Contents

Introduction

NextDNS CLI is a command-line tool that allows you to use NextDNS's DNS-over-HTTPS (DoH) service with advanced capabilities. Although the most advanced features will only work with NextDNS, this program can work as a client for any DoH provider or a mix of NextDNS + another DNS (split horizon).

Installation

1. Enable JFFS if its not done already

```
1. On the router web page click on Administration.
2. Scroll down until you see JFFS2 Support section.
3. Click Enable Flash Storage.
4. Click Save.
5. Wait couple seconds, then click Apply.
6. Wait again. Go back to the Enable JFFS section, and enable Wipe Flash Storage.
7. Do not click Save. Click Apply instead.
8. Wait till you get the web-GUI back, then disable Wipe Flash Storage again.
9. Click Save.
```

2. SSH to your DD-WRT router

3. Execute:

```
sh -c "$(curl -sL https://nextdns.io/install)"
```

Upgrade

To upgrade to the latest version, simply re-run the installer. If a new version is available, the upgrade action will be added to the list of possible actions.

Useful commands

```
cat /jffs/etc/nextdns.conf
```

lists nextdns configuration file

```
/jffs/nextdns/nextdns config list -h
```

lists usage of nextdns config list

```
/jffs/nextdns/nextdns config set show
```

lists what each config option do

https://ping.nextdns.io/

will show servers with best latency

https://test.nextdns.io/

will show which server/profile you use

```
sh -c 'sh -c "$(curl -s https://nextdns.io/diag)"'
```

on unix/linux systems will run connection diagnose tool helping to troubleshoot problems

Tips&Tricks

You can run NextDNS CLI in a conjuction with dnsmasq and no extra steps are needed, but if you run it as a standalone dns client with enabled cache (this mode disables dnsmasq dns capabilities with directive port=0) you need to ssh to your DD-WRT and run:

```
/jffs/nextdns/nextdns config set -forwarder 2.pool.ntp.org=45.90.30.120,45.90.28.120
/jffs/nextdns/nextdns restart
```

this way dd-wrts ntpclient will work before DOH is established and will provide valid time for cert creation, again needed for DOH. Otherwise you will get known `x509: certificate has expired or is not yet valid` error.

For proper work NextDNS CLI edits dnsmasq.conf file with message `Configuration generated by NextDNS` so yours dnsmasq Additional Options will be erased every time router reboots. This is bad if you use dnsmasq for dhcp for example and have static entries or RA on ipv6. To mitigate such behaviour you can create your own dnsmasq.conf file and copy it to the /jffs/etc/dnsmasq.conf location which will be automatically executed by ddwrt on bootup. DO NOT forget to add lines NextDNS CLI added during conf generation (such as port=0 or similar). On linux such file can be easily copied with command:

```
scp /home/$User/Desktop/dnsmasq.conf root@192.168.1.1:/jffs/etc/dnsmasq.conf
```

the same way you can easily edit and copy nextdns configuration file:

```
scp /home/$User/Desktop/nextdns.conf root@192.168.1.1:/jffs/etc/nextdns.conf
```

Troubleshooting

If the installation fails, please run the installer in debug mode and contact team@nextdns.io with the transcript of the installation:

```
DEBUG=1 sh -c "$(curl -sL https://nextdns.io/install)"
```

If you have problem regarding Auto discovery and forwarding of LAN client's name and model (e.g. in logs you have something like Device #1SUO2) make sure multicast isn't blocked because nextdns cli uses mDNS for discovering hosts. DD-WRT is blocking multicast on layer2 so you can check it with:

```
ebtables -t nat -L POSTROUTING
```

to fix it make sure that on Firewall.asp under Block WAN Requests, Multicast Communication isn't checked. For brcm devices you should enable IGMP Snooping on Networking.asp under Bridging section too.