

# Install STUBBY DNS over TLS (DOT)

## Prerequisites

DD-WRT Router with USB support.

Install Entware suitable for your router architecture:

[https://wiki.dd-wrt.com/wiki/index.php/Installing\\_Entware](https://wiki.dd-wrt.com/wiki/index.php/Installing_Entware)

Install stubby: **opkg install stubby**

Install ca-certificates: **opkg install ca-certificates**

Place the following script (named **S61stubby.sh**) in */opt/etc/init.d*

```
#!/bin/sh
logger -t S61stubby "Starting Stubby DNS over TLS $0"
# set environment PATH to system binaries
export PATH=/sbin:/bin:/usr/sbin:/usr/bin:$PATH
ENABLED=yes
PROCS=stubby
ARGS="-g -v 5 -C /opt/etc/stubby/stubby.yml
2>/opt/var/log/stubby.log"
PREARGS=""
DESC=$PROCS
PATH=/opt/sbin:/opt/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin:/sbin:/bin
. /opt/etc/init.d/rc.func
```

( Original script had **PREARGS="nohup"** It may work that way)

Make it executable: **chmod +x /opt/etc/init.d/S61stubby.sh**

Edit stubby.yml using nano: **opkg install nano**

**nano /opt/etc/stubby/stubby.yml**

Or vi, <https://www.cs.colostate.edu/helpdocs/vi.html>

Or notepad++ w/Unix encoding

## Read **`opt/etc/stubby/stubby.yml.default`**

Configure your preferred servers.

Pay special attn. to line indents.

Start stubby with **`/opt/etc/init.d/S61stubby.sh start`** save as startup.

( May need 'sleep 10' before startup) without quotes.

Stop stubby with **`/opt/etc/init.d/S61stubby.sh stop`** save shutdown.

From Command Line to check, start, or stop stubby:

**`/opt/etc/init.d/S61stubby.sh check`** (or start or stop)

**`netstat -p`** catches port 853 intermittently.

**`watch -tn5 "cat /proc/net/nf_conntrack | grep ' dport=853 ' | sort -nrk3"`**

Some routers may need **`ip^_conntrack`**

Thanks egc!

Some routers do not have "watch". Can be seen with tcpdump.

**`https://1.1.1.1/help`**

You may have to set Time Server as IP address at Setup → Basic Setup

→ Server IP/Name

ie: 216.239.35.4 (time.google.com)

## Read **`opt/etc/stubby/stubby.yml.default`**

## Example stubby.yml IPv6 disabled

```
resolution_type: GETDNS_RESOLUTION_STUB
round_robin_upstreams: 1
appdata_dir: "/opt/var/lib/stubby"
tls_authentication: GETDNS_AUTHENTICATION_REQUIRED
tls_query_padding_blocksize: 128
edns_client_subnet_private: 1
idle_timeout: 10000
listen_addresses:
  - 127.0.0.1@5453
  - 0::1@5453
dns_transport_list:
  - GETDNS_TRANSPORT_TLS
upstream_recursive_servers:
# - address_data: 2606:4700:4700::1111
#   tls_auth_name: "cloudflare-dns.com"
# - address_data: 2606:4700:4700::1111
#   tls_auth_name: "cloudflare-dns.com"
# - address_data: 2620:fe::fe, 2620:fe::fe:9
#   tls_auth_name: "dns.quad9.net"
  - address_data: 1.1.1.1
    tls_auth_name: "cloudflare-dns.com"
  - address_data: 1.0.0.1
    tls_auth_name: "cloudflare-dns.com"
# - address_data: 9.9.9.9
#   tls_auth_name: "dns.quad9.net"
  - address_data: 145.100.185.15
    tls_auth_name: "dnsovertls.sinodun.com"
  - address_data: 145.100.185.16
    tls_auth_name: "dnsovertls.sinodun.com"
  - address_data: 185.49.141.37
    tls_auth_name: "getdnsapi.net"
# - address_data: 149.112.112.112
#   tls_auth_name: "dns.quad9.net"
```

# Miscellaneous

## My DNS SETTINGS: YMMV

DHCP Type	DHCP Server
DHCP Server	Enable
Start IP Address	192.168.1.128
Maximum DHCP Users	32
Client Lease Expiration	1440 min
Static DNS 1	0.0.0.0
Static DNS 2	0.0.0.0
Static DNS 3	0.0.0.0
WINS	0.0.0.0
Use DNSMasq for DNS	Enable
DHCP-Authoritative	Enable
Recursive DNS Resolving (Unbound)	Disable
Forced DNS Redirection	Disable

Time Settings ->Server IP/Name      216.239.35.4

<->

### Additional Dnsmasq Options

```
local=/home/  
expand-hosts  
No-resolv                   # REQUIRED FOR STUBBY  
Server=127.0.0.1#5453 # REQUIRED FOR STUBBY  
dhcp-host=50:2E:9F:6P:9V:YZ,my-phone,192.168.1.116,infinite  
dhcp-host=A0:6A:99:UL:75:FH,tvwire,192.168.1.106,infinite  
dhcp-host=lk:6G:79:1S:H8:Q1,tv5g,192.168.1.105,infinite  
ETC
```