



Configuring Your DNS Server: A Step-by-Step Guide



by [Makenzie Buening](#), IT Editorial Expert
reviewed by [Stan Hunter](#), Technical Marketing Engineer

IT Ops

Last updated October 16, 2024



The [Domain Name System](#) (DNS) is the backbone of the internet. Proper **DNS configuration** is essential for seamless internet connectivity and plays a central role in enhancing website performance. In this guide, we will explore DNS configuration and its importance and provide step-by-step instructions for configuring DNS servers on various platforms, as well as client settings.

Try our #1 rated
endpoint management
software on G2

[Free Trial](#)

No credit card required,
full access to all features.

ninjaOne.

See which solutions IT Pros
recommend the most

4.8

5.0

3.2

4.4

[GET THE GUIDE](#)

What is DNS?

The Domain Name System, or DNS, is a fundamental component of the internet that functions as a distributed database. Its primary purpose is to translate user-friendly domain names into corresponding IP addresses. This translation enables computers and servers to locate and communicate with each other across the internet.

Proper DNS configuration is critical for ensuring that websites and other internet-based applications and services are accessible and load quickly for users. When DNS is misconfigured or inefficient, it can result in sluggish website performance, extended loading times, and even complete unavailability. DNS configuration directly impacts a user's experience when navigating the web.

What is a DNS server?

A **DNS server** is a specialized computer that plays a pivotal role in the DNS resolution process. When a user enters a domain name into their web browser, the DNS server queries its database before returning the required IP address to the client, enabling a connection to the domain.

DNS hierarchy and components

The DNS system operates in a hierarchical structure consisting of several key components:

- **Root servers:** These servers are at the top of the DNS hierarchy and maintain information about top-level domains (TLDs) like .com, .org, and .net.
- **Top-Level Domain (TLD) servers:** These servers manage specific TLDs, such as .com or .edu. There are both generic TLDs and country-code TLDs (ccTLDs).
- **Authoritative DNS servers:** These servers are responsible for specific domain names and provide authoritative answers for those domains.
- **Recursive DNS servers:** These servers are typically operated by internet service providers (ISPs) or third-party DNS providers. They perform the task of resolving domain names on behalf of users and recursively querying authoritative DNS servers until they find the IP address.

Reasons to change DNS configuration

DNS configuration involves modifying the settings of DNS servers that your device or network uses. This includes specifying the DNS server's IP addresses and configuring various DNS-related parameters.

The DNS configuration directly impacts internet connectivity. If DNS servers are misconfigured or unresponsive, users may experience slow or intermittent internet access, as domain name resolution will be delayed or fail.

Significance of DNS settings for faster website loading times

Optimized DNS settings can significantly contribute to faster website loading times. By using fast and reliable DNS servers, users can reduce the time it takes for their devices to resolve domain names to IP addresses, leading to quicker website access.

Changing DNS configuration offers several potential benefits:

- **Improved speed:** Faster DNS resolution leads to quicker website access.
- **Enhanced security:** Some DNS servers provide security features to protect against malicious websites and phishing attempts.
- **Bypassing restrictions:** Some DNS services can overcome region-based content restrictions.
- **Privacy:** Some DNS servers prioritize user privacy by not logging DNS queries.

Updating DNS client configuration

Client DNS settings are confined to DNS server IP addresses and are usually pre-configured as part of the process that allocates a device an IP address. Should DNS server settings need changing, follow the steps below relevant to your operating system:

Windows

1. Open "Control Panel" and navigate to "Network and Sharing Center".
2. Click the active network connection.
3. In the new window, click "Properties".
4. Click "Internet Protocol Version 4 (TCP/IPv4)", then navigate to "Properties."
5. Choose "Use the following DNS server addresses," then enter the desired DNS server IP addresses.
6. Click "OK", then close the windows.

macOS

1. Open "System Preferences" and go to "Network."

2. Select your network connection.
3. Click “Advanced” and navigate to the “DNS” tab.
4. Click “+” and enter the DNS server IP addresses.
5. Move the DNS servers just added to the top of the list.
6. Click “OK”, followed by “Apply”.

You might also be interested in:

[Automate DNS Cache Clearing in macOS](#)

Android

1. Open “Settings” and go to “Network & Internet.”
2. Tap on “Wi-Fi”.
3. Tap and hold your current Wi-Fi network.
4. Select “Modify network”.
5. Toggle on “Advanced options.”
6. In the “DNS” field, enter the new DNS server IP addresses.
7. Save your changes.

iOS

1. Open “Settings” and go to “Wi-Fi”.
2. Tap the information icon (i) next to your Wi-Fi network.
3. Scroll down and tap “Configure DNS”.
4. Select “Manual” and add the DNS server IP addresses.
5. Tap “Save”.

Alternative DNS servers, such as OpenDNS, offer enhanced security, content filtering, and faster performance. Users can take advantage of additional features not typically provided by their ISP’s default DNS by using these DNS servers.

DNS server configuration

DNS server configuration is much more complex and situational than that of a client. Consideration of the role of the DNS server in the hierarchy, the domains for which it will be authoritative, and the services supported result in bespoke configurations suitable only for the environment in which they are deployed. A high-level overview of the required steps follows for each operating system:

DNS configuration for Windows servers

1. Open “Server Manager” and select “Add roles and features.”
2. Navigate through the wizard and select the “DNS Server” role.
3. Follow the prompts to install the DNS server role.
4. After installation, open “DNS Manager” to configure DNS settings.
5. Create DNS zones, add DNS records, and configure forwarders as needed.
6. Regularly monitor DNS server logs for any issues or anomalies.

DNS manager and its features

[DNS Manager](#) is a powerful tool for configuring and [managing DNS servers on Windows Server environments](#). It provides a graphical interface for creating and managing DNS zones, records, and other DNS-related settings.

Best practices for Windows DNS server configuration

- Implement redundancy by configuring secondary DNS servers.
- Enable DNS caching to reduce query times.
- Regularly [update DNS records](#) to reflect changes in your network.

DNS configuration for Linux servers

1. Install the BIND (Berkeley Internet Name Domain) package using your package manager.
2. Edit the BIND configuration file (typically named /etc/named.conf) to define zones and DNS options.
3. Create zone files (e.g., /var/named/example.com.zone) for your domains and configure DNS records within them.
4. Start the BIND service and enable it to start on boot.
5. Test your DNS server by querying it for domain names.

BIND is a popular DNS software package for configuring DNS servers on Linux-based systems. It provides extensive configuration options and flexibility for DNS administrators.

Best practices for Linux DNS configuration

- Ensure proper syntax in BIND configuration files to prevent errors.
- Use tools like named-checkconf and named-checkzone to validate configuration files.
- Monitor DNS server logs for issues and errors.

Efficient DNS configuration is critical for optimal performance

DNS is a critical aspect of technology infrastructure that is often overlooked. Understanding and implementing proper DNS configuration is essential for seamless and secure internet connectivity and the optimal performance of internet-connected applications and services.

By following best practices and optimizing DNS settings, individuals and organizations can navigate the digital world more efficiently and securely. In a world where every second counts, efficient DNS

Next Steps

Building an efficient and effective IT team requires a centralized solution that acts as your core service deliver tool. NinjaOne enables IT teams to monitor, manage, secure, and support all their devices, wherever they are, without the need for complex on-premises infrastructure.

Learn more about [Ninja Endpoint Management](#), check out a [live tour](#), or [start your free trial of the NinjaOne platform](#).

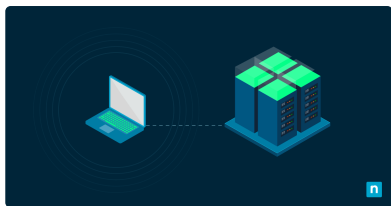
Start your Free Trial

CATEGORY:

IT OPS



YOU MIGHT ALSO LIKE



[How to Backup and Restore Device Drivers in Windows 11 and Windows 10](#)

[Complete Guide: How to Read Windows Update Logs](#)

[How to Change Wireless Network Connection Priority Order in Windows](#)

[How to Enable or Disable BSOD Automatic Restart in Windows](#)

[How to Restore Default Administrative Tools in Windows](#)

[How to Change the Registered Owner and Organization of Your Windows PC](#)

Ready to simplify the hardest parts of IT?

[Start a Free Trial](#)

[Get a demo](#)

Products

[RMM](#)

[Endpoint Management](#)

[Patch Management](#)

Resources

[Resource Center](#)

[Blog](#)

[IT Hub](#)

Compliance

[Privacy Notice](#)

[HIPAA](#)

[Bug Bounty](#)

Contact Info

North America: +1 888 542-8339

Germany: +49 30-76758700

UK: +44 20 3880 9027

