores DNS públicos, entendendo assim suas aplicações, desafios e oportunidades de pesquisa. Também, é apresentado a metodologia de análise definida para

identificar os trabalhos relevantes no contexto desta dissertação. Portanto, neste capítulo, diferentes soluções comerciais e acadêmicas são analisadas e comparadas seguindo uma metodologia de análise bem definida.

No Capítulo 4, apresentamos o PerfResolv, uma abordagem geo-distribuída para medições de servidores resolvedores DNS públicos baseado em popularidade de domínios. A abordagem é descrita em detalhes, incluindo a definição de domínios, arquitetura conceitual e detalhes de implementação.

As avaliações são apresentadas no Capítulo 5. Neste capítulo, são realizados diversos experimentos geo-distribuídos para *(i)* verificar a capacidade do PerfResolv em coletar os resultados de forma eficiente e *(ii)* obter uma análise aprofundada do tempo de resposta de resolvedores DNS públicos através da variação de domínios, países e dias da semana. Os resultados são apresentados e discutidos em detalhes.

Esta dissertação é concluída no Capítulo 6, resumindo as principais contribuições e apresentando conclusões obtidas através da concepção e utilização do PerfResolv. Além disso, é discutido direções e possibilidades de trabalhos futuros.

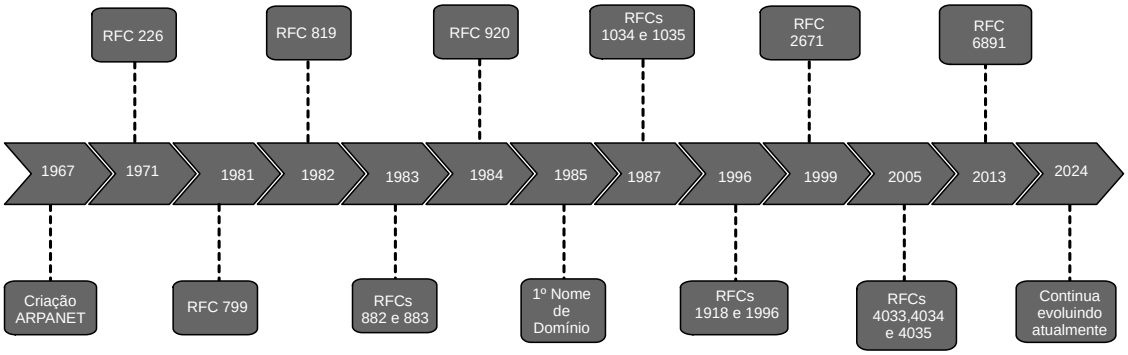
2 REFERENCIAL TEÓRICO

Neste capítulo, é apresentado uma visão abrangente dos componentes que constituem o DNS, explorando suas características distintas e principais funcionalidades. Começamos com uma perspectiva história da criação do DNS na Seção 2.1 e, em seguida, definimos os conceitos de nomes de domínio na Seção 2.2. Após, é apresentado a estrutura hierárquica do DNS na Seção 2.3. Na Seção 2.4 é apresentado e discutido os conceitos de resolvedores DNS, seguido do processo da resolução de DNS na Seção 2.5. Por fim, na Seção 2.6, é discutido as principais implementações do protocolo de DNS, incluindo aspectos de desempenho e segurança.

2.1 Perspectiva Histórica

Nesta seção, apresentamos o DNS sob uma perspectiva histórica, destacando os principais eventos que tiveram um papel crucial na sua criação e composição, bem como os elementos fundamentais da sua evolução. A evolução histórica do protocolo DNS é apresentado na Figura 2.1.

Figura 2.1 – Linha do Tempo do DNS



Fonte: (Autor, 2024)

Assim que a ARPANET foi constituída no Instituto de Pesquisa de Stanford (SRI, do inglês Stanford Research Institute) em 1967, o DNS ainda não existia. Primeiramente, a rede era de tamanho reduzido, possibilitando que usuários e servidores geralmente soubessem como navegar entre diferentes serviços e interagir uns com os outros sem depender de uma estrutura de diretório global. No entanto, a proporção que a ARPANET cresceu, tornou-se evidente que a implementação de um serviço de diretório seria crucial (TOORN et al., 2022).

Em 1971, foi introduzida a RFC 226 (KARP, 1971), que desenvolveu uma tabela chamada `hosts.txt` que definia uma lista de nomes para endereços de todos os recursos da rede. Assim, os usuários podiam manter esse arquivo localmente para facilitar buscas e permitir que os computadores encontrassem tais recursos na rede sem necessidade de conhecimento prévio do endereço de rede. Para isso, os usuários preenchiam um modelo de e-mail, enviado ao SRI, que compilava as alterações na próxima versão da tabela `hosts.txt`, que estava disponível globalmente via Protocolo de Transferência de Arquivos (FTP, do Inglês File Transfer Protocol) (ROSS, 2006).

Neste contexto, a ARPANET crescia com a adição de novos hosts, enfrentando dificuldades devido à falta de atualizações regulares. Assim, as desatualizações causavam colisões de nomes, divisão de um domínio por mais de um host e adicionava mais complexidade ao serviço. Em suma, esses desafios levaram os pesquisadores à conclusão de que uma nova estrutura era necessária, resultando no desenvolvimento do DNS conforme descrito na RFC 799 (MILLS, 1981), implementado pela Corporação de Satélites de Comunicações (COMSAT, do Inglês Communications Satellite Corporation). Assim, foi possível obter os recursos necessários para a criação de um sistema capaz de lidar com milhares de hosts de maneira escalonável (ROSS, 2006).

Com base nisso, em 1982, a RFC 819 (SU; POSTEL, 1982), proposta pelo Instituto de Ciências da Informação (ISI, do Inglês Information Sciences Institute) da Universidade do Sul da Califórnia e pelo professor Zaw-Sing Su do SRI, foi expandir e fornecer o primeiro esboço mais amplo da estrutura do DNS. Assim, essa RFC definiu que o DNS seria a opção viável para uma comunicação mais simples entre diferentes redes. Além disso, em 1983, o ISI, lançou à comunidade cientifica duas novas RFCs chamadas de "Nomes de Domínio e seus Conceitos e Facilidades"na RFC 882 (MOCKAPETRIS, 1983a) e "Nomes de Domínio e sua Implementação e Especificação"na RFC 883 (MOCKAPETRIS, 1983b). Após, no ano 1984, finalizaram o projeto e elaboraram a RFC 920 (POSTEL; REYNOLDS, 1984), definindo as bases das pesquisas futuras e introduzindo novas mudanças no protocolo DNS (MOCKAPETRIS; DUNLAP, 1988).

Em suma, a RFC 920 (POSTEL; REYNOLDS, 1984), apresentou os primeiros nomes de domínio de nível superior planejados para serem adicionados ao DNS (*e.g.*, .com, .net, .org, .edu, .gov, .mil e .arpa). Para tal, a RFC projetou a criação de domínios de nível superior (TLD, do Inglês Top Level Domain) em países usando códigos de letras da Organização Internacional de Normalização (ISO, do Inglês International Organization for Standardization) e TLD para diferentes tipos de organizações e escopo internacional.

Com base nisso, em março de 1985, os dois primeiros nomes de domínio foram registrados, sendo o marco inicial do DNS moderno, com registros notáveis como *symbolics.com* e *think.com* (MOCKAPETRIS; DUNLAP, 1988).

O DNS continuou evoluindo discretamente como um dos alicerces da futura Internet. Entretanto, em 1986, a demanda acadêmica levou à criação da Rede Nacional de Fundação Científica (NSFNET, do Inglês National Science Foundation Network) pela Fundação Nacional de Ciências dos EUA, com a gestão confiada à Merit Networks Inc. Assim, a NSFNET desempenhou um papel crucial na formação da Internet atual (ROSS, 2006). Embora essas RFCs tenham se tornado obsoletas em 1987, após a proposta das novas RFCs 1034 (MOCKAPETRIS, 1987a) e 1035 (MOCKAPETRIS, 1987b), elas foram um marco para a evolução de pesquisas relacionadas a DNS ao introduzir diferentes conceitos-chave, como a delegação e autoridade de DNS (ROSS, 2006).

Em 1990, houve o desligamento da ARPANET, tendo a rede NSFNET expandindo-se para mais de cem mil computadores interconectados. Para tal crescimento da rede, a implementação do DNS foi dividida pela Agência de Comunicações de Defesa (DCA, do Inglês Defense Communications Agency) pois a necessidade de uma estrutura centralizada para gerenciar a raiz e delegar autoridade aos registrantes seria necessária. Para isso, em 1993, com a divisão da ARPANET e Rede Militar (MILNET, do Inglês Military Network), o DCA escolheu o SRI para gerenciar os registros de nomes de domínio no novo DNS, enquanto o ISI ficou responsável pela gestão da raiz e operações do Centro de informações de rede de dados de defesa (DDN-NIC, do Inglês Defense Data Network Information Center) (ROSS, 2006).

Assim, em 1996 a RFC 1918 (REKHTER et al., 1996) propôs um novo conjunto de faixas de endereços IP reservadas para uso particular em redes locais. Com base nisso, essas faixas incluíam intervalos designados para utilização em redes domésticas e corporativas, sem a necessidade de roteamento na Internet pública. Portanto, essa medida teve como foco evitar conflitos de endereços IP e conservar os endereços públicos, desempenhando um papel fundamental no projeto de redes privadas e garantindo a eficiência do roteamento global da Internet (BROIDO; NEMETH; CLAFFY, 2003).

Além disso, também em 1996, a RFC 1996 (VIXIE, 1996) apresentou uma abordagem do protocolo NOTIFY para o DNS. Em suma, este protocolo visava agilizar a propagação de alterações em uma zona DNS, comunicando imediatamente servidores secundários quando a mudanças no servidor primário. Para isso, a RFC 1996 estabeleceu definições de termos, delimitou os papéis dos servidores (primário, secundário e furtivo)

e forneceu detalhes sobre a mensagem NOTIFY, incluindo seu formato DNS e o uso de protocolos de transporte do protocolo de data grama do usuário (UDP, do Inglês User Datagram Protocol) ou Protocolo de Controle de Transmissão (TCP, do Inglês Transmission Control Protocol) reduzindo o atraso na propagação de atualizações e abordando desafios dos tempos de atualizações prolongados das zonas DNS (VIXIE, 1996).

Nesse contexto, em 1999, a RFC 2671 (VIXIE, 1999) introduziu o mecanismo de extensão para DNS (EDNS, do Inglês Extension Mechanisms for DNS). Assim, permitindo a inclusão de informações adicionais em mensagens DNS. Além disso, o EDNS0 foi desenvolvido para facilitar a implementação de recursos avançados, como suporte a tamanhos de mensagens maiores e novos tipos de dados, para melhorar a eficiência e flexibilidade das comunicações DNS na Internet e possibilitando a conexão com servidores DNS comuns em redes mais abrangentes (REGAN; ABDEL-HALIM, 2018).

Após, em 2005, foi proposto o DNSSEC com as RFCs 4033 (ARENDS et al., 2005a), 4034 (ARENDS et al., 2005b) e 4035 (ARENDS et al., 2005c). Assim, essa proposta incorporou mais segurança ao DNS, buscando resolver a propagação de caches maliciosos e assegurando a totalidade e vericidade de dados do DNS por meio de assinaturas digitais criptografadas nas credenciais. Com base nisso, com a validação DNSSEC, os resolvedores podem verificar se os dados em uma determinada resposta de DNS coincidem com os dados da zona do domínio de destino. No entanto, para os requisitos de validação sejam executados, a checagem da vericidade dos dados se fez necessário, assim como os servidores de nomes devem remeter assinaturas e chaves aos resolvedores para verificações de segurança (HERZBERG; SHULMAN, 2015).

Em 2013, foi apresentado a RFC 6891 (DAMAS; GRAFF; VIXIE, 2013), como uma proposta de atualização da RFC 2671 (VIXIE, 1999), que havia introduzido o mecanismo de extensão para DNS (EDNS, do Inglês Extension Mechanisms for DNS) no ano de 1999. Assim, a proposta de atualização da RFC 2671 já ultrapassada se fez necessário para que o EDNS possibilitasse aos servidores DNS estabelecessem comunicação com outros servidores baseados em EDNS, contornando assim a limitação de 512 bytes nos pacotes. Para tal, mudanças no registro EDNS0 possibilitaram que resolvedores DNS e servidores de nomes suportassem novos mecanismos. Por exemplo, o DNSSEC, permitiu a troca de flags que não são armazenadas em cache pelos resolvedores e são utilizadas principalmente para coordenar parâmetros na camada de transporte, sendo que o uso do EDNS0 não exige alterações no software ou protocolo DNS, pois a maioria dos resolvedores e servidores de nomes o suporta (AKANHO et al., 2021).

2.2 Introdução ao DNS

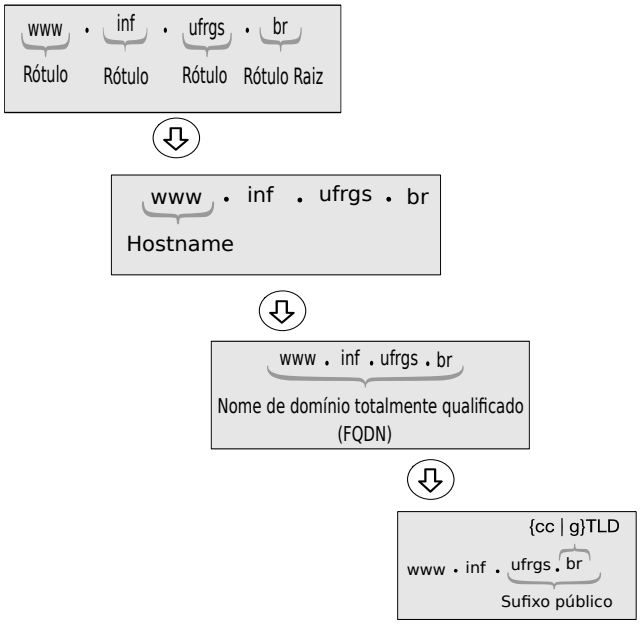
Nesta seção, apresentaremos conceitos e termos sobre nomes de domínio, compreendendo sua composição, bem como os elementos fundamentais da estrutura de nomes de domínio e como a hierarquia de níveis é aplicada.

O conceito de nome de domínio pode ser descrito como uma sequência disposta de letras, números e sinal gráfico hífen tendo como base a tabela do Código Padrão Americano para Intercâmbio de Informações (ASCII, do Inglês American Standard Code for Information Interchange). Assim, os nomes de domínio são compostos através da composição de rótulos distintos, os quais são separados por pontos. Para tal composição dos rótulos deve-se seguir o seguinte critérios: limite máximo de 63 caracteres, contendo letras independentemente de serem maiúsculas ou minusculas, números de 0 a 9 ou sinal gráfico hífen (TOORN et al., 2022).

Com base disso, um nome de domínio é composto por uma sequência de rótulos nos quais letras maiúsculas ou minúsculas não são considerados relevantes, uma vez que resultam no mesmo endereço IP válido. Dessa forma, quando o usuário pesquisar o nome de domínio (*e.g.*, *WWW.inf.ufrgs.br* ou *www.inf.ufrgs.br*, o resultado será o mesmo endereço IP, independentemente de como é escrito. Em suma, o nome de domínio é finalizado com um ponto no final do rótulo raiz, embora este ponto seja frequentemente omitido ou interrompido ao encontrar o rótulo raiz (TOORN et al., 2022).

Além disso, algumas características são dadas aos nome de domínio em uma sequência de rótulos (*e.g.*, www, inf, ufrgs e br). Assim, o rótulo mais a esquerda é chamado de *hostname*. O conjunto de todos os rótulos é definido como Nome de Domínio Totalmente Qualificado (FQDN). Por fim, existem rótulos que constituem o sufixo público dos domínios, *e.g.*, ufrgs.br (TOORN et al., 2022). A Figura 2.2 ilustra o conceito de um rótulo de nome de domínio (*e.g.*, www.inf.ufrgs.br) a fim de ilustrar os diferentes conceitos introduzidos nesta seção. Na seção seguinte, será discutida a hierarquia do DNS dos diferentes rótulos.

Figura 2.2 – Rótulo de Nomes de Domínio



Fonte: Adaptado de (TOORN et al., 2022)

2.3 Hierarquia de DNS

Nesta seção, abordarmos a estrutura da hierarquia do DNS, a disposição organizacional, bem como a estrutura de níveis empregada em cada zona hierárquica e os níveis de domínios.

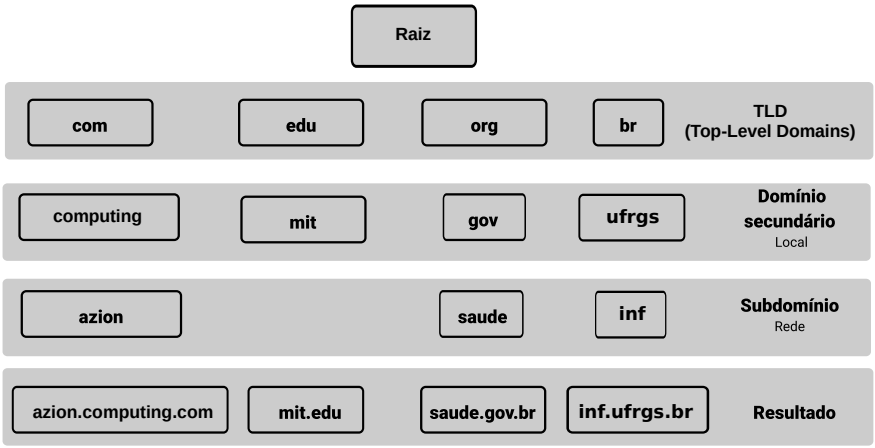
A hierarquia do DNS é composta por uma estrutura de diversas áreas de controle denominadas zonas. Dessa forma, essas zonas tem como ponto inicial a zona raiz desta hierarquia. Além disso, essas zonas raiz do DNS são administradas por 13 servidores localizados em diferentes partes do mundo (TOORN et al., 2022).

Assim, a hierarquia do DNS é semelhante a uma árvore invertida, conforme demonstrado na Figura 2.3. Dessa forma, a zona raiz do DNS gerencia, delega responsabilidades e realiza registros dos TLD. Esses registros dividem o espaço, como demonstrado pelo TLD (*e.g.*, **.br** para países, **.com** para domínios comerciais, **.edu** para instituições acadêmicas e **.org** para organizações) (TOORN et al., 2022).

Além disso, na Figura 2.3, podemos ver domínios de segundo nível (*e.g.*, *.mit* e *.gov)*, que são associados a pessoas ou organizações, seguidos subdomínios (*e.g.*, *.azion* e *.saúde*) e níveis subsequentes. Assim, formando o domínio completo (*e.g.*, *saude.gov.br*). A indústria de nomes de domínio evoluiu, inicialmente centralizada pela Autoridade para Atribuição de Números da Internet (IANA, do Inglês Internet Assigned Numbers Autority). Com o crescimento da Internet, surgiu um modelo escalonado, permitindo que

registradores vendessem nomes de domínio. Para gTLDs, a ICANN define requisitos, enquanto para ccTLDs, a política é determinada pelos operadores dos registros (TOORN et al., 2022).

Figura 2.3 – Hierarquia DNS



Fonte: Adaptado de (TOORN et al., 2022)

Assim, entre 2000 e 2012, a Corporação da Internet para Atribuição de Nomes e Números (ICANN, do Inglês Internet Corporation for Assigned Names and Numbers), introduziu alguns gTLDs (*e.g.*, .gov e .edu)adicionais. Além disso, em 2011, definiu uma nova política que permitiu mais de 1000 novos gTLDs, o incluindo Serviço DNS interno (IDNs, do Inglês Internationalized Domain Names) para Rede Definida por Software (SDN, do Inglês Software defined networking). Por fim, tais medidas impulsionaram as empresas de nomes de domínio privadas, avaliadas em bilhões de dólares, tendo como principal representante a GoDaddy, uma empresa registradora de domínios e hospedeira de sites. Dessa forma, os provedores de DNS privados entraram no mercado, oferecendo serviços para gerir a infraestrutura de DNS (TOORN et al., 2022).

2.4 Resolvedores de DNS

Nesta seção, abordaremos os servidores resolvedores DNS, a disposição organizacional, a estrutura e as operações realizadas por cada servidores resolvedores DNS.

Os resolvedores de DNS são essenciais para o desempenho da Internet, pois grande parte da comunicação começa com uma consulta a eles (SAHA et al., 2023). Assim, essa estrutura se baseia em quatro tipos principais de servidores (*e.g.*, Servidores Recursivos, Servidores Raiz, Servidores TLD e Servidores Autoritativos), sendo essa estrutura hierár-

quica a base dos servidores DNS (ZEMBRUZKI et al., 2020).

Inicialmente, a estrutura é composta pelo servidor recursivo, um tipo de servidor DNS que tem como atribuição a resolução de nomes de domínios. Assim, um usuário solicita a resolução de um nome de domínio, ele recorre ao servidor recursivo local. Após isso, o servidor recursivo inicia uma série de consultas para resolver o nome de domínio para um endereço IP valido. Para isso, são realizadas consultas em diversos servidores DNS na hierarquia do DNS (*e.g.*, servidor raiz, servidor TLD e servidor autoritativo). Por fim, o servidor recursivo prossegue enviando consultas até encontrar o servidor DNS autoritativo responsável pelo domínio solicitado, respondendo à solicitação original do usuário com o número de IP válido (GAO et al., 2014).

Dessa forma, os primeiros servidores a serem consultados são os servidores raiz, desempenhando um papel vital como o topo da hierarquia DNS, existindo apenas 13 servidores raiz usados para consultas das diversas redes de servidores. Tais, servidores raiz são encarregados de fornecer referências autorizadas de nomes de todos os servidores TLD, o que resulta em referências recursivas para todos os nomes de host na Internet (CASTRO et al., 2010).

Em suma, os servidores TLD são responsáveis por fornecer informações sobre os domínios de nível superior na hierarquia do DNS. Para isso, eles atuam como autoridades finais para domínios de alto nível (*e.g.*, .com, .org, .net e assim por diante), direcionando consultas para os servidores autoritativos responsáveis pelos domínios de segundo nível. Além disso, exercem um papel crucial na coordenação e manutenção da integridade e estabilidade do sistema de nomes de domínio global, sendo de suma importância para a eficiência e confiabilidade da infraestrutura de nomes de domínio na Internet (ZEMBRUZKI et al., 2020).

Por fim, os servidores autoritativos armazenam uma lista de endereços IP de nomes de domínio, são geralmente operados por empresas que possuem determinados domínios. Dessa forma, a consulta para domínios pertencentes a um servidor autoritativo deve estar junta ao servidor, independentemente de onde as consultas se originaram (*e.g.*, Brasil, Suíça ou Austrália). Sendo, extremamente benéfico para os responsáveis pela segurança, pois permite o monitoramento e a mitigação de um ponto único em termos de influência global (KWON et al., 2016).

Além disso, existem dois tipos de servidores resolvedores, sendo privados e públicos, que estão presentes em diferentes níveis da hierarquia de servidores DNS. Assim, servidores resolvedores privados são geridos por organizações ou empresas para uso in-

terno e são configurados para atender às necessidades específicas de uma rede privada, como uma rede corporativa oferecendo controle ampliado sobre segurança, privacidade e desempenho para os usuários dentro da rede. Tais servidores podem incluir filtros de conteúdo, bloqueio de sites maliciosos, otimização de cache e outras medidas de segurança. Já os resolvedores públicos são operados por entidades independentes ou privadas e acessíveis pela Internet aberta. Assim, são utilizados ofertados e acessados fora das redes privativas.

Os servidores resolvedores públicos conquistaram atualmente um nível de confiança elevado e tornara-se o padrão *de facto* tanto para usuários quanto empresas. Esse tipo de resolvedor é utilizado como uma alternativa gratuita a resolvedores mantidos localmente e com custos inerentes de operação. Além disso, tais resolvedores podem proporcionar um melhor desempenho e disponibilidade que resolvedores menores (*e.g.*, mantidos localmente ou por pequenos provedores) (SAHA et al., 2023). Além disso, servidores de DNS públicos podem auxiliar em diversos aspectos, como contornar medidas de censura e aumentar a segurança na resolução de domínios (ZEMBRUZKI; JACOBS; GRANVILLE, 2022). A importância de resolvedores de DNS públicos é ressaltada na literatura. Por exemplo, (RADU; HAUSDING, 2020) revela que mais de 50% das consultas de DNS são realizadas por resolvedores de DNS públicos, assim, destacando a sua popularidade e aceitação.

Além disso, os servidores resolvedores DNS também empregam políticas de anycast para uma estratégia de endereçamento e roteamento que utiliza várias rotas entre servidores resolvedores DNS para compartilham o mesmo endereço IP na Internet. Dessa forma, essa abordagem é bastante utilizada para assegurar a disponibilizar a redundância de serviços, (*e.g.*, DNS e CDNs). Em suma, anycast utiliza o Protocolo de Gateway de Borda (BGP, do Inglês Border Gateway Protocol), para direcionar os usuários para a instância anycast mais próxima, de acordo com métricas BGP. Dentre os serviços que utilizam o anycast destacam-se os operadores de servidores DNS tais como os servidores DNS raiz e os operadores de ccTLD e provedores de mitigação de DDoS (*e.g.*, Akamai, Cloudflare e CDNs). No entanto, prever essas rotas de forma previsível pode ser um enorme desafio devido ao grande número de políticas de roteamento entre Sistemas Autônomos (AS, do Inglês autonomous systems), diversas vezes ocultas pelos servidores DNS, operadores e provedores (VRIES W. B., 2020).

A Tabela 2.1 apresenta um resumo dos principais servidores resolvedores públicos mundiais. Assim, as linhas representam os diferentes servidores resolvedores públicos e as colunas as suas características (*e.g.*, quais são os IPs de DNS primário e secundário utilizados pelos provedores). Por fim, foi verificado as localizações (*e.g.*, cidades, estados e países) da sede dos servidores, de modo a compreender a geolocalização e legislação inerente a cada resolvedor DNS.

Tabela 2.1 – Exemplos de Servidores Resolvedores DNS Públicos

Provedor	**DNS Primário**	**DNS Secundário**	**Sede da Empresa**
Google	8.8.8.8	8.8.4.4	Mountain View California, Estados Unidos
CloudFlare	1.1.1.1	1.0.0.1	Los Angeles California, Estados Unidos
Comodo Secure DNS	8.26.56.26	8.20.247.20	Clifton New Jersey, Estados Unidos
Open DNS	208.67.222.222	208.67.220.220	San Francisco California, Estados Unidos
Quad9	9.9.9.9	149.112.112.112	Zurique Distrito de Zurique, Suíça
Control D	76.76.2.0	76.76.10.0	Toronto Ontario, Canada
CleanBrowsing	185.228.168.9	185.228.169.9	Temecula California, Estados Unidos
Alternate DNS	76.76.19.19	76.223.122.150	Lewes Delaware, Estados Unidos
DNS AdGuard	94.140.14.14	94.140.15.15	Limassol Limassol, Chipre
Yandex.DNS13	77.88.8.8	77.88.8.1	Moscou Central Federal District, Russia

Fonte: (Autor, 2024)

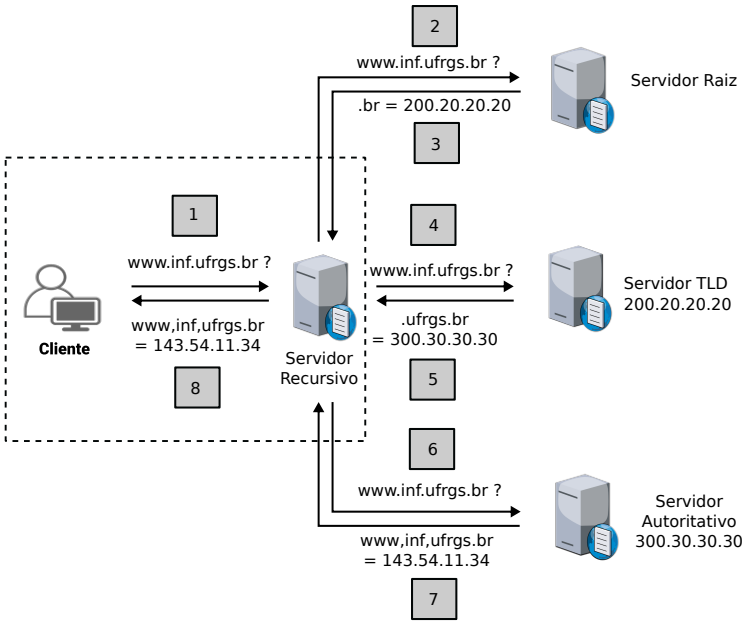
2.5 Resolução do DNS

Nesta seção, apresentamos uma visão sobre a resolução do DNS, incluindo as etapas envolvidas, bem como a estrutura e as operações que cada etapa executa.

A Figura 2.4 detalha o processo de resolução de um nome de domínio, por exemplo, *www.inf.ufrgs.br*, para ilustrar como esse processo funciona. Tal processo é descrito no restante desta seção.

Inicialmente, no Passo (1), o processo de resolução de um nome de domínio compreende uma sequência de etapas geralmente ocultas ao usuário ao acessar um nome de domínio (*e.g.*, *www.inf.ufrgs.br*) ou serviço associado a um domínio específico. Assim, a resolução ocorre por meio do sistema DNS, cujo objetivo principal é obter o endereço

Figura 2.4 – Resolução DNS



Fonte: (Autor, 2024)

IP válido associado ao nome de domínio esperado. Portanto, quando um usuário busca resolver um nome de domínio, como *www.inf.ufrgs.br*, é enviado uma solicitação de resolução de DNS ao seu servidor DNS, sendo geralmente o Provedor de Internet (ISP) do próprio usuário. Porém, se a informação não estiver no cache do ISP. O ISP começa a atuar como um servidor recursivo para resolver os nomes de domínio em nome do usuário, iniciando assim o processo de rastreamento dos rótulos do domínio, sendo que o objetivo é encontrar o servidor DNS necessário para resolução do domínio.

Assim, no Passo (2), se o nome de domínio estiver armazenado, o servidor recursivo enviará uma consulta ao servidor raiz. Em suma, servidores raiz não terão informações sobre um endereço IP específico (*e.g.*, 143.54.11.34), mas saberá onde estão os servidores de nomes que atendem esse TLD (.br). No Passo (3), o Servidor Raiz retornará a lista de servidores TLD para que o provedor ou servidor possa enviar novamente uma consulta, desta vez para um servidor TLD. Dessa forma, no Passo (4), o servidor recursivo envia ao servidor TLD a solicitação do nome de domínio. Já no Passo (5), o servidor TLD retornará então ao servidor recursivo os nomes dos servidores de nomes autoritativo onde o domínio desejado está armazenado.

Assim, no Passo (6) o servidor recursivo que fez a solicitação envia uma consulta ao servidor autoritativo que hospeda a zona do domínio em questão. Onde, no Passo (7), ele responderá ao servidor recursivo do solicitante o endereço IP de *www.inf.ufrgs.br*. Por fim, no Passo (8) o servidor recursivo do usuário armazenará essas informações em

cache para futuras solicitações e as enviará ao seu resolvedor, que as enviará para o seu navegador e permitirá que o usuário acesse o site desejado.

Portanto, como este exemplo, é possível verificar que a resolução do DNS se configura como uma ferramenta essencial para viabilizar a comunicação eficaz na Internet, de forma simplificada do ponto de vista do usuário. Em suma, a resolução do DNS garante que os dispositivos conectados sejam capazes de localizar mutualmente e realizar a troca de informações de maneira ágil e segura.

2.6 Protocolos DNS

Nesta seção, abordaremos os principais protocolos de DNS, suas principais características e capacidades de uso em servidores DNS.

Os protocolos DNS são compostos por diversas camadas funcionais, visando garantir a resolução eficiente e precisa de nomes de domínio em endereços IP. Assim, esses protocolos se baseiam em normas técnicas e especificações técnicas para estabelecer o formato e a transmissão de consultas e respostas DNS pela rede. Dessa maneira, o DNS codifica as mensagens de dados, bem como os protocolos de transporte UDP e TCP, usados para a transmissão de consultas e respostas DNS entre os usuários e os servidores (ZEMBRUZKI et al., 2020).

O protocolo DNS sobre TLS (DoT, do Inglês DNS over Transport Layer Security - TLS), é utilizado para criptografar consultas DNS, garantindo segurança e privacidade. Assim, o protocolo DoT, também pode ser empregado em sites HTTPS adicionando uma camada de criptografia sobre o UDP. Essa abordagem visa proteger as consultas de nomes de domínio contra interferências ilegais durante o trajeto (KOSHY et al., 2021). Além disso, o protocolo DNS sobre HTTPS (DoH, do Inglês, DNS over Hypertext Transfer Protocol Secure - HTTPS), foi desenvolvido para resolver problemas de privacidade associados ao DNS, permitindo o encapsulamento de consultas DNS utilizando o protocolo HTTPS. Em suma, o DNS clássico (ou seja, utilizando UDP na porta 53) apresenta consultas em texto sem criptografia, o que pode revelar dados confidenciais, como os hábitos de navegação do usuário. Dessa forma, o principal objetivo do DoT e DoH é diminuir a vigilância aos usuários e protegê-los contra a criação de perfis de atividades, especialmente para fins de propaganda direcionada e censura (HYNEK et al., 2022).

Outro exemplo de implementação de protocolo DNS é o DNSCrypt. O DNSCrypt é um protocolo que criptografa as comunicações entre clientes e resolvedores, usando

tanto UDP quanto TCP, conforme a infraestrutura de chave pública disponível. Assim, o cliente envia uma consulta sem autenticação, com um certificado e o identificador do provedor, para um resolvedor habilitado. Para tal, o resolvedor responde com certificados assinados e autenticados pelo cliente, utilizando a chave pública do provedor. Portanto, Cada certificado contém um número específico usado pelo cliente para cifrar as consultas. Dessa forma, a lista inclui a chave pública do cliente, utilizada para a descriptografar as solicitações e cifrar as respostas no lado do resolvedor (KURIHARA; TANAKA; KUBO, 2023).

Em outra abordagem, o protocolo DNS sobre QUIC (DoQ, do Inglês, DNS over Quick UDP Internet Connections - QUIC) é proposto como um protocolo cujo objetivo é melhorar a segurança e eficiência das consultas DNS. Dessa forma, o protocolo QUIC é uma variação do UDP, desenvolvido pelo Google e adotado pela Força Tarefa de Engenharia de Internet (IETF, do Inglês Internet Engineering Task Force). Assim, o protocolo dispõe de recursos como criptografia de ponta a ponta, retransmissões rápidas e controle de congestionamento. Por fim, o DoQ oferece consultas DNS rápidas e seguras sobre conexões UDP, melhorando a velocidade e a privacidade das comunicações DNS (SHREEDHAR et al., 2021).

Outro conhecido protocolo é o DNSSEC. O protocolo Segurança sobre DNS (DNSSEC, do Inglês DNS Security) é uma importante extensão do protocolo DNS, uma vez que oferece uma camada de segurança que inclui autenticação de origem, integridade de dados e negação de existência. O protocolo autentica os dados DNS fornecidos por um servidores DNS ou outros servidores. Assim, as respostas de servidores DNSSEC são devidamente assinadas digitalmente. Ao examinar essas assinaturas, um resolvedor DNSSEC pode confirmar a legitimidade da fonte de dados e confirmar se as informações são consistentes com as que estão armazenadas no servidor DNS autoritativo. Por fim, quando as informações não estão no servidor, uma negação autenticada é gerada, garantindo assim a integridade e a autenticidade das operações DNS (ARIYAPPERUMA; MITCHELL, 2007).

Portanto, é possível verificar que além do desempenho, os protocolos DNS também desempenham um papel crucial na garantia da estabilidade e segurança da Internet, contribuindo para a confiabilidade e eficácia das comunicações. Entretanto, esta dissertação de mestrado tem como foco o protocolo DNS tradicional (*i.e.*, DNS53), focando na análise do desempenho (tempo de resposta) dos resolvedores de DNS e não no contexto da segurança oferecida.

3 TRABALHOS RELACIONADOS

Neste capítulo, é apresentado uma visão abrangente dos trabalhos relacionados que estão sendo pesquisados em relação ao DNS, demonstrando suas características distintivas. A Metodologia da análise é apresentada na Seção 3.1, seguida da análise da literatura na Seção 3.2 e concluímos na Seção abordamos os principais protocolos de DNS.

3.1 Metodologia de Análise

Nesta seção, apresentaremos uma análise dos principais trabalhos focados em desempenho de resolvedores DNS públicos, entendo assim suas aplicações, desafios e oportunidades de pesquisa. Para tal, a metodologia de análise foi definida em três etapas: *(i)* Definição das palavras-chave e base de dados para buscas de trabalhos, (*(ii)* Definição dos critérios de inclusão baseado nos artigos coletados e *(iii)* Identificar e analisar artigos relevantes definidos com base nos critérios do item (ii).

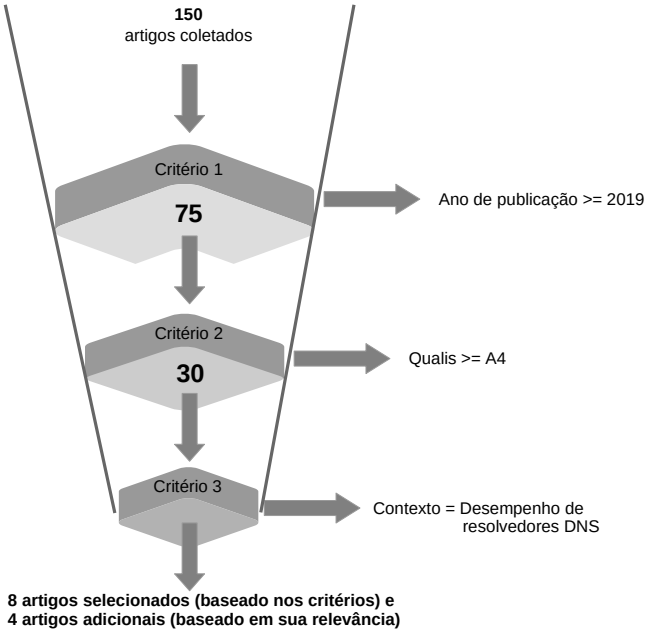
Na primeira etapa, definimos as seguintes palavras-chave para busca: *Domain name system, DNS resolvers, Public DNS resolvers e Performance of Public DNS Resolvers*. Após, buscas foram realizadas, utilizando a combinação dessas palavras-chave. As base de dados utilizadas foram a ACM Digital Library, IEEE eXplore e Google Scholar. Tais bases foram definidas devido à qualidade dos trabalhos publicados (*i.e.*, revisado por pares) e também por indexarem grande quantidade de trabalhos científicos. Para cada artigo resultante da busca foi feita uma verificação a fim de assegurar sua relevância para o domínio deste estudo. Após, foram aplicados diferentes critérios de inclusão dos trabalhos coletados.

O *Critério 1* inclui apenas artigos que foram publicados a partir de 2019 (*i.e.*, últimos 5 anos). No Critério 2 são selecionados apenas artigos publicados em conferências ou revistas de alto impacto baseado no sistema Qualis CAPES [1]. Após, são selecionados apenas os artigos que tem como contexto e foco principal o desempenho de resolvedores DNS.

A abordagem proposta é apresentada na Figura 3.1, incluindo a quantidade de artigos analisadas e a filtragem utilizando os critérios definidos. No topo da figura, temos

[1] https://www.gov.br/capes/pt-br/acesso-a-informacao/acoes-e-programas/avaliacao/avaliacao-quadrienal/metodologia-do-qualis-referencia-quadrienio-2017-2020

Figura 3.1 – Artigos Pesquisados



Fonte: (Autor, 2024)

o total de 150 artigos identificados na literatura. Após aplicar todos os critérios definidos, foram selecionados 8 artigos para serem analisados de forma mais profunda. Além disso, 4 artigos excluídos devido aos critérios aplicados foram reconsiderados e adicionados devido a sua alta relevância para o escopo do trabalho. Assim, tais artigos foram incluídos na lista e analisados de forma independente dos critérios, totalizando 12 artigos mapeados e analisados.

Com base nos artigos selecionados, é possível entender as diferentes motivações e esforços de pesquisas sobre medição do desempenho de resolvedores de DNS, bem como traçar desafios e oportunidades de pesquisas futuras. O restante deste trabalho foca em analisar os resultados e contribuir para o entendimento da área de pesquisa em desempenho de resolvedores DNS.

3.2 Análise da Literatura

Nesta seção, apresentaremos a análise dos métodos de avaliação de resolvedores DNS públicos, revelando as complexidades e oportunidades na análise de desempenho e segurança. Essa análise incentiva melhorias contínuas no desempenho desses resolvedores, visando beneficiar usuários, pesquisadores e operadores de rede. Na Tabela 3.1, há

uma comparação dos trabalhos avaliados, considerando cinco características, incluindo protocolos e métricas predominantes.

Tabela 3.1 – Comparação dos Trabalhos sobre Desempenho de DNS

Trabalho	Descrição	Protocolo DNS	Métricas Analisada	# de Resolvedores	Datasets das Medições	Medições Distribuídas
(BORGOLTE et al., 2019)	Análise centralizada da performance de DoH e DNS local em rede universitária	Do53, DoT, DoH	Tempo de pesquisa do usuário, Tempo de carregamento de pagina Web	4	Privado	Não
(HOUNSEL et al., 2020)	Análise da performance dos protocolos DNS e criptografia através do carregamento de páginas Web	Do53, DoT, DoH	Tempo de carregamento de pagina Web, Tempo de resposta da consulta DNS	3	Público	Sim
(DOAN; FRIES; BAJPAI, 2021)	Análise da performance de servidores DNS utilizando sondas RIPE	Do53	Tempo de resposta da consulta DNS	10	Público	Sim
(CHHABRA et al., 2021)	Análise da performance da rede BrightData para comparar DNSSEC com DNS padrão	DoH, Do53, DNSSEC	Tempo de resposta de carregamento de pagina Web	4	Público	Sim
(AFFINITO; BOTTA; VENTRE, 2022)	Análise da performance de servidores DNS em domínios e o impacto sobre carregamento de pagina Web	Do53, DoH	Tempo de resposta da consulta DNS, Tempo de resposta de carregamento de pagina Web	5	Público	Não
(KOSEK et al., 2022)	Análise da performance dos protocolos DNS em carregamento de pagina Web	DoT, DoH, Do53, DoTCP, DoQ	Tempo de carregamento de pagina Web	Centenas	Privado	Sim
(PerfOps, 2023)	DNSPerf é uma ferramenta Web que testa a latência de mais +200 servidores globais	Do53	Tempo de resposta da consulta DNS	Centenas	Privado	Sim
(BHOWMICK et al., 2023)	Análise da performance de servidores DNS que violam TTL na rede BrightData	DNSSEC e DoH	Tempo de resposta da consulta DNS	Milhares	Público	Sim

Fonte: (Autor, 2024)

Em suma, foram analisados 8 artigos selecionados baseados nos critérios definidos e 4 artigos adicionais baseados em sua relevância. A primeira análise se concentra na avaliação do desempenho realizada usando os protocolos DNS, conforme demonstrado no estudo de (BORGOLTE et al., 2019). Além disso, investigações de desempenho são conduzidas usando o protocolo *DNS Security (DNSSEC)*, com um foco na experiência do usuário final ao acessar páginas da Web, como abordado no por (HOUNSEL et al., 2020).

Diversos estudos avaliam o impacto do protocolo DNS no carregamento de páginas web, exemplificado em (AFFINITO; BOTTA; VENTRE, 2022). O desempenho com o protocolo *Quick UDP Internet Connections (QUIC)* também é analisado, como visto em (KOSEK et al., 2022). A segurança e análises de desempenho relacionadas são discutidas em (CHHABRA et al., 2021), bem como questões envolvendo o *Time-To-Live (TTL)*, exploradas em (BHOWMICK et al., 2023). Outros estudos abordam o desempenho em relação ao tempo de resposta dos resolvedores DNS públicos, usando sondas RIPE Atlas para confiabilidade e segurança, conforme (DOAN; FRIES; BAJPAI, 2021). Além disso, ferramentas comerciais como o *Performance DNS (DNSPerf)* (PerfOps, 2023) realizam testes de latência para avaliar o desempenho.

Os trabalhos adicionais também são relevantes para entender o estado da arte. Em (AGER B., 2010), há uma comparação de resolvedores DNS locais que avalia a capacidade de resposta e o impacto na latência do resolvedor e do cache DNS. Em outro estudo, (OTTO J. S., 2012) analisou como o uso de serviços DNS remotos afeta o desempe-

nho das *Content Delivery Network (CDN)*. Em outro trabalho, (RULA; BUSTAMANTE, 2014) investigou o desempenho dos resolvedores DNS em redes celulares nos EUA e Coreia do Sul, revelando desafios na localização de clientes devido à opacidade da rede e desacordos. Neste estudo, os autores realizaram um experimento com mais de 340 dispositivos, onde foi constatado que, em 75% das vezes, o tempo de resposta em redes celulares se igualou ou superou o de redes tradicionais. Por fim, (HOURS et al., 2016) avaliou o impacto no desempenho de downloads ao usar o DNS do provedor de Internet versus o DNS público do Google.

Com base na análise da literatura, é possível observar um interesse crescente sobre as implicações em questões de desempenho e segurança, como, por exemplo, os impactos do *DNS-over-HTTPS (DoH)* no desempenho e privacidade. Diversos estudos têm focado na medição da variação dos tempos de resposta de resolvedores DNS públicos. Alguns estudos demonstram que em certas regiões, como África e América do Sul, os resolvedores públicos têm tempos de resposta mais longos. As análises também variam em definir quais resolvedores possuem o melhor desempenho geral, visto que diversos atributos devem ser considerados, como, por exemplo, a geolocalização, políticas de segurança implementadas e o tempo de resposta. Além disso, a centralização de resolvedores DNS e seus potenciais impactos na privacidade do usuário e na soberania digital de nações (ZEMBRUZKI; JACOBS; GRANVILLE, 2022; BOEIRA et al., 2023) também é analisado e discutido.

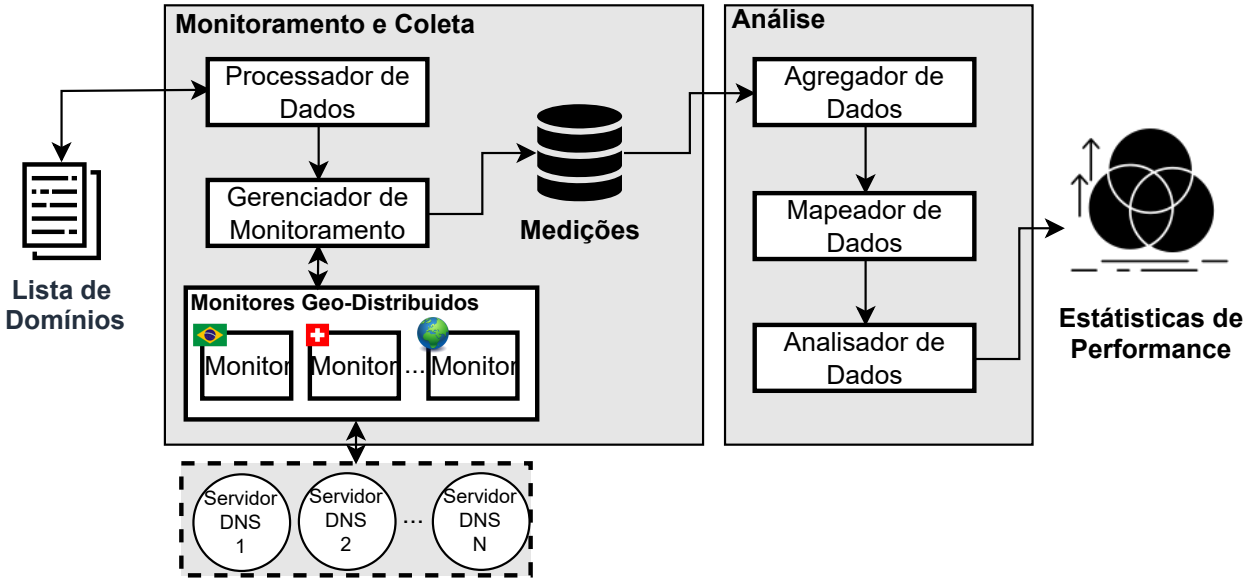
4 PERFRESOLV

Neste capitulo, é apresentado a solução PerfResolv, incluindo sua realização e descrição detalhada desde a fase de monitoramento e coleta, até a análise estatísticas do desempenho dos resolvedores de DNS.

O PerfResolv é proposto como uma abordagem para automação *(i)* do processo de medições de desempenho de servidores resolvedores DNS públicos e *(ii)* da análise de domínios com diferentes níveis de popularidade. Tais medições e análises podem ser executadas de forma geo-distribuída por meio de monitores gerenciados pelo PerfResolv. O Tempo Médio de Greenwich (GMT) é utilizado como forma de auxiliar no processo de análise dos resultados oriundos de diferentes países com fuso-horários diferentes.

Assim, o PerfResolv permite uma análise sobre os servidores resolvedores DNS públicos e seus níveis de desempenho (*i.e.*, tempo médio de resposta) para domínios com diferentes níveis de popularidade. Dias da semana e horários de uso também podem ser analisados de modo a traçar um perfil de uso e os seus impactos no desempenho de servidores resolvedores DNS públicos. A abordagem proposta e implementada pelo PerfResolv é apresentada na Figura 4.1, incluindo os fluxos e componentes necessários para todas as etapas. Tais componentes atuam desde o monitoramento e coleta até a análise dos dados obtidos.

Figura 4.1 – Fluxo de Monitoramento, Coleta e Análise Proposto e Implementado pelo PerfResolv



Fonte: (Autor, 2024)

Durante a fase de monitoramento e coleta, lista de domínios são definidas e processadas pelo *Processador de Dados*. Nesta etapa, é necessário definir a popularidade dos domínios. Os domínios são encaminhados ao Gerenciador de Monitoramento, que controla monitores globais para observar comportamentos de resolvedores DNS em diferentes regiões. No módulo de análise, os resultados obtidos são organizados de forma estruturada (*e.g.*, arquivos CSV), categorizados e analisados para criar subconjuntos para cada popularidade de domínio, incluindo assim a média para cada resolvedor por tipo de domínio, dia da semana e hora. Cada módulo é discutido detalhadamente ao longo deste capítulo, incluindo as configurações e base de dados utilizadas para a realização de medições geo-distribuídas.

4.1 Módulo de Monitoramento e Coleta

Primeiramente, durante a fase de monitoramento e coleta, a lista de domínios é definida para análise e processada pelo *Processador de Dados*. A lista de domínios é composta por 60 nomes de domínios, sendo os 20 mais populares da lista Tranco (Le Pochat et al., 2019), 20 de posições intermediários e 20 novos domínios criados na Rede Tchê. A lista Tranco lista dos domínios mais populares baseado na combinação de outras listas (*e.g.*, Alexa, Cisco, Umbrella, Majestic e Quantcast). Dessa forma, a fusão das listas resulta numa classificação mais estável para pesquisas (Le Pochat et al., 2019). Já a Rede Tchê é uma estrutura de rede de computadores que conecta instituições de ensino superior e centros de pesquisa situados no Rio Grande do Sul, permitindo assim a criação de domínios em ambientes controlados e sem acessos em massa globais.

Dessa forma, este processamento permite a separação dos domínios de acordo com sua popularidade (*e.g.*, baseado na sua posição em rankings e tráfego de acesso). Após, os domínios são encaminhados para o *Gerenciador de Monitoramento*, o qual é encarregado do controle e comunicação com monitores geo-distribuídos em diferentes regiões do mundo (*e.g.*, Austrália, Brasil e Suíça). Para tal, o gerenciador de monitoramento construído para rodar em máquinas virtuais Microsoft Azure Linux rodando em 3 países (Austrália, Brasil e Suíça), dessa maneira os monitores realizam consultas periódicas (*e.g.*, de hora em hora durante 5 dias) para todos os domínios previamente definidos.

Assim, os monitores são estrategicamente distribuídos para observar comportamentos de resolvedores DNS públicos que podem variar em termos de desempenho e segurança conforme o domínio, resolvedores e região. Durante o monitoramento, são

executadas 30 medições para cada domínio a cada hora do dia. Tais, medições de desempenho costumam ser realizadas para diminuir a influência de fatores aleatórios e obter uma média representativa do sistema. Assim, essa prática estatística possibilita uma avaliação mais acurada da variabilidade do desempenho em diferentes circunstâncias (*e.g.*, médias, desvios de padrão e os intervalos de confiança) a partir dessas execuções, tendo uma melhor perspectiva do comportamento global do sistema e crucial para a tomada de decisões e aperfeiçoamento do desempenho do sistema (JAIN, 1991).

Por fim, todas as medições realizadas são encaminhadas para o *Gerenciador de Monitoramento*, o qual centraliza as medições e armazena em um banco de dados local para posterior análise.

4.2 Módulo de Análise

Primeiramente, na etapa de análise, os dados contidos no banco de dados local são acessíveis para serem analisados em cada etapa, por meio de componentes (*i.e.*, Agregador de dados, Mapeador de dados e Analisador de dados).

Assim, a primeira etapa consiste na execução da operação do *Agregador de Dados*. Para tal, essa operação visa compilar todas as informações relevantes em um único arquivo denominado **data-agg.csv**. Dessa forma, os arquivos CSV seguem estruturas específicas. A Tabela 4.1 apresenta uma descrição dos campos utilizados pelo *Agregador de Dados*, incluindo exemplos de valores para cada um deles. Por fim, esses dados são organizados conforme os formatos mencionados, preparando-as para a segunda etapa de processamento.

A segunda etapa compreende a etapa de execução do *Mapeador de Dados*. Nesta etapa, o objetivo é organizar e categorizar os dados de forma lógica e clara em cada campo designado. Dessa forma, ao agrupá-los nos campos correspondentes, eles são preparados para a próxima etapa de processamento.

Por fim, a terceira etapa compreende a execução da fase de *Análise de Dados*. Nessa fase, o objetivo é empregar as médias das medições coletadas dos nomes de domínio junto aos servidores resolvedores, conduzindo uma análise precisa em busca de uma acurácia mais refinada. Desta forma, por meio do estabelecimento de critérios, os tipos de domínio são classificados e apresentados de forma gráfica para avaliação, proporcionando uma compreensão detalhada do desempenho dos resolvedores DNS para posterior avaliação e discussão.

Tabela 4.1 – Campos do Módulo de Análise

Campos	Descrição	Exemplo
Domínio	Nome de domínio da lista de dominios utilizados para realizar as medições do tempo de resposta dos servidores resolvedores públicos.	google.com
Tempo	Tempo de resposta que o servidor resolvedor leva para responder a uma solicitação feita pelos monitores, medido em milissegundos	10 ms
Servidor	Servidor resolvedor público onde são realizadas as consultas da lista de nomes de domínios	OpenDNS
País	País onde os dados são coletados, usado para definir onde o monitoramento é feito.	Austrália
Data GMT	Data de acordo com o fuso horário de Greenwich. É usado como referência comum para as medições.	06/16/2023
Hora GMT	Tempo padrão internacionalmente aceito no meridiano de Greenwich, sem ajustes para horário de verão ou outros fatores.	02:00
Dia da semana GMT	Dia da semana de Greenwich, que é um padrão de referência amplamente utilizado para sincronização de eventos em todo o mundo.	Sexta-feira
Data local	Data de acordo com o fuso horário específico da localidade do monitoramento.	06/16/2023
Hora Local	Hora atual de acordo com o fuso horário específico, da localidade do monitoramento.	12.00
Dia local da semana	Dia da semana de acordo com o fuso horário específico de uma localidade do monitoramento.	Sexta -feira
Tipo de domínio	Categoria de um nome de domínio de acordo com sua popularidade, como por exemplo popular, médio e novo	Popular

Fonte: (Autor, 2024)

4.3 Implementação

Nesta seção, apresentaremos detalhes de implementação do PerfResolv, incluindo as tecnologias e bibliotecas utilizadas. A implementação do PerfResolv e os *datasets* utilizados estão disponíveis publicamente em (SILVA et al., 2023).

Os experimentos foram realizados em máquinas virtuais *Microsoft Azure* rodando em 3 países (Austrália, Brasil e Suíça). Os componentes do PerfResolv para monitoramento e coleta foram implementados utilizando *Python 3.11*. Os monitores utilizam diferentes bibliotecas como, (*e.g.*, *dns.resolver*, *time*, *datatime*, *date*, *glob* e *os*). Dessa forma, a biblioteca *dns.resolver* é a principal, pois usa um conjunto de ferramentas como *dnspython 2.3* que suporta os tipos de registros DNS necessários para execução do PerfResolv. Sendo assim, é uma ferramenta útil para resolução de domínios em diferentes resolvedores de DNS públicos e coletar as médias de desempenho.

Embora algumas funcionalidades não tenham sido utilizadas na implementação do PerfResolv, é importante ressaltar que a ferramenta *dnspython* oferece ainda funcionalidades como, por exemplo, transferências de zona e atualizações dinâmicas e proporciona suporte a mensagens autenticadas por meio de assinaturas de transação (TSIG) e EDNS,

agregando uma camada adicional de segurança e integridade às operações relacionadas ao DNS.

Com base nisso, o *dns.resolver* é executado com os domínios a serem analisados, listando os domínios de cada tipo (*e.g.*, 20 populares, 20 médios e 20 novos). Tal abordagem é executada 30 vezes para cada domínio, sendo executadas a cada hora para cada domínio em servidores resolvedores DNS públicos que serão analisados (*i.e.*, Google, Cloudflare, Comodo, OpenDNS e Quad9). A função utilizada para realizar os experimentos é descrita no Algoritmo 4.1

```
1 def resolver_dns(dominio, tipo):
2     try:
3         resposta = dns.resolver.resolve(dominio, tipo)
4         return resposta
5     except Exception as e:
6         pass
```

Listing 4.1 – Código para Execução do Monitoramento de Desempenho de um Dominio

Para medir o tempo de resolução de um domínio, foi utilizada a biblioteca *time*. Essa biblioteca possui uma função chamada `time()`, que retorna o tempo em segundos desde o *epoch* do Linux (ou seja, 00:00:00 UTC em 1º de janeiro de 1970). O código listado no Algoritmo 4.2 descreve como o tempo médio é calculado utilizando essa função. Na linha 1, é salvo o tempo atual em uma variável chamada *start_time*; em seguida, na linha 2, é realizada a chamada da função *resolver_dns(domínio, tipo)*, conforme descrito no Algoritmo 4.1; por fim, na linha 3, é calculada a diferença entre o tempo atual e o tempo salvo, resultando no tempo de resposta para resolver o domínio.

```
1 start_time = time.time()
2 resolver_dns(domain, tipo)
3 end_time = time.time() - start_time
```

Listing 4.2 – Código para Execução do Monitoramento de Desempenho de um Dominio

Além disso, os arquivos CSV coletados são colocados em pastas separadas por cada dia de coleta. Assim, as medições são agregadas (*e.g.*, média das medições realizadas para um domínio em uma determinada hora) e mapeadas para CSV. Assim, os arquivos CSV são utilizados para coletar dados devido à sua estrutura básica e eficiente. Dessa forma, ao armazenar dados em formato tabular e separados por pontos, esses arquivos tornam-se acessíveis, compatíveis e promovem a interoperabilidade entre sistemas heterogêneos. Portanto, sua estrutura textual é legível tanto para análises semelhantes quanto para processamentos automatizados, fundamentais em análises de grande porte.

Os resultados agregados são então analisados utilizando a biblioteca *pandas 2.0.2*. Esta biblioteca permite versatilidade e eficiência na manipulação e análise de dados em *Python*, oferecendo uma ampla gama de funcionalidades. Assim, a biblioteca permite não apenas a leitura e escrita de dados em diferentes formatos, mas também a execução de operações complexas (*e.g.*, limpeza, transformação e agregação de dados). Além disso, suas capacidades avançadas de indexação e seleção facilitam a manipulação precisa e eficiente de conjuntos de dados volumosos e intricados. Portanto, a biblioteca *pandas* se destaca como uma ferramenta indispensável, contribuindo significativamente para a análise e interpretação de dados em larga escala.

Por fim, a geração de visualizações dos dados é conduzida através da biblioteca *Vega-Altair 5.0.1*, notável por sua robustez e confiabilidade. Além disso, esta biblioteca se distingue por oferecer uma ampla variedade de funcionalidades gráficas, resultando em visualizações de imagens de alta qualidade e precisão.

5 AVALIAÇÃO

Neste capitulo, tratamos da avaliação da solução proposta para esta dissertação, os resultados obtidos através da aplicação da abordagem PerfResolv são analisados e discutidos.

Primeiramente, o objetivo é entender os comportamentos dos diferentes resolvedores DNS públicos em relação à popularidade de domínios, hora e geolocalização. Assim, os experimentos foram realizados definindo, inicialmente, os endereços de IPs dos servidores resolvedores DNS públicos que serão analisados (*i.e.*, Google, Cloudflare, Comodo, OpenDNS e Quad9) e as respostas obtidas foram o tempo de resposta para realizar a consulta e receber a resposta DNS. Tais resultados podem ser acessados no repositório disponível em (SILVA et al., 2023) e foram processados para obtenção de estatísticas agregadas para análise.

Dessa forma, 60 domínios foram analisados, sendo 20 populares, 20 médios e 20 novos. Além disso, todos os domínios novos foram gerados dentro da rede acadêmica da Universidade Federal do Rio Grande do Sul (UFRGS) e de pesquisa para realização deste trabalho. Portanto, os experimentos foram realizados em máquinas virtuais *Microsoft Azure* rodando em 3 países (Austrália, Brasil e Suíça), com 30 repetições sendo executadas a cada hora para cada domínio e resolvedor (JAIN, 1991). Enfim, o período englobou um tempo de 5 dias (segunda-feira até sexta-feira). Assim, é possível obter a média de cada ciclo de execução para garantir uma maior acurácia em nossa análise.

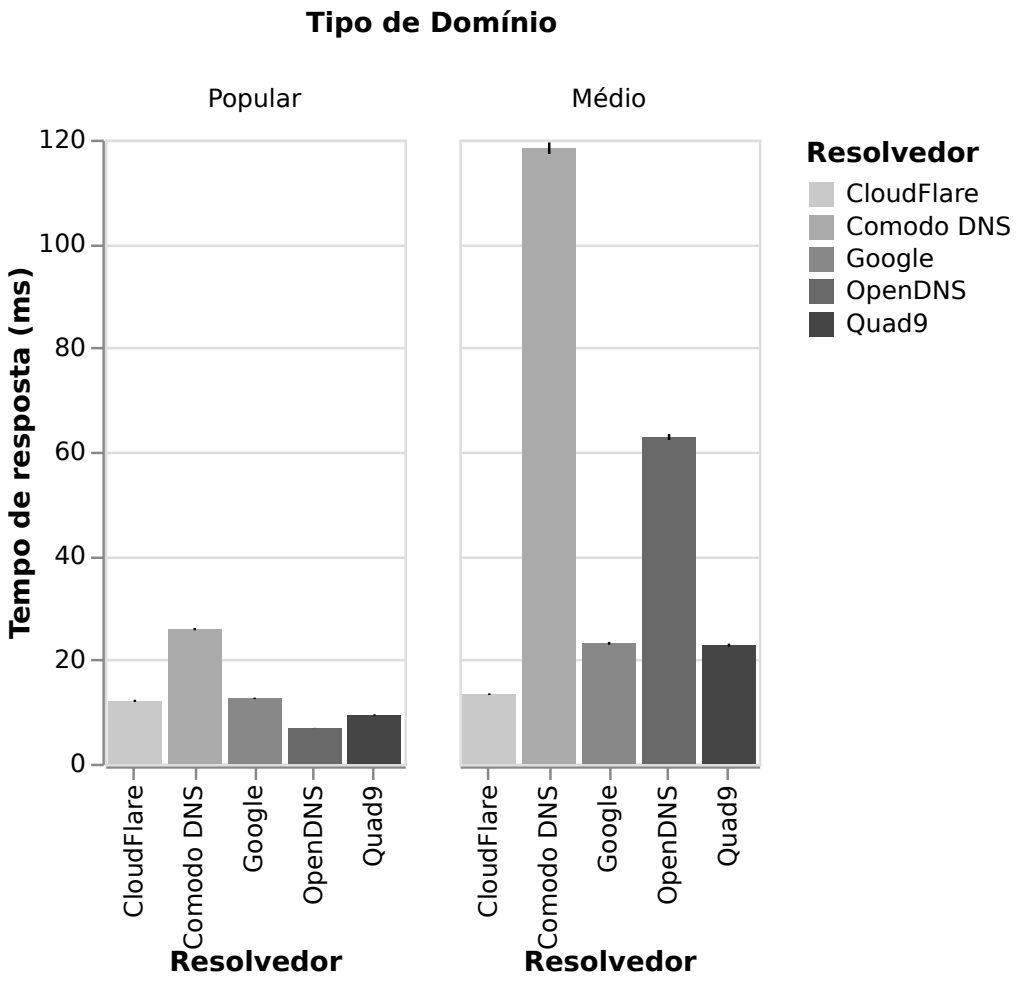
5.1 Avaliação com Domínios Populares e Médios

Nesta seção, apresentaremos a avaliação dos domínios populares e médios e suas métricas de desempenho.

Inicialmente, a primeira análise consiste na verificação do tempo de resposta para domínios populares e médios. Assim, o desempenho dos resolvedores em milissegundos (ms) são obtidas para a resolução de domínios com mais acessos e conhecidos (*i.e.*, 20 domínios mais populares) e também para domínios que não são tão populares, mas ainda assim são conhecidos (*i.e.*, 20 domínios com popularidade média). Esses domínios foram extraídos da lista Tranco.

Para tal, os resultados são apresentados nas Figuras (5.1), (5.2) e (5.3). Assim, na Figura 5.1, é possível observar a comparação dos resolvedores na Austrália. Nessa análise, o servidor resolvedor DNS OpenDNS teve melhor desempenho em domínios populares enquanto o servidor resolvedor DNS CloudFlare teve melhor desempenho em domínios médios, enquanto o servidor resolvedor DNS Comodo DNS teve o pior desempenho em domínios populares e entre os domínios médios. Já os servidores Google e Quad9 obtiveram desempenhos similares para domínios médios.

Figura 5.1 – Desempenho para Resolução de Domínios Popular e Médios por requisições da Austrália

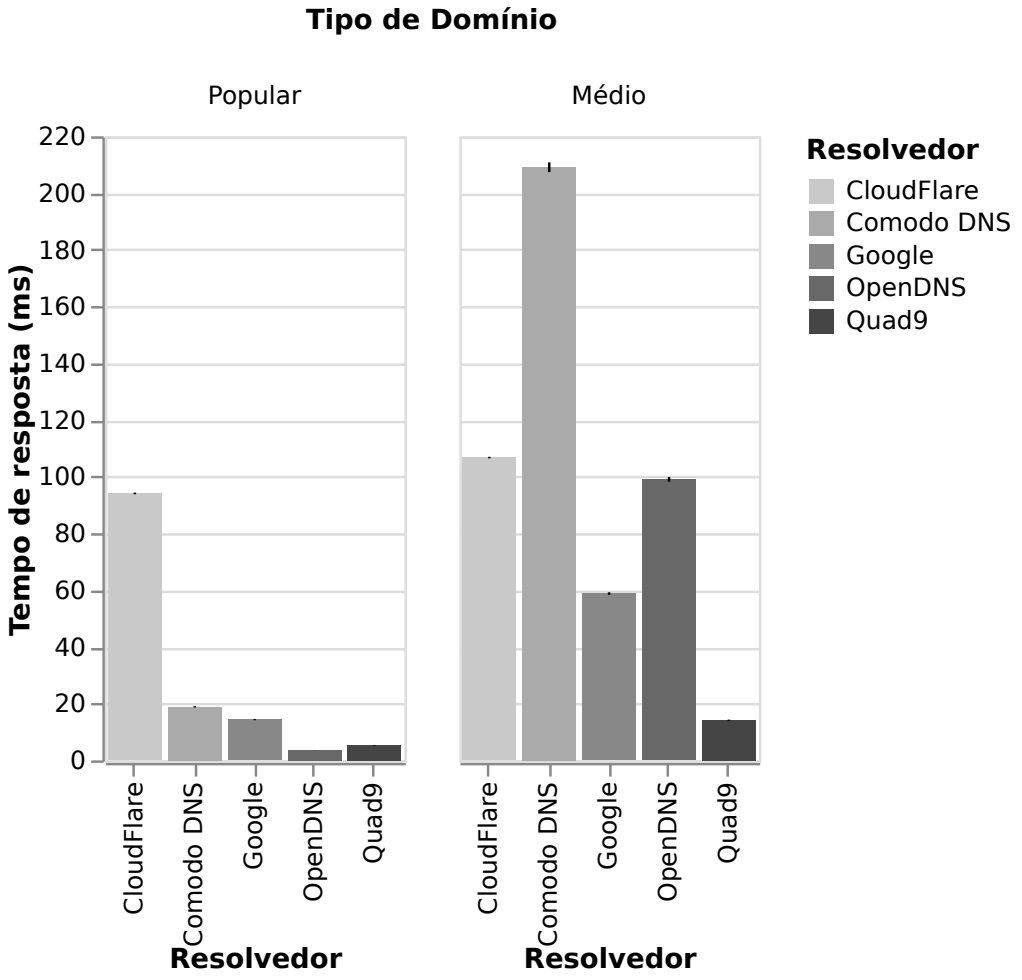


Fonte: (Autor, 2024)

Na Figura 5.2, é apresentado a comparação dos monitores no Brasil, onde o servidor resolvedor DNS OpenDNS teve melhor desempenho nos domínios populares, já o servidor resolvedor Quad9 teve melhor desempenho nos domínios médios e o servidor resolvedor Comodo DNS teve pior desempenho nos domínios médios. Já os servidores resolvedores Quad9 e OpenDNS tiveram desempenhos quase idênticos nos domínios populares.

Porém, ao analisar o servidor resolvedor Cloudflare, é possível observar uma discrepância no desempenho para ambos domínios populares e médios. No entanto, o Cloudflare é conhecido por ter um dos melhores desempenhos gerais de resolvedores de DNS públicos. Assim, é necessária uma análise mais minuciosa de quais politicas de roteamento e segurança são implementadas pelo resolvedor especificamente, visto que tais políticas podem ter impacto direto nos experimentos relacionados ao Cloudflare.

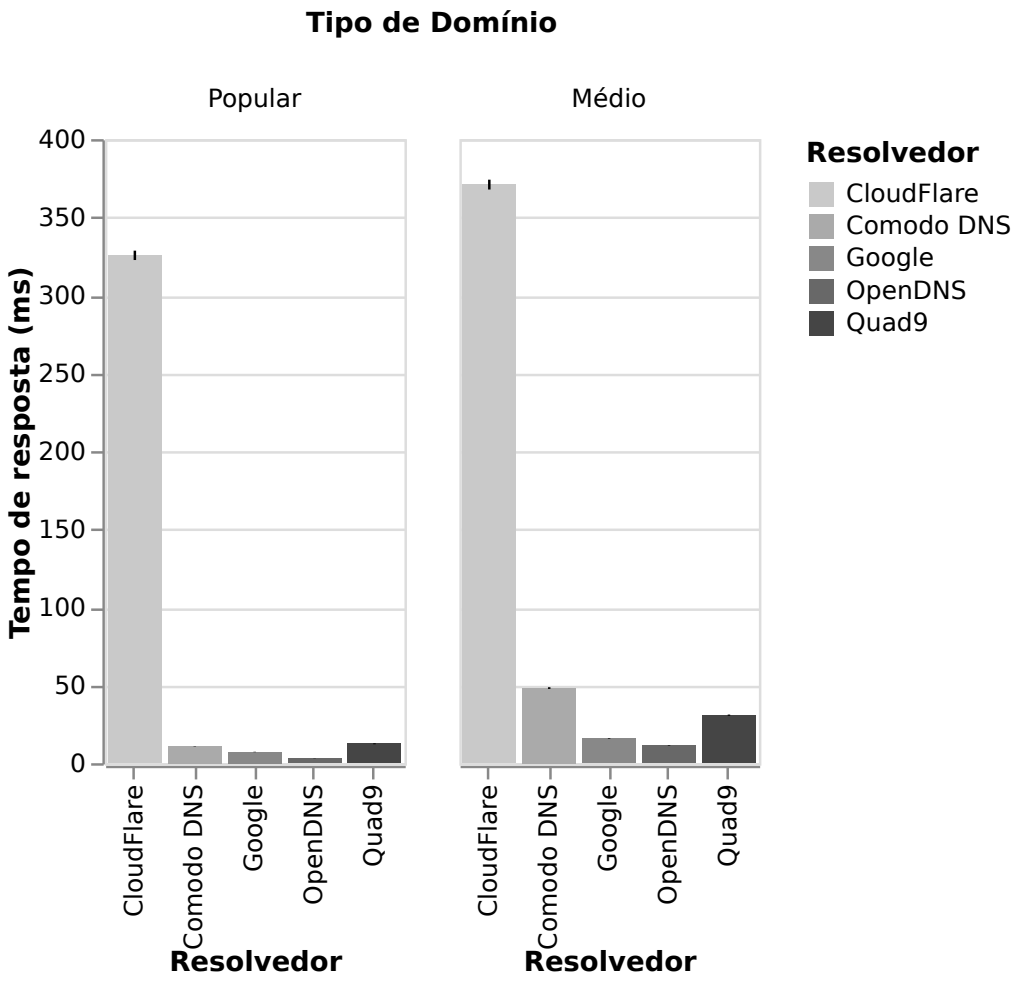
Figura 5.2 – Desempenho para Resolução de Domínios Popular e Médios por requisições do Brasil



Fonte: (Autor, 2024)

A Figura 5.3, apresenta a comparação dos resolvedores através de medições realizada por monitores localizados na Suíça. O servidor resolvedor OpenDNS teve melhor desempenho nos domínios populares e médios. Novamente, o servidor CloudFlare teve desempenho ruim nos domínios populares e médios. De acordo com estatísticas massivas disponibilizadas por empresas especializadas em monitoramento DNS e também discussão com especialistas, um tempo adequado para resolução de domínios não deve ser superior a 100 ms e, em situações normais, deve permanecer próximo dos 20 ms (PerfOps, 2023).

Figura 5.3 – Desempenho para Resolução de Domínios
Popular e Médios por requisições da Suíça



Fonte: (Autor, 2024)

Assim, além dos domínios com popularidade relevante, domínios novos e com poucos acessos também devem ser analisados para verificar o quanto a popularidade (ou a ausência dela) impacta no tempo de resolução. Os resultados da análise de domínios novos são apresentados abaixo.

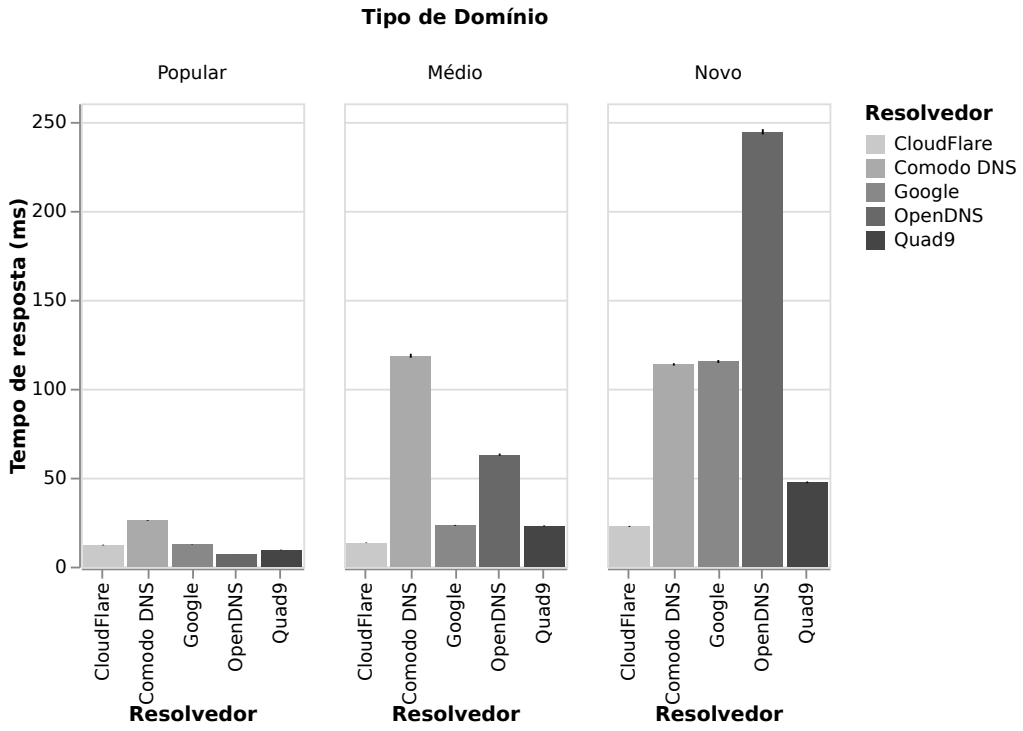
5.2 Avaliação com Novos Domínios

Depois de, analisarmos os domínios populares e médios, foi também definida uma lista de domínios novos para verificar o impacto de domínios pouco conhecidos e acessado no tempo de resolução de cada servidor. Para isso, foram criados 20 domínios em uma rede acadêmica brasileira e comparado o tempo de resolução com os demais níveis de popularidade.

As Figuras 5.4, 5.5 e 5.6, apresentam as comparações dos desempenhos dos resolvedores para domínios populares, médios e novos, para cada um dos países utilizados na coleta. Assim, os resultados permitem observar um impacto no tempo de resposta para domínios novos. Por exemplo, enquanto a média do tempo de resposta para domínios populares e médios ficou abaixo do 50 ms, a média para domínios novos ficou acima de 100 ms.

Dessa forma, as medições realizadas na Austrália (*cf.* Figure 5.4) mostram que o desempenho de todos os resolvedores foi pior para domínios novos. Portanto, nesta análise é possível ver que o OpenDNS teve um desempenho bastante inferior aos demais, mesmo sendo um resolvedor que teve uma excelente desempenho para domínios populares e médios.

Figura 5.4 – Desempenho para Resolução de Domínios Novos por requisições da Austrália

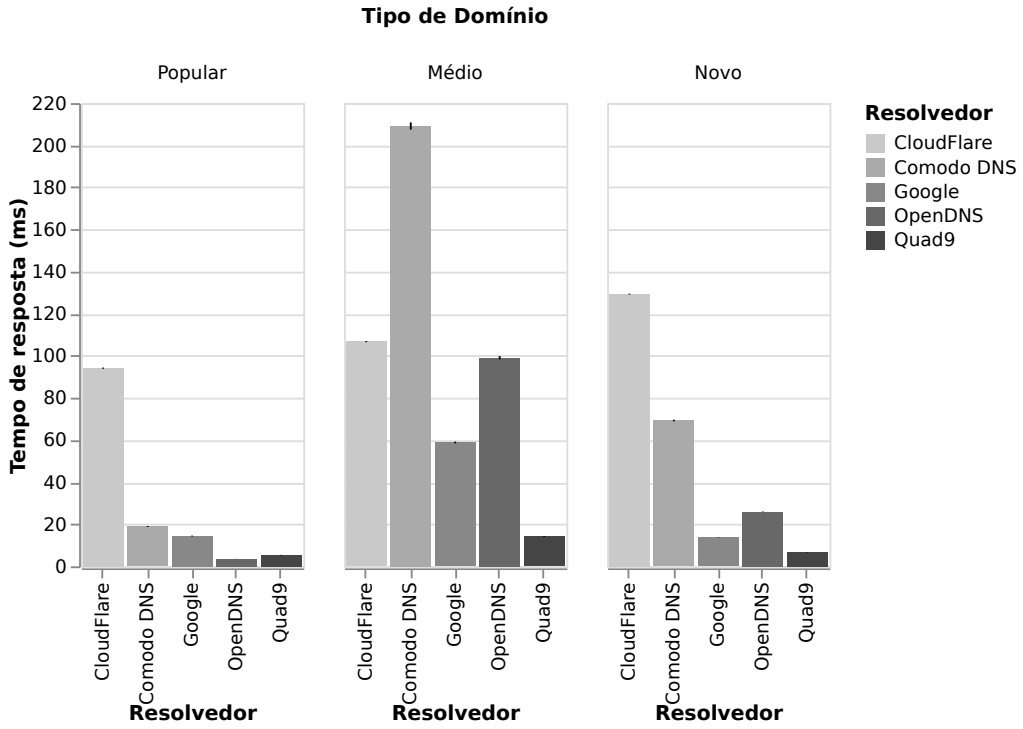


Fonte: (Autor, 2024)

Inicialmente, as medições realizados no Brasil para domínios novos (*cf.* Figura 5.5, o servidor resolvedor Quad9 obteve melhor desempenho, enquanto o servidor resolvedor CloudFlare teve a pior desempenho. Dessa forma, é importante ressaltar que todos os domínios novos possuem *.br* como Domínio de Nível de Topo de Código de País (ccTLD, em Inglês). Portanto, é esperado que, para a coleta de dados do Brasil, todos resolvedores DNS tenham a melhor desempenho para domínios novos.

Porém, isso não se mostrou verdade para o servidor resolvedor Cloudflare, que apresentou um resultado pior no Brasil do que na Austrália para tais domínios. Novamente, isto pode ser dar ao fato da Cloudflare implementar políticas de segurança que interferem nos experimentos realizados.

Figura 5.5 – Desempenho para Resolução de Domínios Novos por requisições do Brasil

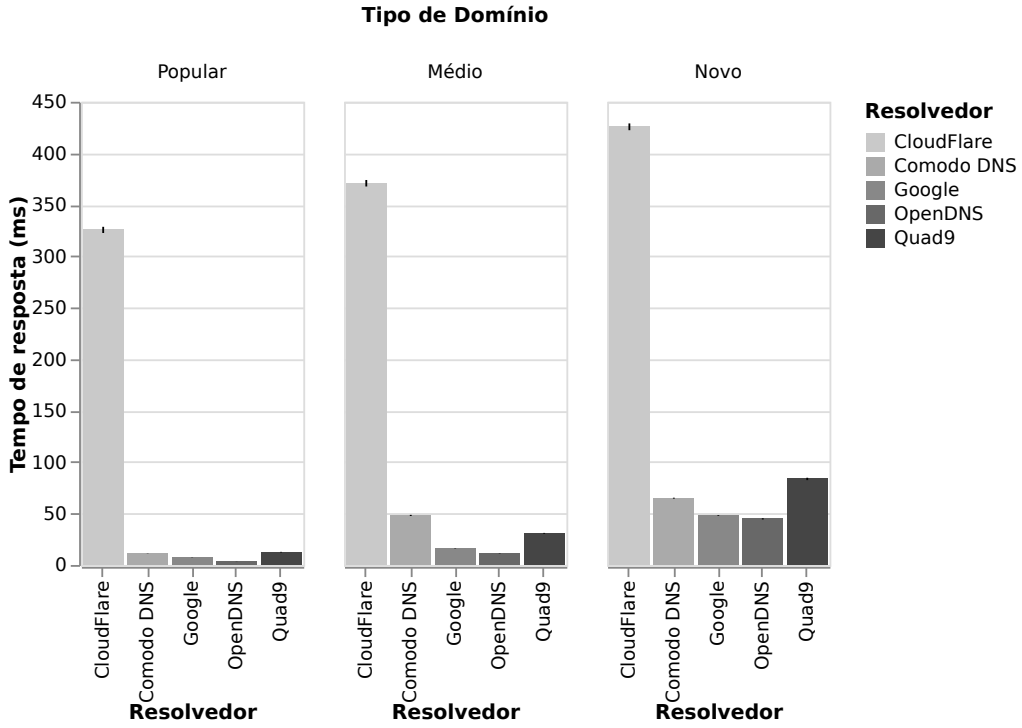


Fonte: (Autor, 2024)

Na Figura 5.6, pode ser observado que o servidor resolvedor OpenDNS teve melhor desempenho nos domínios novos quando monitorados da Suíça, enquanto o servidor resolvedor Cloudflare teve a pior desempenho para domínios novos.

Com base nos resultados obtidos, é possível ter visões sobre as diferenças de resolução de domínios de acordo com sua popularidade, bem como verificar que alguns provedores DNS lidam com as requisições de forma diferente, como, por exemplo, implementando diferentes politicas de segurança.

Figura 5.6 – Desempenho para Resolução de Domínios Novos por requisições da Suíça



Fonte: (Autor, 2024)

Assim, os experimentos realizados na Suíça e no Brasil foram executados com diferentes tipos de implementação (*e.g.*, dnsresolver e dig) e utilizando outras máquinas, inclusive dentro da rede universitária, de modo a verificar se a razão do comportamento verificado no servidor resolvedor Cloudflare pudesse estar relacionado com falhas de implementação ou limitações de máquina. Porém, os resultados não mostraram variação considerável. Por fim, é importante uma análise minuciosa não só do desempenho, mas também de outras políticas que envolvem a resolução do DNS.

5.3 Discussão

Primeiramente, os experimentos realizados mostram uma diferença considerável entre as resoluções de domínios populares vs. não populares. Assim, a geolocalização dos monitores de medição (*i.e.*, onde é realizado as requisições) impactam diretamente os domínios que são novos e que utilizam ccTLD de países com acessos internacionais pouco usuais. Por exemplo, domínios novos *.br* possuem a pior desempenho comparado com domínios mais populares quando monitoradas da Suíça e Austrália.

Além disso, foi possível verificar que, em alguns casos, os domínios médios também podem ter desempenho consideravelmente ruins. Isto se dá pelo fato de que são pouco acessados em certas localidades. Portanto, domínios populares na lista Tranco tendem a ser populares em todos os lugares analisados (*e.g.*, facebook.com, google.com e instagram.com), enquanto domínios médios (*e.g.*, shopiro.ca, freestart.hu e tabsite.com) podem ser populares em determinadas localidades e não-populares em outras.

Além disso, baseado em análises diárias, os dias da semana parecem não impactar no desempenho dos resolvedores DNS, já que todos resolvedores mantém um padrão de desempenho similar de segunda-feira até sexta-feira. Porém, as horas do dia geram algumas variações nos desempenhos. Por exemplo, nos períodos das 10:00-12:00 horas e das 14:00-16:00 horas foram verificados tempo de resposta maiores em relação a outros horários.

Dessa forma, os servidores resolvedores Cloudflare, Quad9 e Google se mantiveram estáveis, porém com alguns picos dentro desses períodos. Entretanto, os resolvedores OpenDNS e Comodo tiveram oscilações muito mais constantes durante os experimentos, chegando a ter variação de até 40% no tempo de resposta durante as diferentes horas dos dias.

As Perguntas de Pesquisa (PPs) definidas neste trabalho (*cf.* Capítulo 1) foram respondidas utilizando o PerfResolv. A PP1), que se propõe a avaliar o tempo médio de resolução geral dos resolvedores DNS públicos, foi respondida analisando o tempo de resposta de diferentes domínios em resolvedores DNS públicos em diferentes monitores. O resultado foi um tempo médio de 0,27 ms para o servidor resolvedor Quad9 que obteve melhor desempenho, seguido pelos servidores resolvedores Google com 0,32 ms, ComodoDNS 0,33 ms, OpenDNS 0,36 ms, sendo que o CloudFlare teve um pior desempenho com 165 ms.

A PP2, que procura examinar a influência do dia e da hora da semana no tempo médio, foi respondida por meio da avaliação do tempo de resposta de vários domínios em resolvedores DNS públicos, tendo como resultado, que durante o final da manhã e o meio da tarde, foram registrados tempos de resposta mais prolongados em comparação com outros horários. os resultados revelam que os dias da semana **não** exercem um impacto significativo no desempenho geral dos resolvedores DNS. Porém, as horas **sim**, exercem um impacto, existindo variações notáveis ao longo do dia.

Para responder a PP3, que visa verificar se os servidores têm tempos de resposta distintos para nomes de domínio populares, médios ou novos, foram examinados 60 domínios, dos quais 20 eram populares, 20 médios e 20 novos. Os resultados revelaram, que **sim**, de fato, os servidores apresentaram variações consideráveis nos tempos de resposta ao resolverem domínios, dependendo da sua popularidade.

No contexto da PP4, que visa verificar se a geolocalização global das consultas é um fator que impacta no tempo de resposta, a resposta foi dada ao analisar os nomes de domínios de acordo com sua popularidade em geolocalizações diferentes (*e.g.*, Austrália, Brasil e Suíça), sendo identificado, que **sim**, a geolocalização impacta no tempo de resposta dos nomes de domínio.

6 CONCLUSÃO E TRABALHOS FUTUROS

Nesta dissertação, apresentou-se o PerfResolv, uma abordagem geo-distribuída para análise de desempenho de resolvedores DNS com base na popularidade de domínios. Tal abordagem permite a coleta de métricas de desempenho (e.g., tempo de resposta), levando em consideração os domínios populares, médios e novos. Por meio de monitores localizados em três países diferentes - Brasil, Suíça e Austrália - e uma lista de 60 domínios classificados em populares, médios e novos de acordo com sua popularidade, foram conduzidos experimentos para avaliar o tempo de resposta de 5 resolvedores DNS públicos na resolução de nomes de domínio com diferentes níveis de popularidade. Os resultados obtidos a partir destes experimentos permitiram analisar se a popularidade do domínio afeta o desempenho dos servidores resolvedores DNS. Dessa forma, a abordagem PerfResolv oferece uma ferramenta para auxiliar na pesquisa e na compreensão sobre quais fatores impactam no desempenho dos resolvedores DNS, levando assim a um melhor entendimento de políticas e práticas aplicadas por tais provedores deste serviço.

Em relação aos resultados dos experimentos conduzidos, foi identificado que os resolvedores DNS analisados nos experimentos desta dissertação apresentaram tempos médios de resposta parecidos, sendo apenas um deles com desempenho fora do padrão identificado. Além disso, quanto à influência dos dias da semana no desempenho dos servidores DNS, não houve impacto significativo, mantendo um padrão similar de segunda a domingo. Entretanto, as horas do dia geraram variações no desempenho, com alguns períodos do dia (*e.g.*, 05h às 10h, 17h às 19h) apresentando tempos de resposta menores.

Relativo ao foco desta dissertação, os resultados dos experimentos realizados demonstraram uma diferença entre o tempo de resolução de domínios populares e não populares (*i.e.*, médio e novos), impactada pela localização dos monitores de medição. Dessa forma, constatou-se que domínios de média popularidade podem ter um desempenho ruim em algumas localidades devido ao baixo acesso. No contexto de domínios populares, foi identificado que tais domínios apresentam um tempo de resposta menor em todas as localizações comparado com domínios médios e novos. Isto pode indicar que resolvedores DNS públicos possuem políticas de *caching* baseado na quantidade de acessos aos domínios. Por fim, a geolocalização dos resolvedores impactou nos resultados, sendo resolvedores localizados na Suíça apresentando tempos de resposta menores para todos os níveis de popularidade em comparação com resolvedores localizados no Brasil e Austrália.

Trabalhos futuros incluem uma análise mais aprofundada do tempo de resolução de domínios não populares em diferentes resolvedores, países e ccTLD. Esta análise permite uma compreensão mais abrangente do impacto da popularidade dos domínios no desempenho dos resolvedores DNS. Além disso, é importante investigar os *trade-offs* entre segurança e desempenho, de modo a explorar medidas para melhorar a eficiência dos resolvedores sem comprometer a segurança dos usuários. Por fim, métricas adicionais, como RTT, TTL e *caching*, podem ser exploradas pelo PerfResolv a fim de obter uma visão mais completa e detalhada do desempenho dos resolvedores DNS.

REFERÊNCIAS

AFFINITO, A.; BOTTA, A.; VENTRE, G. Local and Public DNS Resolvers: do You Trade off Performance Against Security? In: **2022 IFIP Networking Conference (IFIP Networking)**. Catania, Italy: [s.n.], 2022. p. 1–9.

AGER B., M. W. S. G. . U. S. Comparing DNS Resolvers in The Wild. In: **Proceedings of the 10th ACM SIGCOMM conference on Internet measurement**. Melbourne, Australia: [s.n.], 2010. p. 15–21.

AKANHO, Y. et al. African Nameservers Revealed: Characterizing DNS Authoritative Nameservers. In: **Towards new e-Infrastructure and e-Services for Developing Countries: 12th EAI International Conference, AFRICOMM 2020, Ebène City, Mauritius, December 2-4, 2020, Proceedings 12. Springer International Publishing,**. Ebène, Mauritius: [s.n.], 2021. v. 361, n. 1, p. 327–344.

ARENDS, R. et al. **RFC4033: DNS Security Introduction and Requirements**. [S.l.], 2005. 1–21 p. <https://datatracker.ietf.org/doc/html/rfc4033>.

ARENDS, R. et al. **RFC4034: Resource Records for The DNS Security Extensions**. [S.l.], 2005. 1–29 p. <https://datatracker.ietf.org/doc/html/rfc4034>.

ARENDS, R. et al. **RFC4035: Protocol Modifications for The DNS Security Extensions**. [S.l.], 2005. 1–53 p. <https://datatracker.ietf.org/doc/html/rfc4035>.

ARIYAPPERUMA, S.; MITCHELL, C. J. Security Vulnerabilities in DNS and DNSSEC. In: **IEEE - The Second International Conference on Availability, Reliability and Security (ARES'07)**. Vienna, Austria: [s.n.], 2007. p. 335–342.

BHOWMICK, P. et al. TTL Violation of DNS Resolvers in The Wild. In: **Springer International Conference on Passive and Active Network Measurement**. Virtual Event, USA: [s.n.], 2023. p. 550–563.

BOEIRA, D. F. et al. **Traffic Centralization and Digital Sovereignty: An Analysis Under the Lens of DNS Servers**. Porto Alegre, Brazil: [s.n.], 2023. 1–8 p.

BORGOLTE, K. et al. How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in The Internet Ecosystem. In: **47th Research Conference on Communication, Information and Internet Policy**. Washington, USA: [s.n.], 2019. p. 1–9.

BROIDO, A.; NEMETH, E.; CLAFFY, K. C. Spectroscopy of DNS Update Traffic. **ACM SIGMETRICS Performance Evaluation Review**, New York, USA, v. 31, n. 1, p. 320–321, 2003.

CASTRO, S. et al. Understanding and Preparing for DNS Evolution. In: **Springer Traffic Monitoring and Analysis: Second International Workshop, TMA 2010**. Zurich, Switzerland: [s.n.], 2010. p. 1–16.

CHHABRA, R. et al. Measuring DNS-over-HTTPS Performance Around The World. In: **21st ACM Internet Measurement Conference**. Virtual Event, USA: [s.n.], 2021. p. 351–365.

DAMAS, J.; GRAFF, M.; VIXIE, P. **RFC6891: Extension Mechanisms for DNS (EDNS (0)**. [S.l.]: RFC Editor, 2013. 1–16 p. <https://datatracker.ietf.org/doc/html/rfc6891>.

DOAN, T. V.; FRIES, J.; BAJPAI, V. Evaluating Public DNS Services in The Wake of Increasing Centralization of DNS. In: **IFIP Networking Conference (IFIP Networking 2021)**. Espoo and Helsinki, Finland: [s.n.], 2021. p. 1–9.

FRANCO, M. et al. SecGrid: A Visual System for The Analysis and ML-Based Classification of Cyberattack Traffic. In: **IEEE 46th Conference on Local Computer Networks (LCN 2021)**. Edmonton, Canada: [s.n.], 2021. p. 1–8.

GAO, H. et al. Reexamining dns from a global recursive resolver perspective. **IEEE/ACM Transactions on Networking**, Texas,USA, v. 24, n. 1, p. 43–57, 2014.

HAO, S. et al. On The DNS Deployment of Modern Web Services. In: **IEEE International Conference on Network Protocols (ICNP 2015)**. San Francisco, USA: [s.n.], 2015. p. 100–110.

HERZBERG, A.; SHULMAN, H. Cipher-Suite Negotiation for DNSSec: Hop-by-Hop or End-to-End? **IEEE Internet Computing**, Piscataway, New Jersey, USA, v. 19, n. 1, p. 80–84, 2015.

HOUNSEL, A. et al. Analyzing The Costs (and Benefits) of DNS, DoT, and DoH for The Modern Web. In: **Proceedings of The Applied Networking Research Workshop**. Quebec, Canada: [s.n.], 2019. p. 20–22.

HOUNSEL, A. et al. Comparing The Effects of DNS, DoT, and DoH on Web Performance. In: **WWW '20: Proceedings of The Web Conference**. New York, USA: [s.n.], 2020. p. 562–572.

HOURS, H. et al. A Study of The Impact of DNS Resolvers on CDN Performance Using a Causal Approach. **Computer Networks Elsevier**, Virtual Event, USA, v. 109, p. 200–210, 2016.

HYNEK, K. et al. Summary of DNS over Https Abuse. **IEEE Access**, Virtual Event, USA, v. 10, p. 54668–54680, 2022.

JAIN, R. **The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling**. New York, USA: [s.n.], 1991. 1–720 p.

KARP, P. **RFC0226: Standardization of Host Mnemonics**. [S.l.], 1971. 1–1 p. <=>https://www.rfc-editor.org/info/rfc226.

KOSEK, M. et al. DNS Privacy With Speed? Evaluating DNS over QUIC and its Impact on Web Performance. In: **22nd ACM Internet Measurement Conference**. Nice, France: [s.n.], 2022. p. 44–50.

KOSHY, A. M. et al. An Insight Into Encrypted DNS Protocol: DNS over TLS. In: **IEEE - 2021 4th International Conference on Recent Developments in Control, Automation Power Engineering (RDCAPE)**. Noida, India: [s.n.], 2021. p. 379–383.

KURIHARA, J.; TANAKA, T.; KUBO, T. ODNS: A Distributed Approach to DNS Anonymization With Collusion Resistance. **Computer Networks, Elsevier**, Tokyo, Japan, v. 237, p. 1–14, 2023.

KWON, J. et al. PsyBoG: A Scalable Botnet Detection Method for Large-Scale DNS Traffic. **Elsevier Computer Networks 2016**, Virtual Event, USA, v. 97, p. 48–73, 2016.

LAI, T.-L.; TSAI, M.-H. Design and Implementation of a DNS Server With Geolocation Capability. In: **22nd Asia-Pacific Network Operations and Management Symposium (APNOMS 2021)**. Tainan, Taiwan: [s.n.], 2021. p. 370–373.

Le Pochat, V. et al. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: **26th Network and Distributed System Security Symposium (NDSS 2019)**. San Diego, USA: [s.n.], 2019. p. 1–15.

LEINER, B. M. et al. A Brief History of The Internet. **ACM SIGCOMM Computer Communication Review**, New York, USA, v. 39, n. 5, p. 22–31, 2009.

MILLS, D. **RFC0799: Internet Name Domains**. [S.l.]: RFC Editor, 1981. 1–6 p. <https://datatracker.ietf.org/doc/rfc799/>.

MOCKAPETRIS, P. **RFC0882: Domain Names: Concepts and Facilities**. [S.l.]: RFC Editor, 1983. 1–31 p. <https://datatracker.ietf.org/doc/html/rfc882>.

MOCKAPETRIS, P. **RFC0883: Domain Names: Implementation Specification**. [S.l.]: RFC Editor, 1983. 1–73 p. <https://datatracker.ietf.org/doc/html/rfc883>.

MOCKAPETRIS, P.; DUNLAP, K. J. Development of The Domain Name System. In: **SIGCOMM '88 Symposium Proceedings on Communications Architectures and Protocols**. Stanford, USA: [s.n.], 1988. p. 123–133.

MOCKAPETRIS, P. V. **RFC1034: Domain Names - Concepts and Facilities**. [S.l.]: RFC Editor, 1987. 1–54 p. <https://datatracker.ietf.org/doc/html/rfc1034>.

MOCKAPETRIS, P. V. **RFC1035: Domain Names - Implementation and Specification**. [S.l.]: RFC Editor, 1987. 1–54 p. <https://datatracker.ietf.org/doc/html/rfc1035>.

MOURA, G. C. et al. Clouding Up The Internet: How Centralized is DNS Traffic Becoming? In: **IMC '20: Proceedings of the ACM Internet Measurement Conference**. Virtual Event, USA: [s.n.], 2020. p. 42–49.

OTTO J. S., S. M. A. R. J. P.-. B. F. E. Content Delivery and The Natural Evolution of DNS: Remote DNS Trends, Performance Issues and Alternative Solutions. In: **Proceedings of the 2012 Internet Measurement Conference**. Boston, USA: [s.n.], 2012. p. 523–536.

PARK, J. et al. Where Are You Taking Me? Behavioral Analysis of Open DNS Resolvers. In: **49th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2019)**. Portland, USA: [s.n.], 2019. p. 493–504.

PerfOps. **DNSPErf - DNS Performance Analytics and Comparison**. 2023. <https://www.dnsperf.com>.

POSTEL, J.; REYNOLDS, J. K. **RFC0920: Domain Requirements**. [S.l.], 1984. 1–14 p. <https://datatracker.ietf.org/doc/html/rfc920>.

RADU, R.; HAUSDING, M. Consolidation in The DNS Resolver Market–How Much, How Fast, How Dangerous? **Journal of Cyber Policy - Taylor & Francis**, Sheffield, United Kingdom, v. 5, n. 1, p. 46–64, 2020.

REGAN, G.; ABDEL-HALIM, A. Internet of Things Security Domain Name System Policy and Analytics. Virtual Event, USA, p. 1–9, 2018.

REKHTER, Y. et al. **RFC1918: Address Allocation for Private Internets**. [S.l.]: RFC Editor, 1996. 1–9 p. <https://datatracker.ietf.org/doc/html/rfc1918>.

ROSS, R. **One History of DNS**. [S.l.]: Byte.org, 2006. 1–35 p. <http://www.byte.org/one-history-of-dns.pdf>.

RULA, J. P.; BUSTAMANTE, F. E. Behind The Curtain: Cellular DNS and Content Replica Selection. In: **IMC '14: Proceedings of the 2014 Conference on Internet Measurement Conference**. Vancouver, Canada: [s.n.], 2014. p. 59–72.

SAHA, S. et al. YODA: Covert Communication Channel Over Public DNS Resolvers. In: **Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)**. Porto, Portugal: [s.n.], 2023. p. 252–260.

SHREEDHAR, T. et al. Evaluating QUIC Performance over Web, Cloud Storage, and Video Workloads. **IEEE Transactions on Network and Service Management**, Virtual Event, USA, v. 19, n. 2, p. 1366–1381, 2021.

SILVA, M. A. et al. **Repositório PerfResolv - Código Fonte**. Porto Alegre, Brazil: [s.n.], 2023. <https://github.com/ComputerNetworks-UFRGS/PerfResolv>.

SU, Z.; POSTEL, J. **RFC0819: Domain Naming Convention for Internet User Applications**. [S.l.]: RFC Editor, 1982. 1–17 p. <https://datatracker.ietf.org/doc/html/rfc819>.

TOORN, O. V. D. et al. Addressing the Challenges of Modern DNS a Comprehensive Tutorial. **Elsevier Computer Science Review**, Amsterda, Netherlands, v. 45, p. 1–37, 2022.

VIXIE, P. **RFC1996 A Mechanism for Prompt Notification of Zone Changes (DNS Notify)**. [S.l.], 1996. 1–6 p. <https://datatracker.ietf.org/doc/html/rfc1996>.

VIXIE, P. **RFC2671: Extension Mechanisms for DNS (EDNS0)**. [S.l.], 1999. 1–7 p. <https://datatracker.ietf.org/doc/html/rfc2671>.

VRIES W. B., A. S. . v. R.-D. R. D. Global-Scale Anycast Network Management With Verfploeter. In: **NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium**. Budapest, Hungary: [s.n.], 2020. p. 1–9.

YAN, Z. et al. Is DNS Ready for Ubiquitous Internet of Things? **IEEE Access 7**, Virtual Event, USA, v. 7, p. 28835–28846, 2019.

ZEMBRUZKI, L.; JACOBS, A. S.; GRANVILLE, L. Z. On The Consolidation of The Internet Domain Name System. In: **IEEE Global Communications Conference (GLOBECOM 2022)**. Rio de Janeiro, Brazil: [s.n.], 2022. p. 2122–2127.

ZEMBRUZKI, L. et al. Measuring Centralization of DNS Infrastructure in The Wild. In: **34th International Conference on Advanced Information Networking and Applications (AINA-2020)**. Caserta, Italy: [s.n.], 2020. p. 871–882.

APÊNDICE A — ARTIGO PUBLICADO – ERRC 2023

SILVA, Marcelo A.; FRANCO, Muriel F.; SCHEID, Eder J.; ZEMBRUZKI, Luciano; GRANVILLE, Lisandro Z.. Desempenho de Resolvedores de DNS Públicos: Uma Análise do Estado da Arte. In: ESCOLA REGIONAL DE REDES DE COMPUTADORES (ERRC), 20. , 2023, Porto Alegre/RS. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2023 . p. 43-48. DOI: https://doi.org/10.5753/errc.2023.912.

- **Título:** *Desempenho de Resolvedores de DNS Públicos: Uma Análise do Estado da Arte*
- **Resumo:** O Sistema de Nomes de Domínio (DNS) representa um dos sistemas centrais para a operação da Internet. Neste artigo, apresentamos uma análise da pesquisa sobre a medição do desempenho de resolvedores públicos de DNS nos últimos cinco anos. Assim, este trabalho fornece uma visão geral do estado da arte sobre os métodos utilizados para análise do desempenho de resolvedores DNS públicos, indicando o estado atual, direções e oportunidades de pesquisa.
- **Estado:** Publicado
- **Qualis:** -
- **Conferência:** 20ª Escola Regional de Redes de Computadores (ERRC 2023)
- **Data:** 23 de Outubro - 25 de Outubro, 2023
- **Local:** Porto Alegre, RS, Brasil
- **URL:** <https://sol.sbc.org.br/index.php/errc/article/view/26003>
- **Digital Object Identifier (DOI):** <https://doi.org/10.5753/errc.2023.912>

Desempenho de Resolvedores de DNS Públicos: Uma Análise do Estado da Arte

Marcelo A. Silva, Muriel F. Franco, Eder J. Scheid, Luciano Zembruzki, Lisandro Z. Granville

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
{marceloalmeida.silva, mffranco, ejscheid, lzembruzki, granville}@inf.ufrgs.br

Abstract. *The Domain Name System (DNS) represents one of the central systems for Internet operation. In this article, we present an analysis of research on the performance measurement of Public DNS Resolvers over the last five years. In this work, we provide an overview of the state of the art of the method for analysis of Public DNS resolvers, thus helping to understand the current state, directions, and opportunities for the research field.*

Resumo. *O Sistema de Nomes de Domínio (DNS) representa um dos sistemas centrais para a operação da Internet. Neste artigo, apresentamos uma análise da pesquisa sobre a medição do desempenho de resolvedores públicos de DNS nos últimos cinco anos. Assim, este trabalho fornece uma visão geral do estado da arte sobre os métodos utilizados para análise do desempenho de resolvedores DNS públicos, indicando o estado atual, direções e oportunidades de pesquisa.*

1. Introdução

A Internet é um componente essencial para empresas e pessoas, simplificando tarefas e facilitando a comunicação em todo o mundo. O Sistema de Nomes de Domínio (DNS, do Inglês *Domain Names System*) desempenha um papel essencial na Internet, traduzindo nomes de domínio legíveis para humanos em endereços *Internet Protocol (IP)*. O desempenho do DNS é crucial para suprir serviços da Internet, como, por exemplo, o acesso a páginas Web e a localização de arquivos em endereços eletrônicos de forma rápida e intuitiva. Para suprir tais serviços de maneira eficaz, a resolução de domínios podem serem realizados por *(i)* servidores resolvedores DNS privados, remunerados pelos serviços prestados, garantindo a proteção aos usuários, desempenho e privacidade ou por *(ii)* Servidores resolvedores DNS públicos, os quais não possuem custos e também entregam um alto grau de segurança e eficiência [Borgolte et al. 2019].

Os servidores de DNS públicos são geralmente fornecidos por grandes provedores da Internet (*e.g*, Google, Cloudflare e Quad9). Tais provedores oferecem resolução de nomes gratuita e segura, incluindo recursos de segurança para identificar domínios maliciosos [Affinito et al. 2022]. Geralmente, resolvedores públicos apresentam desempenho superior, com tempo de resposta inferior, a DNS privados. No entanto, a crescente centralização de serviços, fluxos de rede e infraestrutura associados a esses provedores preocupa a academia, indústria e sociedade [Zembruzki et al. 2022, Boeira et al. 2023]. Além disso, a terceirização de serviços para provedores de DNS públicos sem medidas eficazes de segurança pode expor os usuários a riscos, afetando negativamente a resolução de nomes em casos de ataques maliciosos, como ataques de amplificação e de negação

APÊNDICE B — ARTIGO PUBLICADO – AINA 2024

SILVA, Marcelo A.; FRANCO, Muriel F.; SCHEID, Eder J.; ZEMBRUZKI, Luciano; GRANVILLE, Lisandro Z.. PerfResolv: A Geo-Distributed Approach for Performance Analysis of Public DNS Resolvers Based on Domain Popularity. In: INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS (AINA), 38., 2024, Kitakyushu, Japan. p. 1-12.

- **Título:** *PerfResolv: A Geo-Distributed Approach for Performance Analysis of Public DNS Resolvers Based on Domain Popularity*
- **Resumo:** The Domain Name System (DNS) represents one of the cornerstones of the World Wide Web and plays an indispensable role in its operation. DNS is an extensive distributed database structured to resolve readable domain names for people, companies, and institutions into corresponding and reliable IP addresses. This paper presents PerfResolv, an approach for performance analysis on public DNS resolver servers (e.g., Google, Cloudflare, OpenDNS, Quad9, and ComodoDNS). The analysis was performed with PerfResolv located at geographically distributed points in three different countries: Brazil, Switzerland, and Australia. The results were obtained considering the response time for resolving domain names with different popularity levels to verify if and how geolocation, domain name popularity, week, day, and time affect the performance of DNS resolver servers. The results show considerable fluctuations in the response time of some DNS resolvers, with a variation of up to 40% in response time across different hours of the day. Further, there are differences between the resolution time of popular and unpopular domains, which are also influenced by the geolocation of the measurement monitors.
- **Estado:** Publicado
- **Qualis:** A3
- **Conferência:** 38th International Conference on Advanced Information Networking and Applications (AINA 2024)
- **Data:** 17 de Abril - 19 de Abril, 2024
- **Local:** Kitakyushu, Japan
- **URL:** A ser publicado.
- **Digital Object Identifier (DOI):** A ser publicado.

PerfResolv: A Geo-Distributed Approach for Performance Analysis of Public DNS Resolvers Based on Domain Popularity

Marcelo Almeida Silva, Muriel Figueredo Franco, Eder John Scheid,
Luciano Zembruzki, Lisandro Zambenedetti Granville

Abstract The Domain Name System (DNS) represents one of the cornerstones of the World Wide Web and plays an indispensable role in its operation. DNS is an extensive distributed database structured to resolve readable domain names for people, companies, and institutions into corresponding and reliable IP addresses. This paper presents PerfResolv, an approach for performance analysis on public DNS resolver servers (e.g., Google, Cloudflare, OpenDNS, Quad9, and ComodoDNS). The analysis was performed with PerfResolv located at geographically distributed points in three different countries: Brazil, Switzerland, and Australia. The results were obtained considering the response time for resolving domain names with different popularity levels to verify if and how geolocation, domain name popularity, week, day, and time affect the performance of DNS resolver servers. The results show considerable fluctuations in the response time of some DNS resolvers, with a variation of up to 40% in response time across different hours of the day. Further, there are differences between the resolution time of popular and unpopular domains, which are also influenced by the geolocation of the measurement monitors.

1 Introduction

The Internet has become indispensable due to the importance of its applications and possibilities of use in different sectors of industry, government, and entertainment. The Domain Name System (DNS) represents one of the foundations of the Internet, playing an indispensable role in its operation. The DNS works a large, distributed, and structured database for resolving readable domain names into corresponding and valid Internet Protocol (IP) addresses [16]. The creation of DNS began in the 1980s, with the emergence of the Advanced Research Projects Agency Network (ARPANET) [14]. The DNS concepts and standards were published in Request for Comments (RFC) 882 and 883, updated later in RFCs 1034 and 1035. These standards are still relevant today and widely used [12].

Different DNS protocol approaches and implementations make it possible to offer users varying levels of performance and security. DNS is also used as an instrument for doing business, with various organizations offering domain resolution as

Institute of Informatics (INF) – Federal University of Rio Grande do Sul (UFRGS)
Porto Alegre, Brazil
E-mail: [marceloalmeida.silva, mffranco, ejscheid, lzembruzki, granville]@inf.ufrgs.br