DNS - Domain Name Server

Article URL
DNS - Domain Name Server

Author
SecurityHome.eu

Published: 26 September 2026

Last updated on 25 November 2026.

Â

The DNS (Domain Name Server) you use can have a influence on your privacy.
It translate the name of the website you want to visit, in to a IP-address.
Like www.yahoo.com = 87.248.114.12

These DNS servers knows (almost) all the sites you visit, because your PC ask what the IP address for each site is.
They might also filter it. For example they might take a domain name that is used for malware, or for illegal movie downloads,
and give the IP-address for a police site instead.
Sometimes you want this, for example, like filtering adult sites for a family PC.

So it is important to know what DNS servers you use.
Your PC (or modem) usually get these DNS servers via DHCP-request (Dynamic Host Configuration Protocol) from your internet provider.
Mostly this is ok, But on public (WIFI-)networks, it might be dangerous. It might be rogue DNS servers.

Also remember that your internet provider might still block site on IP-basis, not only block them on their DNS-servers.
So even if you get the correct IP-address from another DNS-server, you still don't have access.
You'll need a VPN to work around that.

Some countries, including several European countries,
block access to several DNS-servers.
Because they don't want to block specific websites.
Again a VPN, can be a workaround.

DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT)

DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) are both protocols that sends DNS lookups using encrypted HTTPS requests instead of plain-text DNS,
which helps prevent eavesdropping and tampering by anyone who can see the traffic in between. (Internet provider or public WIFI network, ...)

When your DNS-server provides this option, use it !

DNS over HTTPS (DoH) sends DNS queries over the HTTP/2 protocol, while DNS over TLS (DoT) uses the TLS protocol directly over TCP port 853.
Both methods encrypt DNS queries to enhance privacy and security, but they operate at different layers of the network

You can configure your browser to use a secure DNS server, even a different one for each browser.
Or set in on the OS-level.

Linux new way :

edit */etc/systemd/resolved.conf*

[Resolve]
DNS=8.8.8.8 8.8.4.4
FallbackDNS=1.1.1.1

check with
resolvectl status

Linux old way :

edit */etc/resolv.conf*

nameserver 1.1.1.1 #Cloudflare
nameserver 1.0.0.1 #Cloudflare
nameserver 8.8.8.8 #Google

Always add at least 2, a primary and a secondary, in case the primary goes down.
But you can add more.

Chromium
chrome://settings/security
Settings > Privacy and Security > Use Secure DNS

Brave
brave://settings/security
Settings > Privacy and Security > Use Secure DNS

Firefox
about:preferences#privacy
Settings > Privacy and Security > DNS over HTTPS

Public DNS servers:

* *Google Public DNS*

(USA)
Primary DNS: 8.8.8.8
Secondary DNS: 8.8.4.4
Features: Known for speed and reliability, it supports DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) for secure communication. It also integrates with Google's Safe Browsing to block malicious websites.

*
DNS4EU

more filtered (Europe)
86.54.11.100 86.54.11.200
2a13:1001::86:54:11:100 2a13:1001::86:54:11:200

*
Cloudflare DNS

(USA)
Primary DNS: 1.1.1.1
Secondary DNS: 1.0.0.1
Features: Offers the fastest DNS resolution globally, with a strong focus on privacy (no logging of user data). It supports DoH and DoT for encrypted connections.

*
OpenDNS

Primary DNS: 208.67.222.222
Secondary DNS: 208.67.220.220
Features: Provides robust security by blocking phishing and malware sites. It also offers parental controls and customizable filtering options.

*
Quad9

(Switzerland)
Primary DNS: 9.9.9.9
Secondary DNS: 149.112.112.112
Features: Focuses on security by blocking access to malicious domains using a constantly updated threat intelligence database. It supports encrypted DNS queries via DoH and DoT.

*
AdGuard DNS

Primary DNS: 94.140.14.14
Secondary DNS: 94.140.15.15
Features: Known for its ad-blocking capabilities, it also blocks trackers and phishing attempts, ensuring a cleaner and safer browsing experience.

*

Alternate DNS

Primary DNS: 76.76.19.19
Secondary DNS: 76.223.122.150
Features: Blocks ads and malicious websites, providing a secure and private browsing experience.

*

CleanBrowsing

Primary DNS: 185.228.168.9
Secondary DNS: 185.228.169.9
Features: Designed for family-friendly browsing, it blocks adult content and offers customizable filtering options.

*

OpenNIC

Primary DNS: 216.87.84.211
Secondary DNS: 23.90.4.6
Features: A decentralized, community-driven DNS service that provides uncensored access to the internet.

*

Verisign DNS

(USA)
Primary DNS: 64.6.64.6
Secondary DNS: 64.6.65.6
Features: Offers high reliability and security, focusing on stability and privacy without logging user data.

*

Control D

(Canada)
Primary DNS: 76.76.2.0
Secondary DNS: 76.76.10.0
Features: Provides advanced customization options, blocks malicious websites, and supports encrypted DNS queries.

*

UncensoredDNS

Primary DNS: 91.239.100.100
Secondary DNS: 89.233.43.71
Best for fast, uncensored internet access in Europe and the US for free.

*

Yandex DNS

(Russia)
Basic Primary DNS: 77.88.8.8 | Secondary DNS: 77.88.8.1
Safe Primary DNS: 77.88.8.88 | Secondary DNS: 77.88.8.2
Family Primary DNS: 77.88.8.7 | Secondary DNS: 77.88.8.3
Best for safe and reliable internet access for individuals in Russia and eastern Europe.

*

Level 3

Primary DNS: 209.244.0.3 | Secondary DNS: 209.244.0.4
Best for personal and business users looking to access the internet backbone for free.