# O que é um servidor de DNS?

Quando os usuários digitam nomes de domínio na barra de URL do navegador, os servidores de DNS são responsáveis pela tradução desses nomes de domínio em endereços de IP numéricos, levando-os ao site correto.

**Glossário de DNS**

Copiar o link do artigo

# O que é um servidor de DNS?

O Domain Name System (DNS) é a lista telefônica da Internet. Quando os usuários digitam nomes de domínio como 'google.com' ou 'nytimes.com' nos navegadores da web, o DNS é responsável por encontrar o endereço de IP correto para esses sites. Os navegadores então usam esses endereços para se comunicar com os servidores de origem ou com os servidores de borda da CDN para acessar as informações do site. Tudo isso acontece graças aos servidores de DNS: máquinas dedicadas para responder às solicitações ao DNS.

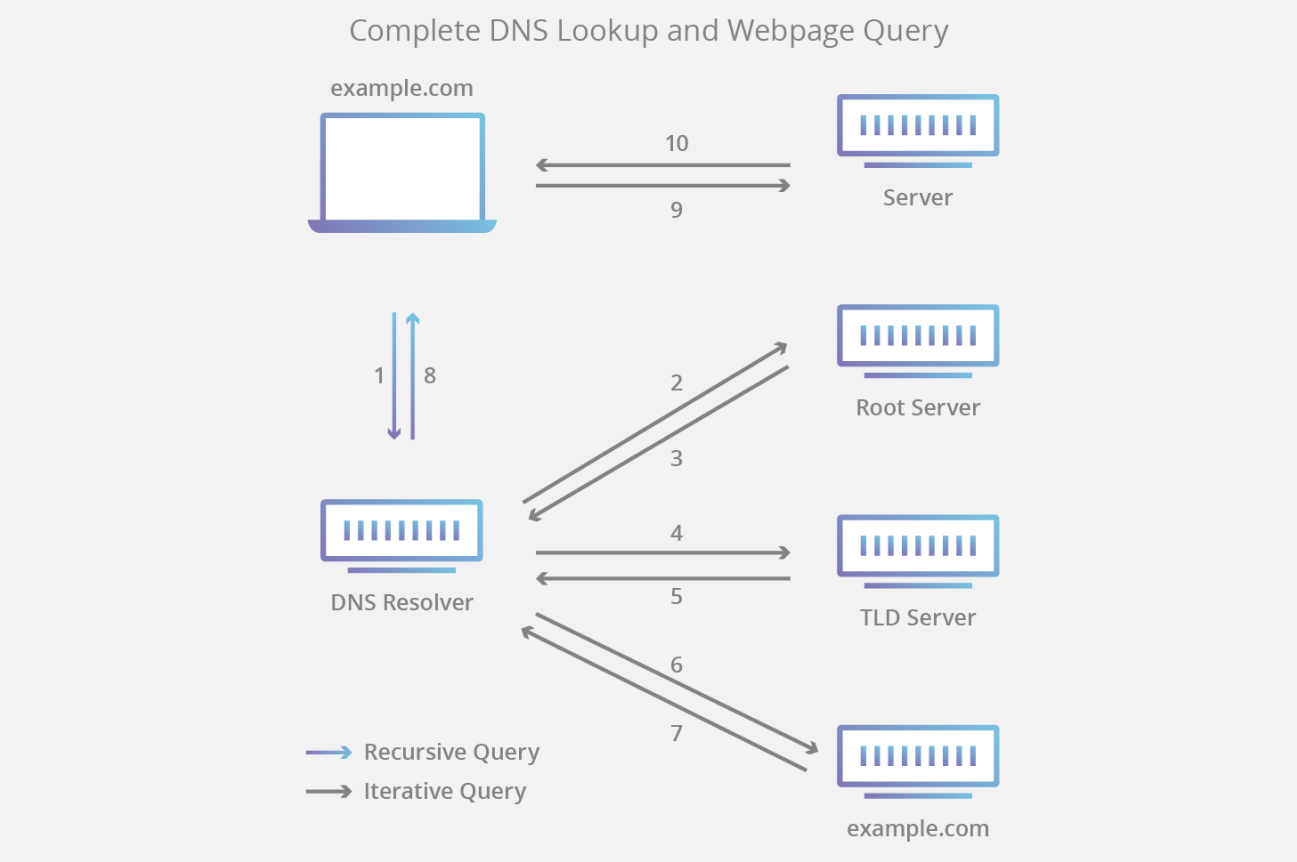
# O que é um servidor?

Um servidor é um dispositivo ou programa dedicado à prestação de serviços para outros programas, chamados de "clientes". Os clientes DNS, que são integrados à maioria dos sistemas operacionais modernos dos desktops e de dispositivos móveis, permitem que os navegadores web interajam com os servidores de DNS. Para obter mais informações, veja O Modelo Cliente-Servidor.

# Como os servidores de DNS resolvem uma consulta DNS?

Em uma consulta DNS típica sem nenhum armazenamento em cache, existem quatro servidores que trabalham juntos para enviar um endereço de IP ao cliente: resolvedores recursivos, nameservers raiz, nameservers TLD, e nameservers autoritativos.

O recursor DNS (também chamado de resolvedor DNS) é um servidor que recebe a consulta do cliente DNS e depois interage com outros servidores de DNS para buscar o IP correto. Depois de receber a solicitação do cliente, o resolvedor então realmente se comporta como um cliente, consultando os outros três tipos de servidores de DNS em busca do IP correto.




Primeiro o resolvedor consulta o nameserver raiz. O servidor raiz é o primeiro passo na tradução (resolução) de nomes de domínio legíveis por seres humanos em endereços de IP. O servidor raiz então responde ao resolvedor com o endereço de um servidor de DNS de domínio de topo(TLD) (como .com ou .net) que armazena as informações para seus domínios.

Em seguida, o resolvedor consulta o servidor TLD. O servidor TLD responde com o endereço de IP do nameserver autoritativo do domínio. O recursor então consulta o nameserver autoritativo, que responderá com o endereço de IP do servidor de origem.

Por fim, o resolvedor passará o endereço de IP do servidor de origem de volta para o cliente. Usando esse endereço de IP, o cliente pode então iniciar uma consulta diretamente ao servidor de origem, e o servidor de origem responderá enviando dados do site que podem ser interpretados e exibidos pelo navegador da web.

## O que é o armazenamento de DNS em cache?

Além do processo descrito acima, os resolvedores recursivos também podem resolver consultas DNS usando dados em cache. Depois de recuperar o endereço de IP correto para um determinado site, o resolvedor então armazenará essa informação em seu cache por um período limitado de tempo. Durante esse período de tempo, se qualquer outro cliente enviar solicitações para esse nome de domínio, o resolvedor pode pular o processo normal de busca no DNS e simplesmente responder ao cliente com o endereço de IP salvo no cache.

Uma vez expirado o prazo de armazenamento em cache, o resolvedor deve recuperar novamente o endereço de IP, criando uma nova entrada em seu cache. Esse limite de tempo, denominado tempo até entrar no ar (TTL) é definido explicitamente nos registros DNS para cada site. Normalmente, o TTL situa-se na faixa de 24-48 horas. É necessário um TTL porque os servidores web ocasionalmente mudam seus endereços de IP, de modo que os resolvedores não podem informar o mesmo IP do cache indefinidamente.

## O que acontece quando os servidores de DNS falham?

Os servidores de DNS podem falhar por várias razões, como quedas de energia, ataques cibernéticos e mau funcionamento de hardware. Nos primeiros tempos da internet, as quedas de energia dos servidores DNS podiam ter um impacto relativamente grande. Felizmente, hoje em dia há muita redundância incorporada ao DNS. Por exemplo, há muitos exemplos de servidores de DNS raiz e servidores de nomes TLD, e a maioria dos provedores tem resolvedores recursivos de backup para seus usuários. (Usuários individuais também podem usar resolvedores DNS públicos, como o 1.1.1.1. da Cloudflare) A maioria dos sites populares também tem múltiplas instâncias de seus nameservers autoritativos.

No caso de uma grande interrupção do servidor de DNS, alguns usuários podem sofrer atrasos devido à quantidade de solicitações sendo tratadas por servidores de backup, mas seria necessária uma interrupção do DNS de proporções muito grandes para tornar uma parte significativa da internet indisponível. (Isso realmente aconteceu em 2016 quando o provedor

de DNS Dyn sofreu um dos maiores ataques DDoS da história). A Cloudflare oferece um serviço de DNS gerenciado com segurança de DNS integrada destinado a proteger os servidores de DNS contra ataques e contra outras fontes comuns de falha de servidores.

## CONTEÚDO RELACIONADO

**DNS Anycast**

**Ataque de amplificação de DNS**

**Envenenamento de cache de DNS**

**Inundação de DNS**

**DNS**