SmartDNS

SmartDNS is a local DNS server. SmartDNS accepts DNS query requests from local clients, obtains DNS query results from multiple upstream DNS servers, and returns the fastest access results to clients. Avoiding DNS pollution and improving network access speed, supports high-performance ad filtering. Unlike dnsmasq's all-servers, smartdns returns the fastest access resolution.
Latest guide can be found here

Index

Warning

If you use a VPN and rely on DNS settings via your VPN then note that SmartDNS is not compatible with this.
To prevent DNS leaks you have to manually route the used DNS servers via the VPN.

Official configuration guide

https://pymumu.github.io/smartdns/en/

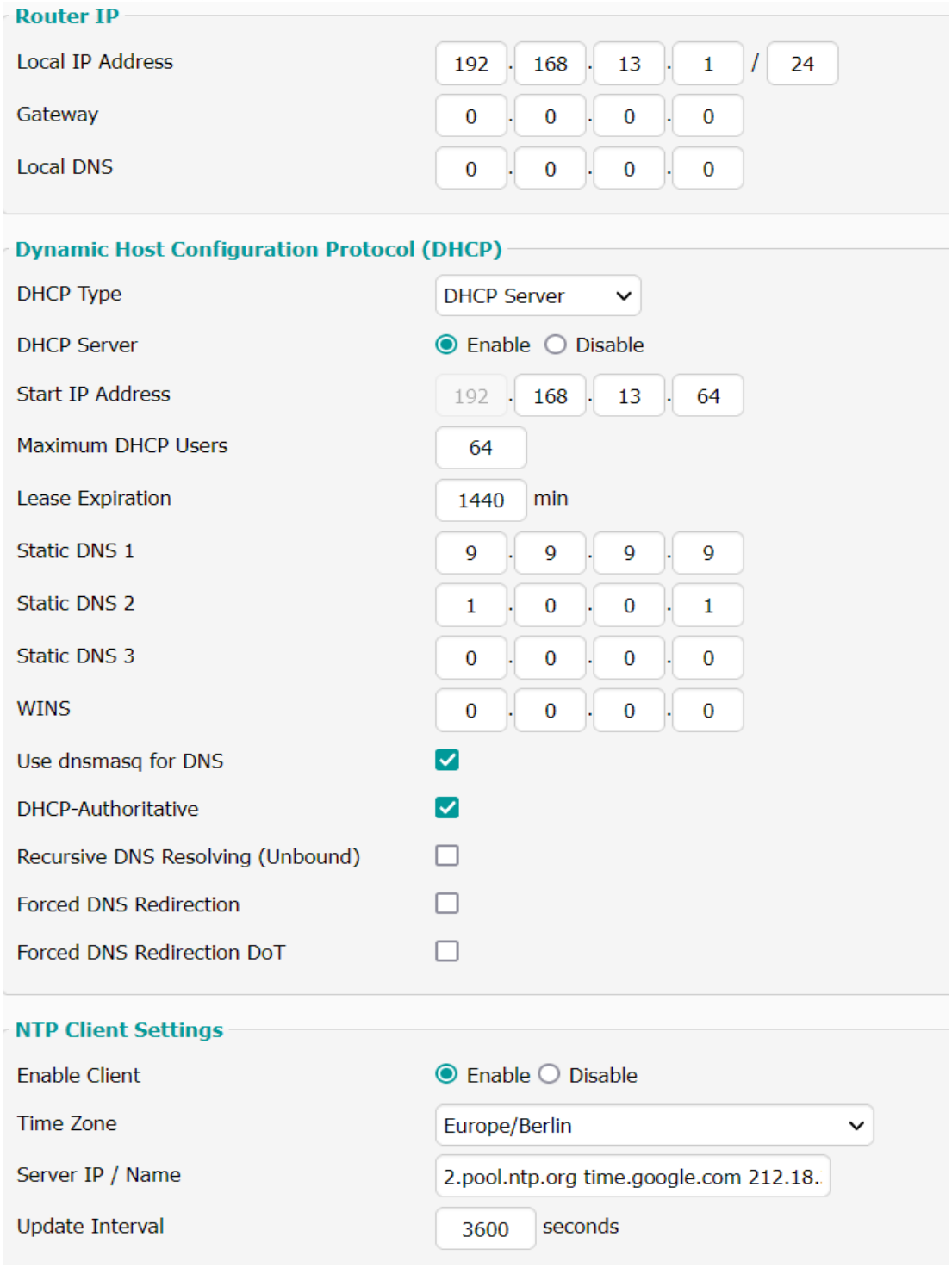
Simple SmartDNS AdBlock

https://github.com/egc112/ddwrt/tree/main/adblock/smartdns

My settings

Although you are encouraged to study the whole document I will start with my settings
I use SmartDNS as upstream resolver for DNSMasq so DNSMasq still does the local name resolving.
I use DoT but you can also use DoH.

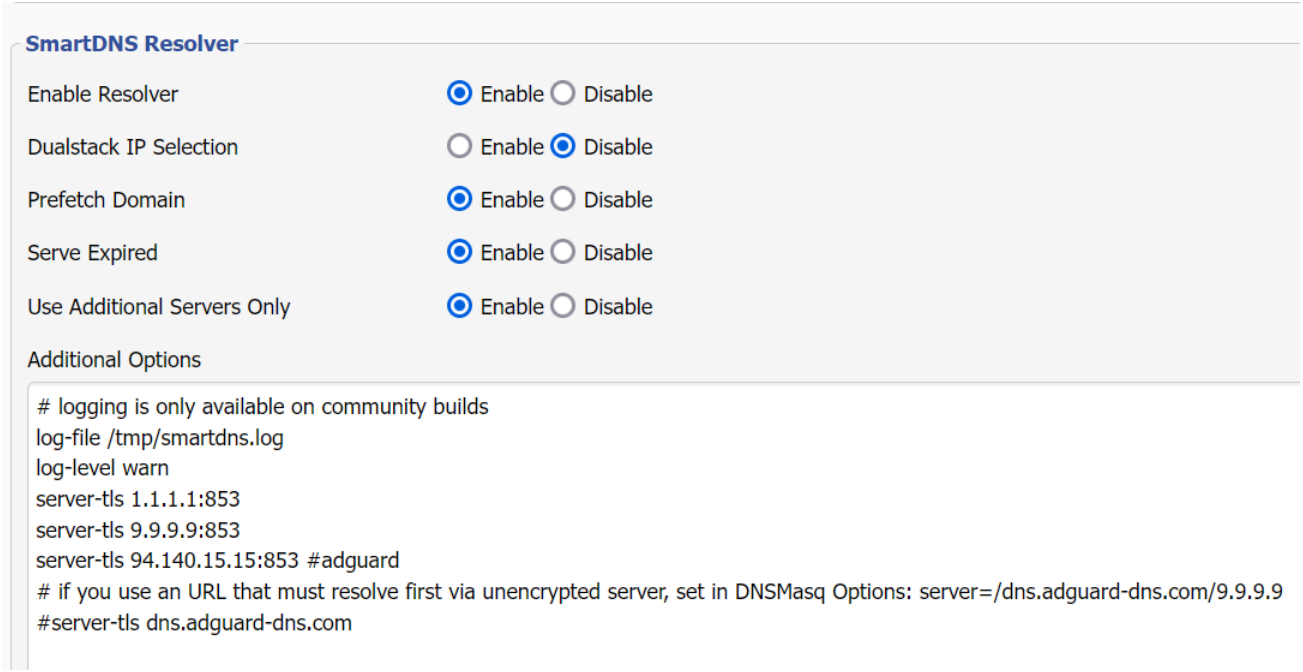
Basic Setup Page

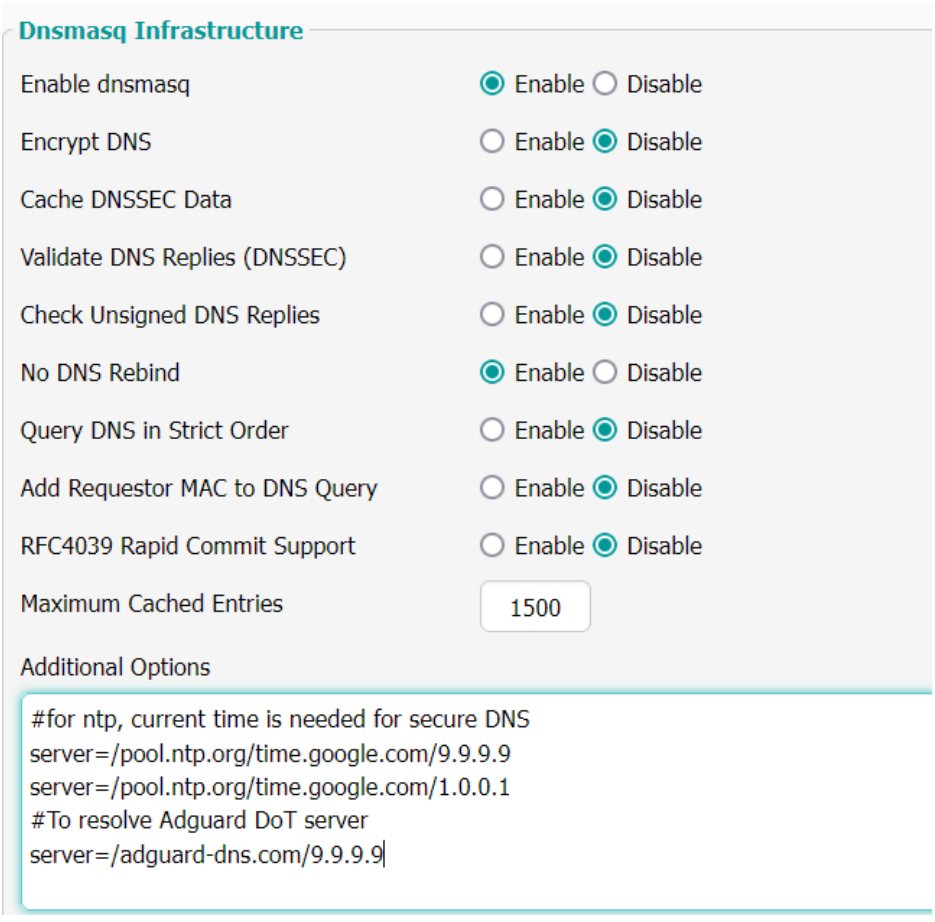


NTP/time servers used:
2.pool.ntp.org time.google.com 212.18.3.19 216.239.35.0

See NTP Problems

Services Page





New Settings

```
log-level info      # fatal,error,warn,notice,info,debug
server 8.8.8.8 -bootstrap-dns
server 8.8.8.8 -group time -exclude-default-group
nameserver /pool.ntp.org/time
nameserver /time.google.com/time
nameserver /cloudflare-dns.com/time
server-tls 9.9.9.9:853 -host-name dns.quad9.net
server-tls 1.0.0.1:853 -host-name cloudflare-dns.com
server-https https://1.1.1.1/dns-query
server-https https://9.9.9.9/dns-query
```

Explanation of settings

Dualstack IP Selection:

When Enabled SmartDNS will favor the usually faster IPv4.

Prefetch Domain:

When Enabled SmartDNS will be pre-fetching domain names to improve query hit rate.
This feature will consume more CPU when idle, so do not use it on low end routers

Serve Expired:

When Enabled it will improve the cache hit rate and reduce the CPU consumption.

Use Additional Servers only:

When Enabled SmartDNS will only use the DNS servers you have entered in the SmartDNS additional Options.
When Disabled SmartDNS will also use the existing DNS servers from /tmp/resolv.dnsmasq (which are usually the DNS servers you specified in Static DNS 1,2 and 3 etc, unless you are using VPN's which can alter DNS servers)

For more details See the FAQ

Logging

Recent builds finally have logging enabled.
Settings to use in the Additional Options:

```
#log-file /jffs/smartdnsegc.log
log-level notice        # fatal,error,warn,notice,info,debug
log-size 8K
#audit-enable yes
#audit-file /tmp/smartdns-audit.log
```

Using alternate smartdns.conf

SmartDNS reads its config file (smartdns.conf) from /tmp.
It first tries to read from /jffs/etc.
So you can make your own smartdns.conf file and put it in /jffs/etc
However if /jffs/etc is placed on a USB stick this will not be available when the router reboots.
You can then restart SmartDNS automatically by placing in Administration/Commands, Save USB:
restart smartdns

List of servers

DoH

```
server-https https://9.9.9.9/dns-query
server-https https://1.1.1.1/dns-query
server-https https://1.1.1.2/dns-query
server-https https://1.0.0.2/dns-query
server-https https://2606:4700:4700::1112/dns-query
server-https https://2606:4700:4700::1002/dns-query
server-https https://2620:fe::9/dns-query
```

DoT

server-tls 1.1.1.1:853
server-tls 1.1.1.1:853 -host-name cloudflare-dns.com -tls-host-verify cloudflare-dns.com # to verify
server-tls 1.1.1.2:853
server-tls 1.0.0.2:853
server-tls 9.9.9.9:853 -host-name dns.quad9.net
server-tls 5.2.75.75:853 -host-name dot.nl.ahadns.net
server-tls 78.46.244.143:853 -host-name dot-de.blahdns.com
server-tls 95.216.212.177:853 -host-name dot-fi.blahdns.com
server-tls 116.202.176.26:853 -host-name dot.libredns.gr
server-tls 2606:4700:4700::1112:853
server-tls 2606:4700:4700::1002:853
server-tls 2620:fe::9:853

Note the use of a colon to indicate a hostname e.g. -hostname**:** is no longer valid!

NTP (time server) and Tunnel endpoint Problems

When using DoT and /or DoH you need to have a current/correct time to get going but to get the current NTP time you need to resolve the built-in *2.pool.ntp.org* time server domain.
Even when specifying a non secure DNS server for the time servers, it can be problematic.
So if you experience time problems specify multiple url's and also hardcoded IP addresses.
On Basic Setup page Server IP/Name: *2.pool.ntp.org time.google.com 212.18.3.19 216.239.35.0*

In additional DNSMasq options set:
server=/pool.ntp.org/time.google.com/1.0.0.1
server=/pool.ntp.org/time.google.com/9.9.9.9

This will make sure that the used NTP domain 2.pool.ntp.org and time.google.com are resolved via DNS server 9.9.9.9 and 1.0.0.1 as soon as DNSmasq has started.

Alternatively you can specify IP addresses as Time server but the above is the superior option as the Domain name should always resolve to a working IP address of a Time server.

When using a Domain name as endpoint for your WireGuard or OpenVPN tunnel make sure to also add a non secure DNS server in the Additional DNSMasq options to resolve the endpoint!

Running SmartDNS without DNSMasq

Normally DNSMasq is used for DNS resolution and DNSMasq uses SmartDNS as upstream resolver.
This is done because in dnsmasq.conf the following lines are added when SmartDNS is enabled:
server=127.0.0.1#6053
no-resolv
This tells DNSMasq not to use the upstream resolvers in *resolv.dnsmasq* but to use a DNS server which is listening on *127.0.0.1#6053* which is SmartDNS.

Note: using SmartDNS or any other DNS is not compatible with DNS handling by OpenVPN or WireGuard.

It is however possible to cut out the middle man and use SmartDNS exclusively.
This can simple be done by unticking *Use dnsmasq for DNS* on Basic Setup page.

DNSMasq will have *port 0* in the dnsmasq.conf which will stop it from binding to port 53.
SmartDNS will now bind to port 53 and use the *dnsmasq.leases* for local name resolving.

Although this sounds great, in practice there seems to be very little speed difference in DNS resolving.

Software Show

Ali DNS

Use Ali DNS to query Baidu's IP and test the results.

```
pi@raspberrypi:~/code/smartdns_build $ nslookup www.baidu.com 223.5.5.5
Server:         223.5.5.5
Address:        223.5.5.5#53

Non-authoritative answer:
www.baidu.com   canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 180.97.33.108
Name:   www.a.shifen.com
Address: 180.97.33.107

pi@raspberrypi:~/code/smartdns_build $ ping 180.97.33.107 -c 2
PING 180.97.33.107 (180.97.33.107) 56(84) bytes of data.
64 bytes from 180.97.33.107: icmp_seq=1 ttl=55 time=24.3 ms
64 bytes from 180.97.33.107: icmp_seq=2 ttl=55 time=24.2 ms

--- 180.97.33.107 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 24.275/24.327/24.380/0.164 ms
pi@raspberrypi:~/code/smartdns_build $ ping 180.97.33.108 -c 2
PING 180.97.33.108 (180.97.33.108) 56(84) bytes of data.
64 bytes from 180.97.33.108: icmp_seq=1 ttl=55 time=31.1 ms
64 bytes from 180.97.33.108: icmp_seq=2 ttl=55 time=31.0 ms

--- 180.97.33.108 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 31.014/31.094/31.175/0.193 ms
```

smartdns

Use SmartDNS to query Baidu IP and test the results.

```
pi@raspberrypi:~/code/smartdns_build $ nslookup www.baidu.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.baidu.com   canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 14.215.177.39

pi@raspberrypi:~/code/smartdns_build $ ping 14.215.177.39 -c 2
PING 14.215.177.39 (14.215.177.39) 56(84) bytes of data.
64 bytes from 14.215.177.39: icmp_seq=1 ttl=56 time=6.31 ms
64 bytes from 14.215.177.39: icmp_seq=2 ttl=56 time=5.95 ms

--- 14.215.177.39 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 5.954/6.133/6.313/0.195 ms
```

From the comparison, smartdns found the fastest IP address to visit www.baidu.com, so accessing Baidu's DNS is 5 times faster than Ali DNS.

Features

1. **Multiple upstream DNS servers**
   Support configuring multiple upstream DNS servers and query at the same time.the query will not be affected, Even if there is a DNS server exception.

2. **Return the fastest IP address**
   Supports finding the fastest access IP address from the IP address list of the domain name and returning it to the client to avoid DNS pollution and improve network access speed.

3. **Support for multiple query protocols**
   Support UDP, TCP, TLS, HTTPS queries, and non-53 port queries, effectively avoiding DNS pollution.

4. **Domain IP address specification**
   Support configuring IP address of specific domain to achieve the effect of advertising filtering, and avoid malicious websites.

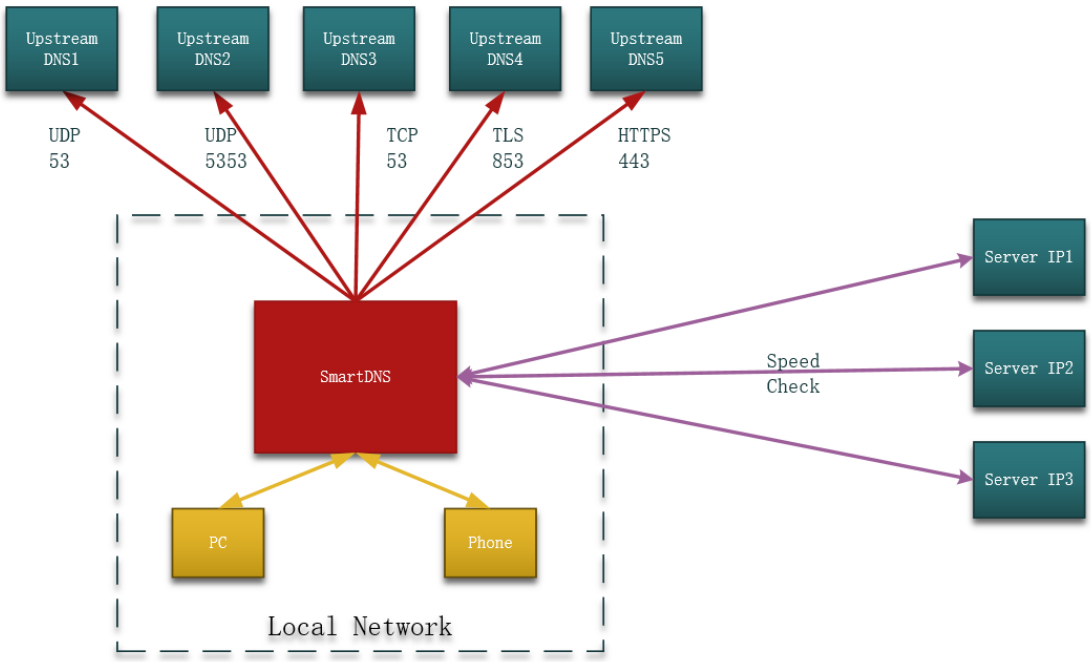
5. **Domain name high performance rule filtering**
   Support domain name suffix matching mode, simplify filtering configuration, filter 200,000 recording and take time <1ms.

6. **Linux/Windows multi-platform support**
   Support standard Linux system (Raspberry Pi), openwrt system various firmware, ASUS router native firmware. Support Windows 10 WSL (Windows Subsystem for Linux).

7. **Support IPV4, IPV6 dual stack**
   Support IPV4, IPV6 network, support query A, AAAA record, dual-stack IP selection, and disale IPV6 AAAA record.

8. **High performance, low resource consumption**
   Multi-threaded asynchronous IO mode, cache cache query results.

Architecture



Architecture

1. SmartDNS receives DNS query requests from local network devices, such as PCs and mobile phone query requests.
2. SmartDNS sends query requests to multiple upstream DNS servers, using standard UDP queries, non-standard port UDP queries, and TCP queries.
3. The upstream DNS server returns a list of Server IP addresses corresponding to the domain name. SmartDNS detects the fastest Server IP with local network access.
4. Return the fastest accessed Server IP to the local client.

DDWRT

Has built-in SmartDNS

Optware/Entware

1. Prepare
   When using this software, you need to confirm whether the router supports USB disk and prepare a USB disk.
2. Install SmartDNS
   Upload the software to `/tmp` directory of the router using winscp, and run the flollowing command to install.
   `ipkg install smartdns.xxxxxxx.mipsbig.ipk`
3. Modify the smartdns configuration
   `Vi /opt/etc/smartdns/smartdns.conf`
   Note: if you need to support IPV6, you can set the worke-mode to 2, this will disable the DNS service of dnsmasq, and smartdns run as the primary DNS server. Change `SMARTDNS_WORKMODE` in the file `/opt/etc/smartdns/smartdns-opt.conf` to 2.

```
SMARTDNS_WORKMODE="2"
```

4. Restart the router to take effect
   After the router is started, use `nslookup -querytype=ptr smartdns` to query the domain name. See if the `name` item in the command result is displayed as `smartdns` or `hostname`, such as `smartdns`

```
Pi@raspberrypi:~/code/smartdns_build $ nslookup -querytype=ptr smartdns
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
smartdns        name = smartdns.
```

   Note: If the service does not start automatically, you need to set optwre/entware to start automatically. For details, see the optware/entware documentation.

Configuration parameter

parameter	Parameter function	Default value	Value type	Example
server-name	DNS name	host name/smartdns	any string like hosname	server-name smartdns
bind	DNS listening port number	[::]:53	Support binding multiple ports `IP:PORT`: server IP, port number. `[-group]`: The DNS server group used when requesting. `[-no-rule-addr]`: Skip the address rule. `[-no-rule-nameserver]`: Skip the Nameserver rule. `[-no-rule-ipset]`: Skip the Ipset rule. `[-no-rule-soa]`: Skip address SOA(#) rules. `[-no-dualstack-selection]`: Disable dualstack ip selection. `[-no-speed-check]`: Disable speed measurement. `[-no-cache]`: stop caching	bind :53
bind-tcp	TCP mode DNS listening port number	[::]:53	Support binding multiple ports `IP:PORT`: server IP, port number. `[-group]`: The DNS server group used when requesting. `[-no-rule-addr]`: Skip the address rule. `[-no-rule-nameserver]`: Skip the Nameserver rule. `[-no-rule-ipset]`: Skip the Ipset rule. `[-no-rule-soa]`: Skip address SOA(#) rules. `[-no-dualstack-selection]`: Disable dualstack ip selection. `[-no-speed-check]`:	bind-tcp :53

			Disable speed measurement. `[-no-cache]`: stop caching	
cache-size	Domain name result cache number	512	integer	cache-size 512
cache-persist	enable persist cache	Auto: Enabled if the location of `cache-file` has more than 128MB of free space.	[yes|no]	cache-persist yes
cache-file	cache persist file	/tmp/smartdns.cache	路径	cache-file /tmp/smartdns.cache
tcp-idle-time	TCP connection idle timeout	120	integer	tcp-idle-time 120
rr-ttl	Domain name TTL	Remote query result	number greater than 0	rr-ttl 600
rr-ttl-min	Domain name Minimum TTL	Remote query result	number greater than 0	rr-ttl-min 60
rr-ttl-max	Domain name Maximum TTL	Remote query result	number greater than 0	rr-ttl-max 600
log-level	log level	error	fatal,error,warn,notice,info,debug	log-level error
log-file	log path	/var/log/smartdns.log	File Pah	log-file /var/log/smartdns.log
log-size	log size	128K	number+K,M,G	log-size 128K
log-num	archived log number	2	Integer	log-num 2

audit-enable	audit log enable	no	[yes|no]	audit-enable yes
audit-file	audit log file	/var/log/smartdns-audit.log	File Path	audit-file /var/log/smartdns-audit.log
audit-size	audit log size	128K	number+K,M,G	audit-size 128K
audit-num	archived audit log number	2	Integer	audit-num 2
conf-file	additional conf file	None	File path	conf-file /etc/smartdns/smartdns.more.conf
server	Upstream UDP DNS server	None	Repeatable `[ip][:port]`: Server IP, port optional. `[-blacklist-ip]`: The "-blacklist-ip" parameter is to filtering IPs which is configured by "blacklist-ip". `[-whitelist-ip]`: whitelist-ip parameter specifies that only the IP range configured in whitelist-ip is accepted. `[-group [group] ...]`: The group to which the DNS server belongs, such as office, foreign, use with nameserver. `[-exclude-default-group]`: Exclude DNS servers from the default group	server 8.8.8.8:53 -blacklist-ip
server-tcp	Upstream TCP DNS server	None	Repeatable `[ip][:port]`: Server IP, port optional. `[-blacklist-ip]`: The "-blacklist-ip" parameter is to filtering IPs which is configured by "blacklist-ip". `[-whitelist-ip]`: whitelist-ip parameter specifies that only the IP	server-tcp 8.8.8.8:53

			range configured in whitelist-ip is accepted. `[-group [group] ...]`: The group to which the DNS server belongs, such as office, foreign, use with nameserver. `[-exclude-default-group]`: Exclude DNS servers from the default group	
server-tls	Upstream TLS DNS server	None	Repeatable `[ip][:port]`: Server IP, port optional. `[-spki-pin [sha256-pin]]`: TLS verify SPKI value, a base64 encoded SHA256 hash `[-host-name]`:TLS Server name. `[-tls-host-verify]`: TLS cert hostname to verify. `-no-check-certificate:`: No check certificate. `[-blacklist-ip]`: The "-blacklist-ip" parameter is to filtering IPs which is configured by "blacklist-ip". `[-whitelist-ip]`: whitelist-ip parameter specifies that only the IP range configured in whitelist-ip is accepted. `[-group [group] ...]`: The group to which the DNS server belongs, such as office, foreign, use with nameserver. `[-exclude-default-group]`: Exclude DNS servers from the default group	server-tls 8.8.8.8:853 server-tls 9.9.9.9:853 server-tls 1.1.1.1:853 server-tls 94.140.15.15:853 # if you use an URL that must resolve first via unencrypted server set in DNSMasq Options server=adguard-dns.com/94.140.14.14 #server-tjs dns.adguard-dns.com

server-https	Upstream HTTPS DNS server	None	Repeatable `https://[host][:port]/path`: Server IP, port optional. `[-spki-pin [sha256-pin]]`: TLS verify SPKI value, a base64 encoded SHA256 hash `[-host-name]`:TLS Server name `[-http-host]` : http header host. `[-tls-host-verify]`: TLS cert hostname to verify. `-no-check-certificate:`: No check certificate. `[-blacklist-ip]`: The "-blacklist-ip" parameter is to filtering IPs which is configured by "blacklist-ip". `[-whitelist-ip]`: whitelist-ip parameter specifies that only the IP range configured in whitelist-ip is accepted. `[-group [group] ...]`: The group to which the DNS server belongs, such as office, foreign, use with nameserver. `[-exclude-default-group]`: Exclude DNS servers from the default group	server-https https://cloudflare-dns.com/dns-query EGC: do not use URL but use IP-address: server-https https://1.1.1.1/dns-query server-https https://9.9.9.9:5053/dns-query?name=quad9.net AdGuard: server-https https://94.140.14.14/dns-query
speed-check-mode	Speed mode	None	[ping|tcp:[80]|none]	speed-check-mode ping,tcp:443
address	Domain IP address	None	address /domain/[ip|-|-4|-6|#|#4|#6], - for ignore, # for return SOA, 4 for IPV4, 6 for IPV6	address /www.example.com/1.2.3.4
nameserver	To query domain with specific	None	nameserver /domain/[group|-], group is the group name, - means ignore this rule, use the -	nameserver /www.example.com/office

	server group		group parameter in the related server	
ipset	Domain IPSet	None	ipset /domain/[ipset|-|#[4|6]:[ipset|-][,#[4|6]:[ipset|-]]], - for ignore	ipset /www.example.com/#4:dns 4,#6:-
ipset-timeout	ipset timeout enable	auto	[yes]	ipset-timeout yes
domain-rules	set domain rules	None	domain-rules /domain/ [-rules...] [-c|-speed-check-mode]: set speed check mode, same as parameter speed-check-mode [-a|-address]: same as parameter address [-n|-nameserver]: same as parameter nameserver [-p|-ipset]: same as parameter ipset [-d|-dualstack-ip-selection]: same as parameter dualstack-ip-selection	domain-rules /www.example.com/ -speed-check-mode none
bogus-nxdomain	bogus IP address	None	[IP/subnet], Repeatable	bogus-nxdomain 1.2.3.4/16
ignore-ip	ignore ip address	None	[ip/subnet], Repeatable	ignore-ip 1.2.3.4/16
whitelist-ip	ip whitelist	None	[ip/subnet], Repeatable, When the filtering server responds IPs in the IP whitelist, only result in whitelist will be accepted	whitelist-ip 1.2.3.4/16
blacklist-ip	ip blacklist	None	[ip/subnet], Repeatable, When the filtering server responds IPs in the IP blacklist, The result will be discarded directly	blacklist-ip 1.2.3.4/16

force-AAAA-SOA	force AAAA query return SOA	no	[yes|no]	force-AAAA-SOA yes
force-qtype-SOA	force specific qtype return SOA	qtype id	[qtypeid	...]
prefetch-domain	domain prefetch feature	no	[yes|no]	prefetch-domain yes
serve-expired	Cache serve expired feature	no	[yes|no], Attempts to serve old responses from cache with a TTL of 0 in the response without waiting for the actual resolution to finish.	serve-expired yes
serve-expired-ttl	Cache serve expired limite TTL	0	second, 0 : disable, > 0 seconds after expiration	serve-expired-ttl 0
serve-expired-reply-ttl	TTL value to use when replying with expired data	5	second, 0 : disable, > 0 seconds after expiration	serve-expired-reply-ttl 30
dualstack-ip-selection	Dualstack ip selection	no	[yes|no]	dualstack-ip-selection yes
dualstack-ip-selection-threshold	Dualstack ip select threadhold	30ms	millisecond	dualstack-ip-selection-threshold [0-1000]
ca-file	certificate file	/etc/ssl/certs/ca-certificates.crt	path	ca-file /etc/ssl/certs/ca-certificates.crt

ca-path	certificates path	/etc/ssl/certs	path	ca-path /etc/ssl/certs

FAQ

1. What is the difference between SmartDNS and DNSMASQ?
   Smartdns is not designed to replace DNSMASQ. The main function of Smartdns is focused on DNS resolution enhancement, the difference are:
   - Multiple upstream server concurrent requests, after the results are measured, return the best results;
   - `address`, `ipset` domain name matching uses efficient algorithms, query matching is faster and more efficient, and router devices are still efficient.
   - Domain name matching supports ignoring specific domain names, and can be individually matched to IPv4, IPV6, and supports diversified customization.
   - Enhance the ad blocking feature, return SOA record, this block ads better;
   - IPV4, IPV6 dual stack IP optimization mechanism, in the case of dual network, choose the fastest network.
   - Supports the latest TLS, HTTPS protocol and provides secure DNS query capabilities.
   - DNS anti-poison mechanism, and a variety of mechanisms to avoid DNS pollution.
   - ECS support, the query results are better and more accurate.
   - IP blacklist support, ignoring the blacklist IP to make domain name queries better and more accurate.
   - Domain name pre-fetch, more faster to access popular websites.
   - Domain name TTL can be specified to make access faster.
   - Cache mechanism to make access faster.
   - Asynchronous log, audit log mechanism, does not affect DNS query performance while recording information.
   - Domain group mechanism, specific domain names use specific upstream server group queries to avoid privacy leakage.
   - The second DNS supports customizing more behavior.
2. What is the best practices for upstream server configuration?
   Smartdns has a speed measurement mechanism. When configuring an upstream server, it is recommended to configure multiple upstream DNS servers, including servers in different regions, but the total number is recommended to be around 10. Recommended configuration
   - Carrier DNS.
   - Public DNS, such as `8.8.8.8`, `8.8.4.4`, `1.1.1.1`.

   For specific domain names, if there is a pollution, you can enable the anti-pollution mechanism.
3. How to enable the audit log
   The audit log records the domain name requested by the client. The record information includes the request time, the request IP address, the request domain name, and the request type. If you want to enable the audit log, configure `audit-enable yes` in the configuration file, `audit-size`, `Audit-file`, `audit-num` configure the audit log file size, the audit log file path, and the number of audit log files. The audit log file will be compressed to save space.
4. How to avoid DNS privacy leaks By default, smartdns will send requests to all configured DNS servers. If the upstream DNS servers record DNS logs, it will result in a DNS privacy leak. To avoid privacy leaks, try the following steps:
   - Use trusted DNS servers.
   - Use TLS servers.
   - Set up an upstream DNS server group.
5. How to block ads Smartdns has a high-performance domain name matching algorithm. It is very efficient to filter advertisements by domain name. To block ads, you only need to configure records like the following configure. For example, if you block `*.ad.com`, configure as follows:
   `Address /ad.com/#`

The suffix mode of the domain name, filtering *.ad.com, # means returning SOA record. If you want to only block IPV4 or IPV6 separately, add a number after #, such as #4 is for IPV4 blocking. If you want to ignore some specific subdomains, you can configure it as follows. e.g., if you ignore `pass.ad.com`, you can configure it as follows:

```
Address /pass.ad.com/-
```

6. DNS query diversion In some cases, some domain names need to be queried using a specific DNS server to do DNS diversion. such as.

```
.home -> 192.168.1.1
.office -> 10.0.0.1
```

The domain name ending in .home is sent to 192.168.1.1 for resolving The domain name ending in .office is sent to 10.0.0.1 for resolving Other domain names are resolved using the default mode. The diversion configuration for this case is as follows:

```
# Upstream configuration, use -group to specify the group name, and -exclude-default-group to exclude the server from the default group.
Server 192.168.1.1 -group home -exclude-default-group
Server 10.0.0.1 -group office -exclude-default-group
Server 8.8.8.8

#Configure the resolved domain name with specific group
Nameserver /.home/home
Nameserver /.office/office
```

You can use the above configuration to implement DNS resolution and offload. If you need to implement traffic distribution on the requesting port, you can configure the second DNS server. The bind configuration is added. The group parameter specifies the traffic distribution name.

```
Bind :7053 -group office
Bind :8053 -group home
```

7. How to use the IPV4, IPV6 dual stack IP optimization feature
   At present, IPV6 network is not as fast as IPV4 in some cases. In order to get a better experience in the dual-stack network, SmartDNS provides a dual-stack IP optimization mechanism, the same domain name, and the speed of IPV4. Far faster than IPV6, then SmartDNS will block the resolution of IPV6, let the PC use IPV4, the feature is enabled by `dualstack-ip-selection yes`, `dualstack-ip-selection-threshold [time]` is for threshold. if you want to disable IPV6 AAAA record complete, please try `force-AAAA-SOA yes`.
8. How to improve cache performace
   Smartdns provides a domain name caching mechanism to cache the queried domain name, and the caching time is in accordance with the DNS TTL specification. To increase the cache hit rate, the following configuration can be taken:
   - Increase the number of cache records appropriately
     Set the number of cache records by `cache-size`. In the case of a query with a high pressure environment and a machine with a large memory, it can be appropriately adjusted.
   - Set the minimum TTL value as appropriate
     Set the minimum DNS TTL time to a appropriate value by `rr-ttl-min` to extend the cache time. It is recommended that the timeout period be set to 10 to 30 minutes to avoid then invalid domain names when domain ip changes.
   - Enable domain pre-acquisition
     Enable pre-fetching of domain names with `prefetch-domain yes` to improve query hit rate. by default, Smartdns will send domain query request again before cache expire, and cache the result for the next query. Frequently accessed domain names will continue to be cached. This feature will consume more CPU when idle.

- Cache serve expired feature
  Enable cache serve expired feature with `serve-expired yes` to improve the cache hit rate and reduce the CPU consumption. This feature will return TTL = 0 to the client after the TTL timeout, and send a new query request again at the same time, and cache the new results for later query.

9. How does the second DNS customize more behavior?
   The second DNS can be used as the upstream of other DNS servers to provide more query behaviors. Bind configuration support can bind multiple ports. Different ports can be set with different flags to implement different functions, such as
   ```
   # Binding 6053 port, request for port 6053 will be configured with the upstream query of the office group, and the result will not be measured. The address configuration address is ignored.
   bind [::]:6053 -no-speed-check -group office -no-rule-addr
   ```
10. How to get SPKI of DOT
    The SPKI can be obtained from the page published by the DNS service provider. If it is not published, it can be obtained by the following command, replace IP with your own IP.
    ```
    echo | openssl s_client -connect '1.0.0.1:853' 2>/dev/null | openssl x509 -pubkey -noout | openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64
    ```

References

Use for ad blocking: https://forum.openwrt.org/t/smartdns-config-with-dns-over-https/130488/27
Use SmartDNs as only resolver: https://tadeubento.com/2022/dd-wrt-proper-dns-with-smartdns/

Check

To test cloudfare which also shows if you are using DoT/DoH: https://1.1.1.1/help
To test if you are using Quad9: https://on.quad9.net/

https://www.cloudflare.com/ssl/encrypted-sni/

https://superuser.com/questions/1708212/how-to-verify-that-youre-using-dns-over-https-doh-with-quad9-other-non-clou

https://support.quad9.net/hc/en-us/articles/10514256222349

In depth explanation about the cooperation between DNSmasq and SmartDNS

First, whether you use an IPv6 address for a DNS server or an IPv4 address does not matter much as it is the same DNS server you eventually query and that DNS server will answer with both an IPv4 and IPv6 address (if the client is dual stack).

The client itself will decide if it uses the IPv6 or IPv4 address but most modern clients favor the use of IPv6 addresses.

See the nslookup from a Windows client first to a DNS server with an IPV6 address and then a DNS server with a IPv4 address, both return IPv4 and IPv6 addresses for ipleak.net.
[code]PS C:\Users> nslookup ipleak.net 2001:4860:4860::8888
Server: dns.google
Address: 2001:4860:4860::8888

Non-authoritative answer:
Name: ipleak.net
Addresses: 2a03:b0c0:0:1010::509:d001
          95.85.16.212

PS C:\Users> nslookup ipleak.net 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: ipleak.net
Addresses: 2a03:b0c0:0:1010::509:d001
          95.85.16.212[/code]

Now on to how DNSMasq works in relation to SmartDNS.
If you enable SmartDNS it will place this in /tmp/dnsmasq/conf:
[quote]server=127.0.0.1#6053
no-resolv
[/quote]

You should check if that is present.
"no-resolv" means that resolv.dnsmasq is *not* used.

What DNSmasq is using as upstream resolvers is specified by the "server" directive
So "server=127.0.0.1#6053" means use the DNS server listening on port 6053 on IP address 127.0.0.1 which is SmartDNS.

In syslog you can see that:
[quote]root@EA6900:~# grep -i dnsmasq /var/log/messages
Jan 10 09:39:13 EA6900 user.info : [dnsmasq] : successfully started
Jan 10 09:39:13 EA6900 daemon.info dnsmasq[7832]: using nameserver 127.0.0.1#6053
Jan 10 09:39:13 EA6900 daemon.info dnsmasq[7832]: using nameserver 9.9.9.9#53 for domain pool.ntp.org
Jan 10 09:39:13 EA6900 daemon.info dnsmasq[7832]: using nameserver 9.9.9.9#53 for domain time.google.com[/quote]
Syslog shows that indeed DNSMasq is using SmartDNS and for two NTP domains it uses an other DNS server (as SmartDNS needs the correct time because it uses secure DNS servers (Dot, DoH)).

Of course if you add more "server=XXXX" in DNSMasq additional options then those will also be used which nullifies the use of SmartDNS, so you cannot use other "server=" entries unless used for specific domains as for the NTP servers.

SmartDNS will then use the upstream DNS server you have specified in the SmartDNS additional options (but if you have "Use Additional Servers Only" Disabled then SmartDNS will also use the DNS server from resolv.dnsmasq, [b]so you have to make sure you have "Use Additional Servers Only" Enabled[/b])

You cannot see what SmartDNS is using for DNS server as regular builds do not have SmartDNS logging.
I do have logging and this is my SmartDNS log:
[quote][2023-01-10 09:39:13,477][INFO][dns_cache.c:782] load cache file /tmp/smartdns.cache, total 0 records
[2023-01-10 09:39:13,478][INFO][dns_server.c:5489] IPV6 is ready, enable IPV6 features
[2023-01-10 09:39:13,646][INFO][dns_client.c:1116] add server 2606:4700:4700::1112:853:853, type: tls
[2023-01-10 09:39:13,646][INFO][dns_client.c:1116] add server 2606:4700:4700::1002:853:853, type: tls
[2023-01-10 09:39:13,646][INFO][dns_client.c:1116] add server 1.1.1.1:443, type: https
[2023-01-10 09:39:13,646][INFO][dns_client.c:1116] add server 9.9.9.9:5053, type: https[/quote]It shows that SmartDNS is using all 4 specified DNS servers

So DNSMasq is using SmartDNS and SmartDNS is using the DNS servers specified in the SmartDNS Additional Options.
resolv.dnsmasq, which can take its entries from Static DNS 1, 2, 3, from the Static DNS entries on the IPv6 tab, from VPN clients and from the WAN DNS is *not* used, not by DNSmasq as there is "no-resolv" in dnsmasq.conf and not by SmartDNS as "Use Additional Servers Only" is enabled.