# A Guide to Changing DNS Servers on Your System

*Note: Make sure you have the appropriate permissions to modify files and execute scripts on your Linux system.*

A DNS (Domain Name System) server is responsible for translating human-readable domain names (e.g., www.example.com) into IP addresses that computers can understand, enabling internet communication by resolving domain names to their corresponding IP addresses.

## DNS server IP addresses that you can use:

Google Public DNS:
IPv4: **8.8.8.8, 8.8.4.4**

Cloudflare DNS:
IPv4: **1.1.1.1, 1.0.0.1**

OpenDNS:
IPv4: **208.67.222.222, 208.67.220.220**

Quad9:
IPv4: **9.9.9.9, 149.112.112.112**

Level3 (CenturyLink):
IPv4: **209.244.0.3, 209.244.0.4**

Norton ConnectSafe:
IPv4: **199.85.126.10, 199.85.127.10**

***The availability and performance*** of DNS servers can vary based on several factors, including network infrastructure, geographical location, and server load.

The DNS servers mentioned earlier, such as *Google Public DNS, Cloudflare DNS, OpenDNS, Quad9, Level3, and Norton ConnectSafe*, are widely used and generally known for their reliability and speed. These providers invest in robust infrastructure and employ techniques like Anycast routing to ensure efficient routing and quick response times. They often have multiple data centers distributed globally to minimize latency and improve availability.

However, it's important to note that even reputable DNS providers can experience occasional outages or performance issues due to various reasons, including network disruptions, maintenance, or attacks. It's recommended to have a backup DNS server configured or use a secondary DNS provider to ensure continuity of service.

***Data tracking and mining:***DNS servers play a crucial role in internet communication, but they also have the potential to collect and track user data. When you use a DNS server, it can log information about your queries, including the domain names you visit. This data can be used for various purposes, such as troubleshooting, analytics, and potentially even targeted advertising.

Data tracking and mining by DNS servers raise concerns about privacy and potential misuse of personal information. Some DNS providers have implemented privacy-focused measures to address these concerns. For example, Cloudflare's 1.1.1.1 DNS service claims not to log any personally identifiable information (PII) and purges all logs within 24 hours. Similarly, Quad9 and OpenDNS offer options that prioritize privacy and security!!!

However, it's important to understand that DNS servers sit in the path of your internet traffic, and even with privacy measures in place, there is still potential for data collection by other entities, such as internet service providers (ISPs) or websites themselves.

*DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) protocols have been introduced to enhance privacy and encS rypt*

DNqueries, making it harder for intermediaries to intercept or track the data.

To further protect your privacy, you can use a Virtual Private Network (VPN) service, which encrypts your internet traffic and can help mask your DNS queries from your ISP or other potential trackers.

In conclusion, the availability and performance of DNS servers can vary, but reputable providers mentioned earlier strive to offer reliable and fast service. However, it's essential to be mindful of data tracking and mining potential associated with DNS queries. While some DNS providers prioritize privacy, additional measures such as DoH, DoT, or using a VPN can further enhance your privacy and mitigate potential data tracking risks.

## *Guide:*

1.Change this file type to executable on Linux, first navigate to the directory where the script file is located using the "cd" command in the terminal.

2.Verify the current file permissions using the "ls -l" command and ensure the script file has the necessary executable permissions (e.g., -rwxr-xr-x).

3.If the permissions are not set correctly, use the "chmod" command to modify them. For example, you can run "chmod +x change_dns.sh" to make the script executable.

4.Once the file permissions are set, you can execute the script by typing "./change_dns.sh" in the terminal, ensuring to include the "./" prefix to specify the current directory.

5.Press Enter to run the script, and the DNS server configuration will be updated accordingly.