

# How to set up OpenVPN Server on HH5a with OpenWrt 21.02

based on OpenWrt wiki article written  
by 'vgaetera' as of December 2021

## Document revision history:

v0.2b	(8 Aug 2022)	- Verified working with 22.03.0-rc6
v0.2	(24 Dec 2021)	-
v0.1	(20 Dec 2021)	- Created by 'bill'.

## Contents

1. Introduction .....	3
2. Installing the OpenVPN Server .....	4
2.1 Configuring LAN and WAN interfaces .....	4
Edit default LAN IP address .....	5
Edit WAN settings .....	7
Modem-router Owners Only: .....	9
All router owners: .....	10
DDNS .....	11
2.2 Downloading and configuring OpenVPN server .....	11
Quick installation method .....	12
Preparation .....	13
Key Management.....	16
Firewall .....	19
VPN Service .....	21
2.3 Configure Port forwarding rule on ISP facing router .....	22
AsusWRT router .....	22
OpenWrt router .....	23
TPlink router .....	23
2.4 Download and editing the client ovpn file .....	24
2.5 Configuring the OpenVPN Client.....	25
Microsoft Windows.....	25
Android .....	27
2.6 LED configuration .....	28
2.7 Frequently Asked Questions .....	28
2.8 OpenWrt settings .....	29
OpenVPN.....	29
Firewall .....	30
System Log.....	32
3. Bug fixes for Home Hub 5A.....	33
3.1 How to disable 'dsl_control' (DSL port) .....	33
3.2 Random WAN port MAC address fix .....	34
OpenWrt - up to 19.07.....	34
OpenWrt – all versions.....	35
OpenWrt - 21.02 only.....	37

## 1. Introduction

This is a supplement to the ‘OpenWrt/LEDE Installation Guide for the BT Home Hub 5A’ modem-router. It describes how to install and configure the OpenVPN server. Although this guide was written with the HH5a in mind, the instructions should work with all other makes and models of OpenWrt routers too.

This document is written for OpenWrt 21 and supplements the OpenWrt wiki instructions for OpenWrt server installation, which I believe was created and is maintained by OpenWrt member ‘**vgaetera**’.

This guide is written with Microsoft Windows users in mind and is correct as of December 2021.

For HH5a owners, allow at least **90** minutes to complete all these steps.

The OpenWrt OpenVPN server wiki instructions do not work with previous major releases of OpenWrt when tested as of 24 December 2021. The generated OpenVPN files are missing `tls-crypt-v2` sections due to a bug. The wiki article offers a link to an older version of the wiki article which does work with OpenWrt 19.07 when tested.

For Windows users, please refer to section 10 of the ‘OpenWrt/LEDE installation guide for HH5a’ for quick guide to using PuTTY, Notepad++, and WinSCP.

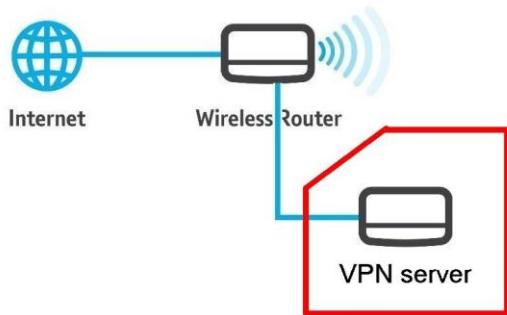
Speed test results using [www.speedtest.net](http://www.speedtest.net) for some routers I have tested over **ethernet** connection:

Device	OpenWrt	SoC	OpenVPN speed
BT Home Hub 5A	21.02.1	500 MHz MIPS VRX268	9 Mbps
Linksys EA6350 v3	21.02.1	710 MHz ARM IPQ4018	25 Mbps

Note that some internet providers, especially mobile phone services, may operate Carrier Grade NAT (CGNAT), where same IP address is shared by multiple customers. The OpenVPN server is unlikely to work with CGNAT. Contact the service provider to request a non-CGNAT connection if they are able to offer it.

## 2. Installing the OpenVPN Server

### 2.1 Configuring LAN and WAN interfaces



The HH5a is an 'underpowered' modem-router with OpenVPN throughput unlikely to exceed 9 mbps. For this reason, this tutorial shows how to install a separate HH5a OpenVPN server wired to an existing ISP facing router.

Advice is included where there is only a single OpenWrt router which connects to the internet and will also host the OpenVPN server.

To install OpenVPN server, a working internet connection is required. The red WAN port on the HH5A will be enabled for this purpose, so it can be connected to an existing router for internet access.

Example configuration:

Main ISP router LAN IP address	192.168.1.1
HH5a VPN server LAN IP address	192.168.111.1
HH5a VPN server static WAN IP address	192.168.1.209
OpenWrt 21 or later.	

It is recommended to factory reset the HH5a.

Power on the HH5a and wait a few minutes. Press and hold the Reset button on the back of the HH5A for at least 10 seconds. Release the button when the main power light starts blinking rapidly in red colour. When the colour changes to a constant green colour, the factory reset is complete.

Alternatively, navigate to **LuCI -> System -> Backup/Flash Firmware** menu. Click on **Perform Reset** button.



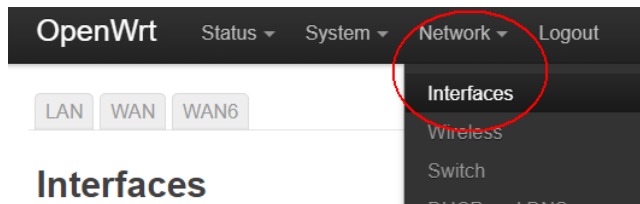
# OpenVPN Server for BT Home Hub 5A

## Edit default LAN IP address

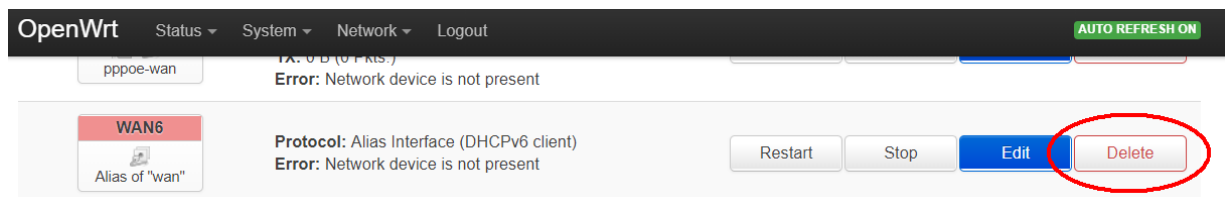
Connect a computer to one of the yellow LAN sockets on the HH5a with an Ethernet cable, and use a web browser and go to 192.168.1.1 and log into LUCI web admin.

Do **not** connect anything to the red WAN port at this time.

In LuCI and go to Network -> Interfaces.

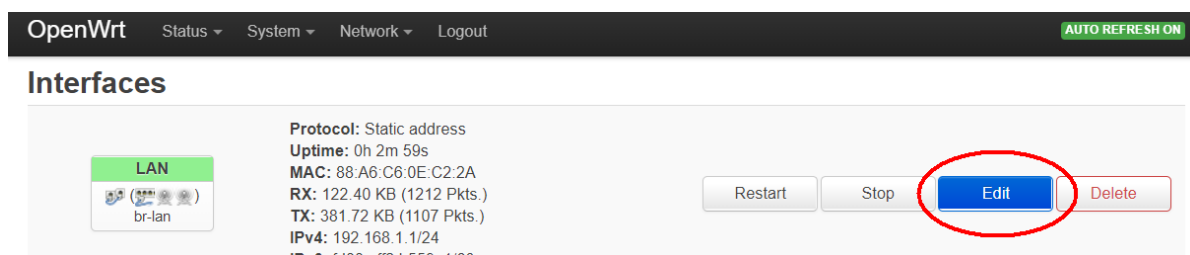


IPv6 is beyond the scope of this document, so you may wish to delete the WAN6 interface.



Press 'Save & Apply' button at the bottom of the page.

Navigate to Network -> Interfaces -> LAN.

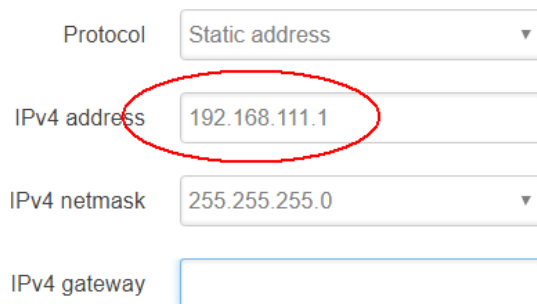


Click on 'Edit' button.

# IMPORTANT:

If necessary, change the LAN IP address of the HH5a to use a different subnet (eg. 192.168.111.x). **Do NOT** use the same subnet, such as 192.168.1.x, on both WAN and LAN interfaces.

This example shows 192.168.111.1 assigned to the LAN interface of the HH5A.



Protocol: Static address

IPv4 address: 192.168.111.1

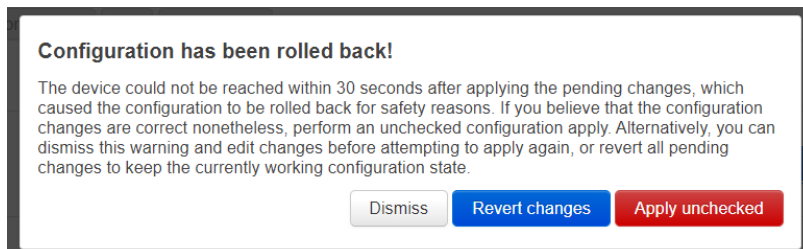
IPv4 netmask: 255.255.255.0

IPv4 gateway:

Press 'Save' button.

Press 'Save & Apply' button at bottom of the page.

The following prompt will appear after 30 seconds.



Simply click on the Apply unchecked button to continue.

After another 30 seconds has elapsed, the following message is likely to appear, to confirm the IP address has successfully changed.

### Device unreachable!

Could not regain access to the device after applying the configuration changes. You might need to reconnect if you modified network related settings such as the IP address or wireless security credentials.

```
uci set network.lan.ipaddr='192.168.111.1'
uci commit
/etc/init.d/network restart
```

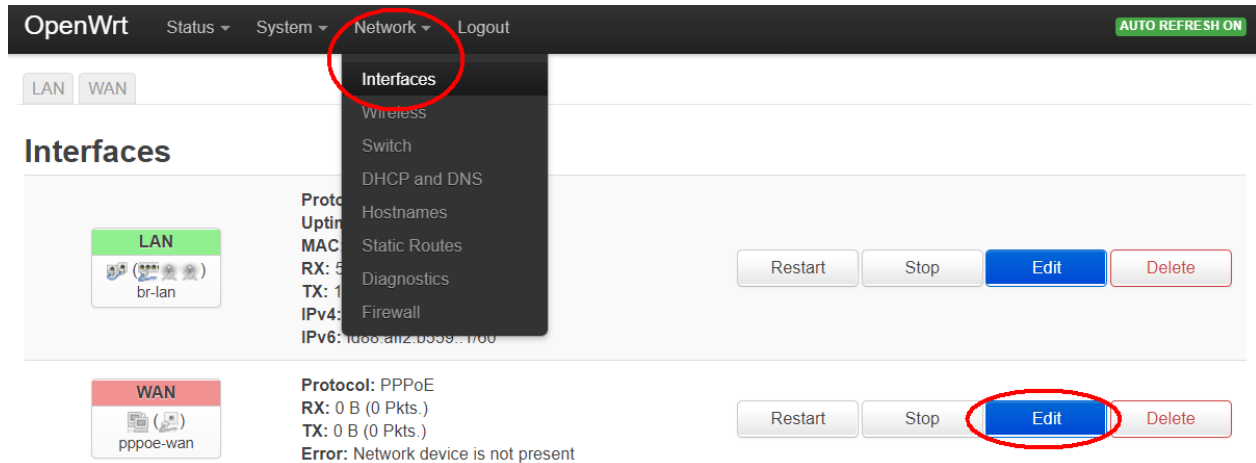
[illegible]

# OpenVPN Server for BT Home Hub 5A

The next step is to edit the WAN interface settings.

Navigate to Network -> Interfaces -> WAN.

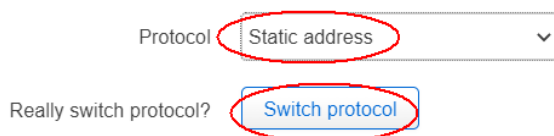
For the 'WAN' interface, click 'Edit'.



The default protocol for most routers is 'DHCP client', but as the HH5a is a modem-router, its default is 'PPPoE'.

As this will be a server it is recommended to change the Protocol to use 'Static Address'.

Click on 'Switch Protocol' button.



Press 'Save' button.

Press 'Save & Apply' button at the bottom of the page.

For 'Static address', complete the remaining fields.

For this example, the main ISP facing router has LAN IP address 192.168.1.1, and 192.168.1.209 is unlikely to be in use, so has been chosen for the HH5a WAN interface. 8.8.8.8 is Google's DNS server. Use these settings:



# OpenVPN Server for BT Home Hub 5A

IPv4 address: 192.168.1.209  
IPv4 gateway: 192.168.1.1 (ie. the LAN IP address of your ISP facing router)  
DNS servers: 8.8.8.8 and 8.8.4.4 (Google servers)

Protocol: Static address

Device: eth0.2

Bring up on boot: ☒

IPv4 address: 192.168.1.209

IPv4 netmask: 255.255.255.0

IPv4 gateway: 192.168.1.1

## Modem-router Owners Only:

This is specific to routers which possess a Lantiq based DSL modem. For all other cable routers, you can review and skip past the following step.

Next select device called 'eth0.2' for the HH5a modem-router, click on 'Device' pull down.

Interfaces » WAN

General Settings | Advanced Settings | Firewall Settings | DHCP Server

Status: Device: dsl0.101  
RX: 0 B (0 Pkts.)  
TX: 0 B (0 Pkts.)  
Error: Network device is not present

Protocol: DHCP client

Device: eth0.2

Bring up on boot: ☐

Hostname to send when requesting DHCP:

Device selection dropdown:

- unspecified
- Bridge: "br-lan" (lan)
- Ethernet Switch: "eth0"
- Switch VLAN: "eth0.1"
- Switch VLAN: "eth0.2"**
- Wireless Network Master "OpenWrt" (lan)

# OpenVPN Server for BT Home Hub 5A

Press 'Save' button.

Press 'Save & Apply' button at the bottom of the page.

## All router owners:

Navigate to Network -> Interfaces -> WAN.

For the 'WAN' interface, click 'Edit'.

Click on 'Advanced Settings' tab

### Interfaces » WAN

General Settings **Advanced Settings** Firewall Settings DHCP Server

Force link ☒ ? Set interface properties regardless of the li

Use default gateway ☒ ? If unchecked, no default route is configure

Use custom DNS servers

8.8.8.8	x
8.8.4.4	x
	+

Press 'Save' button.

Press 'Save & Apply' button at the bottom of the page.

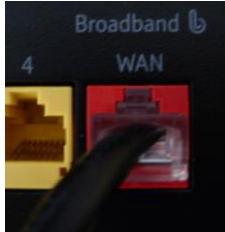
Save & Apply Save Reset

# OpenVPN Server for BT Home Hub 5A

---

**For HH5a owners**, complete the steps described in [section 3](#) to disable DSL\_Control. This is **very important** to ensure the HH5a does not randomly reboot when completing the lengthy procedure described in the following pages.

The next step is to download and install the OpenVPN server packages.



Connect an Ethernet cable from the red ethernet WAN port of the HH5a to a vacant LAN socket on your internet wired router.

Verify there is internet access by browsing websites and running a speed test before proceeding any further.

## DDNS


If your ISP does not provide a static address, then consider installing DDNS on your ISP facing internet router if possible.

Alternatively, see section 9.16 of the 'OpenWrt/LEDE installation guide for HH5a' to set up the free DuckDNS service on this HH5a OpenVPN server.

## 2.2 Downloading and configuring OpenVPN server

Next to follow the steps published in the OpenWrt wiki. For beginners, the command line method looks very daunting at first, but in reality it is pretty much a simple 'copy and paste' exercise.

<https://OpenWrt.org/docs/guide-user/services/vpn/openvpn/server>

OpenWrt

Supported devices

Packages

Downloads

Documentation

Quick start guide

User guide

Developer guide

Security

FAQ

Forum

Contributing

Submitting patches

Reporting bugs

Contributing to wiki

Project

About OpenWrt

Rules

Infrastructure

Donate

Merchandise

Website

Trademark policy

License

Contacts

# OpenVPN server

This article relies on the following:

- [Accessing OpenWrt CLI](#)
- [Managing configurations](#)
- [Managing packages](#)
- [Managing services](#)

## Introduction

- This how-to describes the method for setting up w/ [OpenVPN](#) server on [OpenWrt](#)
- Follow [OpenVPN](#) client for client setup and [OpenVPN extras](#) for additional tuning.

## Goals

- Encrypt your internet connection to enforce security and privacy.
  - Prevent data leak and traffic spoofing on the client side.
- Bypass regional restrictions using commercial providers.
  - Escape client side content filters and internet censorship.
- Access your [LAN](#) services remotely without port forwarding.

## Command-line instructions

### 1. Preparation

Install the required packages. Specify the [VPN](#) server configuration parameters.

```
# Install packages
opkg update
opkg install openvpn-openssl openvpn-easy-rsa

# Configuration parameters
```

[illegible]

---

# OpenVPN Server for BT Home Hub 5A

There are four batches of commands to be executed. They are for:

- Preparation
- Key Management
- Firewall
- VPN service

It is simply a matter of copy and pasting all the commands in each section into PuTTY.

eg. you could choose to blindly highlight and copy all the commands listed within the 'Preparation' section (including the comments with lines beginning with #) from the OpenWrt wiki page, and paste them into PuTTY to execute.

## 1. Preparation

Install the required packages. Specify the VPN server configuration p

```
# Install packages
opkg update
opkg install openvpn-openssl openvpn-easy-rsa

# Configuration parameters
OVPN_DIR="/etc/openvpn"
OVPN_PKI="/etc/easy-rsa/pki"
OVPN_PORT="1194"
OVPN_PROTO="udp"
OVPN_POOL="192.168.8.0 255.255.255.0"
OVPN_DNS="${OVPN_POOL%.*}.1"
OVPN_DOMAIN="$(uci get dhcp.@dnsmasq[0].domain)"

# Fetch WAN IP address
. /lib/functions/network.sh
network_flush_cache
network_find_wan NET_IF
network_get_ipaddr NET_ADDR "${NET_IF}"
OVPN_SERV="${NET_ADDR}"

# Fetch FQDN from DNS client
NET_FQDN="$(uci -q get ddns.@service[0].lookup_host)"
if [ -n "${NET_FQDN}" ]
then OVPN_SERV="${NET_FQDN}"
fi
```

(Do not try to highlight, copy and paste from above image. It will not work)

However, I found during brief testing, some commands may fail. For example, if the 'opkg update' fails early in the script, it causes other commands such as 'opkg install' to fail within the 'Preparation' list of commands. Re-running the commands seems to resolve the problem.

For this reason and educational purposes, this guide will break down each batch of commands into smaller tasks, so you can observe the results as they are executed.

## Preparation

Execute the two commands to download the required packages, by highlighting the first command from the OpenWrt wiki page as shown below.

## OpenVPN Server for BT Home Hub 5A

```
# Install packages
opkg update
opkg install openvpn-openssl openvpn-easy-rsa
```

Do not try to highlight, copy and paste from above image. It will not work.

Now Copy the highlighted single 'opkg update' command line. To paste the command into PuTTY, simply move the mouse pointer to anywhere in the black space within the PuTTY screen and click on the right mouse or trackpad button.

```
root@OpenWrt:~#
root@OpenWrt:~# opkg update
Downloading https://downloads.openwrt.org/
/packages/Packages.gz
Updated list of available packages in /var
Downloading https://downloads.openwrt.org/
```

Press the Enter/Return key to ensure the command has been successfully completed.

Repeat the process. Copy and paste the next opkg install command line.

```
# Install packages
opkg update
opkg install openvpn-openssl openvpn-easy-rsa
```

```
Signature check passed.
root@OpenWrt:~# opkg install openvpn-openssl openvpn-easy-rsa
Installing openvpn-openssl (2.5.3-3) to root...
Downloading https://downloads.openwrt.org/releases/21.02.1/package
```

Press the Enter/Return key to ensure the command has been successfully completed.

The following should appear if the packages have been successfully installed.

```
Configuring kmod-tun.
Configuring libopenssl1.1.
Configuring libopenssl-conf.
Configuring openssl-util.
Configuring liblzo2.
Configuring openvpn-openssl.
Configuring openvpn-easy-rsa.
root@OpenWrt:~#
```

Next highlight the remainder of the Preparation commands as shown below, and copy and paste all lines shown below in one go. (No need to copy and paste each line individually).

# OpenVPN Server for BT Home Hub 5A

The wiki presumes standard UDP protocol and port number 1194 will be used. (Alternative is TCP protocol and port 443 as used for HTTPS traffic)

```
# Install packages
opkg update
opkg install openvpn-openssl openvpn-easy-rsa

# Configuration parameters
OVPN_DIR="/etc/openvpn"
OVPN_PKI="/etc/easy-rsa/pki"
OVPN_PORT="1194"
OVPN_PROTO="udp"
OVPN_POOL="192.168.8.0 255.255.255.0"
OVPN_DNS="${OVPN_POOL%.* *} .1"
OVPN_DOMAIN="$(uci get dhcp.@dnsmasq[0].domain)"

# Fetch WAN IP address
. /lib/functions/network.sh
network_flush_cache
network_find_wan NET_IF
network_get_ipaddr NET_ADDR "${NET_IF}"
OVPN_SERV="${NET_ADDR}"

# Fetch FQDN from DDNS client
NET_FQDN="$(uci -q get ddns.@service[0].lookup_host)"
if [ -n "${NET_FQDN}" ]
then OVPN_SERV="${NET_FQDN}"
fi
```


```
root@TPlinkFixRouter: ~
OVPN_POOL="192.168.8.0 255.255.255.0"
root@TPlinkFixRouter:~# OVPN_DIR="/etc/openvpn"
root@TPlinkFixRouter:~# OVPN_PKI="/etc/easy-rsa/pki"
root@TPlinkFixRouter:~# OVPN_PORT="1194"
# Fetch WAN IP address
root@TPlinkFixRouter:~# OVPN_PROTO="udp"
. /lib/functions/network.sh
root@TPlinkFixRouter:~# OVPN_POOL="192.168.8.0 255.255.255.0"
root@TPlinkFixRouter:~# OVPN_DNS="${OVPN_POOL%.* *} .1"
root@TPlinkFixRouter:~# OVPN_DOMAIN="$(uci get dhcp.@dnsmasq[0].domain)"
root@TPlinkFixRouter:~#
root@TPlinkFixRouter:~# # Fetch WAN IP address
root@TPlinkFixRouter:~# . /lib/functions/network.sh
root@TPlinkFixRouter:~# network_flush_cache
root@TPlinkFixRouter:~# network_find_wan NET_IF
root@TPlinkFixRouter:~# network_get_ipaddr NET_ADDR "${NET_IF}"
root@TPlinkFixRouter:~# OVPN_SERV="${NET_ADDR}"
root@TPlinkFixRouter:~#
root@TPlinkFixRouter:~# # Fetch FQDN from DDNS client
root@TPlinkFixRouter:~# NET_FQDN="$(uci -q get ddns.@service[0].lookup_host)"
root@TPlinkFixRouter:~# if [ -n "${NET_FQDN}" ]
> then OVPN_SERV="${NET_FQDN}"
> fi
root@TPlinkFixRouter:~#
```

Press the Enter/Return key to ensure the command has been successfully completed.

## Key Management

Copy and paste the first 6 command lines as shown below

### 2. Key management

Use  EasyRSA to manage the PKI. Utilize private

```
# Configuration parameters
export EASYRSA_PKI="${OVPN_PKI}"
export EASYRSA_REQ_CN="ovpnca"
export EASYRSA_BATCH="1"

# Remove and re-initialize PKI directory
easyrsa init-pki

# Generate DH parameters
```

```
root@TPlinkFixRouter:~#
root@TPlinkFixRouter:~# # Configuration parameters
root@TPlinkFixRouter:~# export EASYRSA_PKI="${OVPN_PKI}"
root@TPlinkFixRouter:~# export EASYRSA_REQ_CN="ovpnca"
root@TPlinkFixRouter:~# export EASYRSA_BATCH="1"
root@TPlinkFixRouter:~#
root@TPlinkFixRouter:~# # Remove and re-initialize PKI directory
root@TPlinkFixRouter:~# easyrsa init-pki
root@TPlinkFixRouter:~#
```

Press the Enter/Return key to ensure the command has been successfully completed.

Copy and paste this command

```
easyrsa init-pki

# Generate DH parameters
easyrsa gen-dh

# Create a new CA
```



[illegible]

For the MIPs powered HH5a, the above step takes **55** minutes to complete on OpenWrt 21.02.1. By comparison, the ARM powered Linksys EA6350 v3 can complete same task in less 5 minutes on 21.02.1!

For OpenWrt 19.07.7, DH generation takes less than 20 minutes on HH5a.

Copy and paste the single line.

```
# Create a new CA
easysrsa build-ca nopass
```

```
root@openwrt:~#  
root@OpenWrt:~#  
root@OpenWrt:~# easyrsa build-ca nopass  
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021  
Generating RSA private key, 2048 bit long modulus (2 primes)  
.....+++++  
.....+++++  
e is 65537 (0x010001)
```

Press the `Enter/Return` key to ensure the command has been successfully completed.

Copy and paste the single line.

```
# Generate server keys and certificate
easysrsa build-server-full server nopass
openvpn --genkey tls-crypt-v2-server ${EASYSRSA_PKI}/private/server.pem
```

## OpenVPN Server for BT Home Hub 5A

```
root@OpenWrt:~# easyrsa build-server-full server nopass
Using SSL: openssl OpenSSL 1.1.1l  24 Aug 2021
Generating a RSA private key
....+++++
.....
writing new private key to '/etc/easy-rsa/pki/easy-rsa-1320
-----
Using configuration from /etc/easy-rsa/pki/easy-rsa-13208.3
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :ASN.1 12:'server'
Certificate is to be certified until Mar 26 15:37:06 2024 0
Write out database with 1 new entries
Data Base Updated
```

Press the Enter/Return key to ensure the command has been successfully completed.

Copy and paste the next single line.

```
# Generate server keys and certificate
easyrsa build-server-full server nopass
openvpn --genkey tls-crypt-v2-server ${EASYRSA_PKI}/private/server.pem
```

```
root@OpenWrt:~# openvpn --genkey tls-crypt-v2-server ${EASYRSA_PKI}/private/serv
er.pem
root@OpenWrt:~# █
```

Press the Enter/Return key to ensure the command has been successfully completed.

Copy and paste the single line.

```
# Generate client keys and certificate
easyrsa build-client-full client nopass
openvpn --tls-crypt-v2 ${EASYRSA_PKI}/private/server.pem \
--genkey tls-crypt-v2-client ${EASYRSA_PKI}/private/client.pem
```

## OpenVPN Server for BT Home Hub 5A

```
root@OpenWrt:~# easyrsa build-client-full client nopass
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/easy-rsa/pki/easy-rsa-132
-----
Using configuration from /etc/easy-rsa/pki/easy-rsa-13286.
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :ASN.1 12:'client'
Certificate is to be certified until Mar 26 15:40:04 2024

Write out database with 1 new entries
Data Base Updated
```

Press the Enter/Return key to ensure the command has been successfully completed.

Copy and paste the next VERY LONG single command line.

```
# Generate client keys and certificate
easyrsa build-client-full client nopass
openvpn --tls-crypt-v2 ${EASYRSA_PKI}/private/server.pem \
--genkey tls-crypt-v2-client ${EASYRSA_PKI}/private/client.pem
```

```
root@OpenWrt:~# openvpn --tls-crypt-v2 ${EASYRSA_PKI}/private/server.pem \
> --genkey tls-crypt-v2-client ${EASYRSA_PKI}/private/client.pem
root@OpenWrt:~#
```

Press the Enter/Return key to ensure the command has been successfully completed.

## Firewall

Copy and paste ALL of the commands.

## OpenVPN Server for BT Home Hub 5A

```
# Configure firewall
uci rename firewall.@zone[0]="lan"
uci rename firewall.@zone[1]="wan"
uci del_list firewall.lan.device="tun+"
uci add_list firewall.lan.device="tun+"
uci -q delete firewall.ovpn
uci set firewall.ovpn="rule"
uci set firewall.ovpn.name="Allow-OpenVPN"
uci set firewall.ovpn.src="wan"
uci set firewall.ovpn.dest_port="${OVPN_PORT}"
uci set firewall.ovpn.proto="${OVPN_PROTO}"
uci set firewall.ovpn.target="ACCEPT"
uci commit firewall
/etc/init.d/firewall restart
```

```
root@OpenWrt:~#
root@OpenWrt:~# uci rename firewall.@zone[0]="lan"
uci rename firewall.@zone[1]="wan"
uci del_list firewall.lan.device="tun+"
uci add_list firewall.lan.device="tun+"
uci -q delete firewall.ovpn
uci set firewall.ovpn="rule"
uci set firewall.ovpn.name="Allow-OpenVPN"
uci set firewall.ovpn.src="wan"
uci set firewall.ovpn.dest_port="${OVPN_PORT}"
uci set firewall.ovpn.proto="${OVPN_PROTO}"
uci set firewall.ovpn.target="ACCEPT"
uci commit firewall
/etc/init.d/firewall restart
```

Press the **Enter/Return** key to ensure the command has been successfully completed.

The following should appear on execution for OpenWrt 21.02:

**Added:** Nothing will be returned for OpenWrt 22.03.0-rc6 when tested.

```
* Zone 'lan'
* Zone 'wan'
* Populating IPv6 mangle table
* Zone 'lan'
* Zone 'wan'
* Set tcp_ecn to off
* Set tcp_syncookies to on
* Set tcp_window_scaling to on
* Running script '/etc/firewall.user'
root@OpenWrt:~#
```

(fyi, Allow-OpenVPN rule will appear in 'Traffic Rules' in 'Firewall' menu in LUCI)

# OpenVPN Server for BT Home Hub 5A

## VPN Service

Copy and paste ALL of the commands.

### 4. VPN service

Configure VPN service and generate client profiles.

```
# Configure VPN service and generate client profiles
umask go=
OVPN_DH="$(cat ${OVPN_PKI}/dh.pem)"
OVPN_CA="$(openssl x509 -in ${OVPN_PKI}/ca.crt)"
ls ${OVPN_PKI}/issued \
| sed -e "s/\.\w*//" \
| while read -r OVPN_ID
do
    OVPN_CA="$(openssl x509 -in ${OVPN_PKI}/ca.crt)"
    OVPN_TC="$(cat ${OVPN_PKI}/private/${OVPN_ID}.pem)"
    OVPN_KEY="$(cat ${OVPN_PKI}/private/${OVPN_ID}.key)"
    OVPN_CERT="$(openssl x509 -in ${OVPN_PKI}/issued/${OVPN_ID}.crt)"
    OVPN_EKU="$(echo "${OVPN_CERT}" | openssl x509 -noout -purpose)"
    case ${OVPN_EKU} in
        (*All server : Yes*))
            OVPN_CONF="$(cat ${OVPN_PKI}/${OVPN_ID}.conf)"
            cat << EOF > ${OVPN_CONF} ;;
        user nobody
        group nogroup
        dev tun
        port ${OVPN_PORT}
        proto ${OVPN_PROTO}
        server ${OVPN_ADDR}
        topology subnet
        client-to-client
        keepalive 10 60
        persist-tun
        persist-key
        push "dhcp-option DNS ${OVPN_DNS}"
        push "dhcp-option DOMAIN ${OVPN_DOMAIN}"
        push "redirect-gateway def1"
        push "persist-tun"
        push "persist-key"
        cd ${OVPN_DIR}
        c/df
        rm
        (*All client : Yes*)
        OVPN_CONF="$(cat ${OVPN_PKI}/${OVPN_ID}.conf)"
        cat << EOF > ${OVPN_CONF} ;;
        user nobody
        group nogroup
        dev tun
        mode1
        client
        remote ${OVPN_ADDR} ${OVPN_PORT} ${OVPN_PROTO}
        auth-no-cache
        remote-cert-tls server
        top
        ec2
        cat << EOF > ${OVPN_CONF}
        tls-crypt-req
        ${OVPN_TC}
        c/tls-crypt-req
        ckey
        ${OVPN_KEY}
        c/keys
        ccert
        ${OVPN_CERT}
        c/cert
        ccas
        ${OVPN_CA}
        c/cas
        rm
        done
    /etc/init.d/openvpn restart
    ls ${OVPN_DIR}/${OVPN_ID}.ovpn
```

Starts with

```
root@OpenWrt:~#
root@OpenWrt:~# umask go=
root@OpenWrt:~# OVPN_DH="$(cat ${OVPN_PKI}/dh.pem)"
OVPN_CA="$(openssl x509 -in ${OVPN_PKI}/ca.crt)"
ls ${OVPN_PKI}/issued \
| sed -e "s/\.\w*//" \
| while read -r OVPN_ID
do
    root@OpenWrt:~# OVPN_CA="$(openssl x509 -in ${OVPN_PKI}/ca.crt)"
    OVPN_TC="$(cat ${OVPN_PKI}/private/${OVPN_ID}.pem)"
    OVPN_KEY="$(cat ${OVPN_PKI}/private/${OVPN_ID}.key)"
    OVPN_CERT="$(openssl x509 -in ${OVPN_PKI}/issued/${OVPN_ID}.crt)"
    OVPN_EKU="$(echo "${OVPN_CERT}" | openssl x509 -noout -purpose)"
    case ${OVPN_EKU} in
        (*All server : Yes*))
```

Finishes with:

# OpenVPN Server for BT Home Hub 5A

---

```
> <cert>
> ${OVPN_CERT}
> </cert>
> <ca>
> ${OVPN_CA}
> </ca>
> EOF
> done
root@OpenWrt:~# /etc/init.d/openvpn restart
root@OpenWrt:~# ls ${OVPN_DIR}/*.ovpn
/etc/openvpn/client.ovpn
root@OpenWrt:~#
```

Press the `Enter/Return` key to ensure the command has been successfully completed.

If you are installing OpenVPN server directly onto a single fully functioning ISP facing router running OpenWrt, you can skip section 2.3, and jump to section 2.4, [retrieving and editing the client.ovpn file](#).

## 2.3 Configure Port forwarding rule on ISP facing router

As the HH5a is behind another 'router', the next step is to configure a firewall rule on the ISP facing router. This will allow openvpn clients from the internet to reach the OpenVPN server.


The following parameters are required:

IPv4 address of OpenVPN server WAN port	192.168.1.209	(for this example)
Port number	1194	(default)
Protocol	UDP	(default)

Note in these following examples, the `External Port` number has been deliberately changed from 1194 to 31195. OpenVPN clients on the internet must use UDP protocol on port 31195 to connect to this OpenVPN server. You can of course choose to use default port no. 1194.

### AsusWRT router


# OpenVPN Server for BT Home Hub 5A

Port Forwarding List (Max Limit : 32)						
Service Name	Source Target	Port Range	Local IP	Local Port	Protocol	Add / Delete
openvpnServer		31195	192.168.1.209	1194	UDP	

## OpenWrt router



nb. This is **NOT** the HH5a running OpenVPN server!

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
OpenVPNserver	UDP	wan	31195	lan	192.168.1.209	1194	

## TPlink router


### Virtual Servers

 Add  Delete

<input type="checkbox"/>	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
<input type="checkbox"/>	--	--	--	--	--	--	--	--

Service Type:

openVPNserver



External Port:

31195

(XX-XX or XX)

Internal IP:

192.168.1.209

Internal Port:

1194

(XX or Blank ,1-65535)

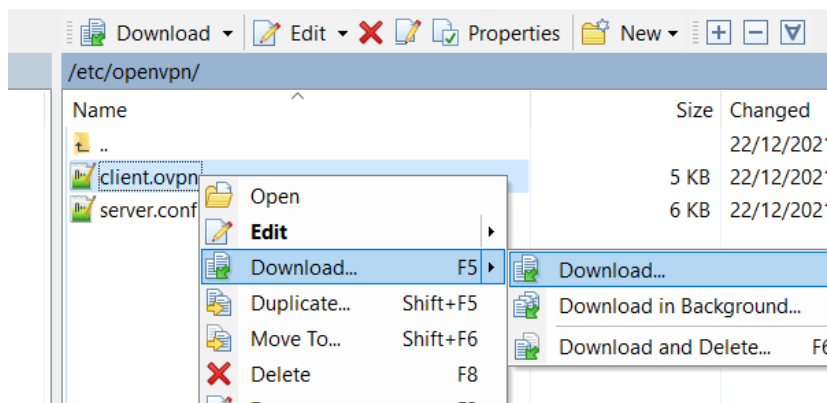
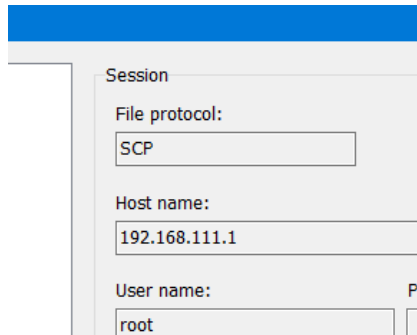
Protocol:

UDP

☒ Enable This Entry

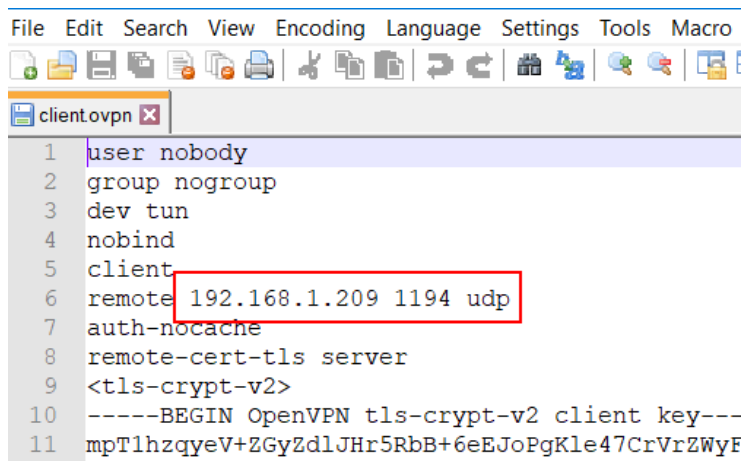
## 2.4 Download and editing the client ovpn file

Use WinSCP to retrieve the `client.ovpn` file from the HH5a to a computer.



Use Notepad++ to open the `client.ovpn` file.

The WAN IP address of the HH5a (eg. 192.168.1.209) and the default port number, 1194, used by openvpn server may be visible.





# OpenVPN Server for BT Home Hub 5A

The IP address and the port number contained within the original `client.ovpn` file should be modified where necessary.

If your ISP has assigned a static IP address to your internet connection, use that IP address.

If you use DDNS, enter the fully qualified domain name. eg. `mytestDNS.duckdns.org`

```
1 user nobody
2 group nogroup
3 dev tun
4 nobind
5 client
6 remote mytestDNS.duckdns.org 31195 udp
7 auth-nocache
8 remote-cert-tls server
9 <tls-crypt-v2>
10 -----BEGIN OpenVPN tls-crypt-v2 client key--
```

Don't forget to edit the port number if necessary! (eg. port 31195 in above example)

If you don't yet use DDNS, and you don't have a static IP address assigned by your ISP, you can obtain your current dynamic IP address assigned to your broadband connection by visiting websites such as `myip.com`



Enter the reported IP address into the `client.ovpn` file.

**Warning:** The dynamic IP address of your internet connection could change.

(see section 9.16 of the 'OpenWrt/LEDE installation guide for HH5a to set up the free DuckDNS service)

## 2.5 Configuring the OpenVPN Client

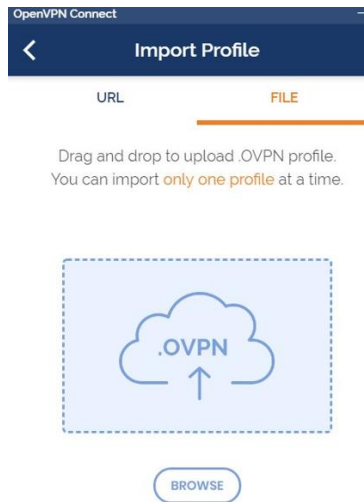
### Microsoft Windows

# OpenVPN Server for BT Home Hub 5A

Download and install the OpenVPN Connect for Windows client

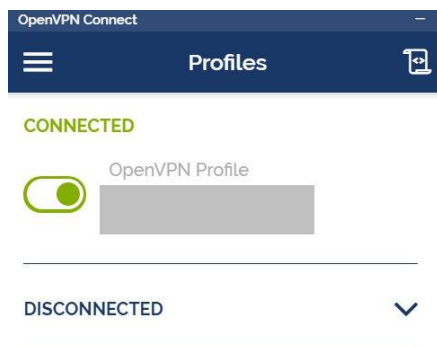
<https://openvpn.net/client-connect-vpn-for-windows/>

Start the OpenVPN Connect client and click on the '+' button to add an ovpn file.

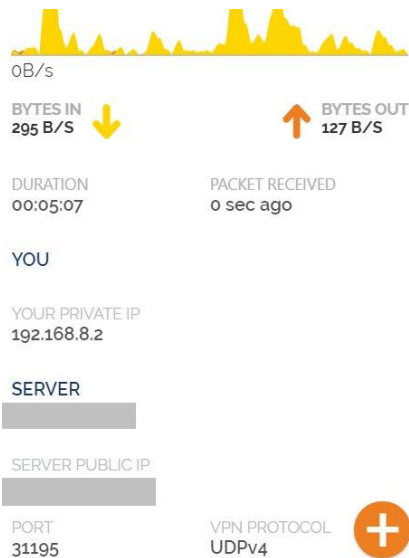


Load the edited `client.ovpn` file and move the slider button to connect to the OpenVPN server.

Here is screen capture of a successful openvpn connection.



# OpenVPN Server for BT Home Hub 5A



Observe the PC has a LAN IP address of 192.168.8.2 in this example. It is NOT on the same subnet 192.168.111.x as the HH5a.

## Android

Simply go to the Google Play store and install the OpenVPN Connect app.



### OpenVPN Connect – Fast & Safe SSL VPN Client

OpenVPN Tools

★★★★★ 174,885

PEGI 3

This app is available for your device

Installed

**Tip:** for smartphone users, create an email and include the `client.ovpn` file as an attachment on the computer.

Open the email.

When you try to view the attachment, you will get an error. Click on button to save the file attachment to the phone's storage.

Launch the OpenVPN Connect app.

# OpenVPN Server for BT Home Hub 5A

---

The `client.ovpn` file will probably be located in '**Internal Storage**' > '**Download**' folder.

## 2.6 LED configuration

Go to `System -> LED Configuration` menu. You may wish to edit the existing LED configuration for 'Internet' as shown below. The 'b' (broadband) indicator will light up.

Edit the settings by renaming the original 'dsl' LED configuration as shown below:

### LED Configuration

Name	<input type="text" value="dsl"/>
LED Name	<input type="text" value="blue:broadband"/>
Trigger	<input type="text" value="Network device activity (kernel: r"/>
Device	<input type="text" value="tun0"/>
Trigger Mode	<input type="text" value="Link On"/>

## 2.7 Frequently Asked Questions

Q. Can I use LuCI to manage the configured OpenVPN server configuration?

A. No. LuCI is not at this time compatible with the command-line method described in the OpenWrt wiki article.

Q. The maximum openvpn transfer speed is only 9Mbps. How can I increase the speed?

A. You could explore using Wireguard protocol. Otherwise, get a faster (and more expensive) router which supports OpenWrt, or consider alternatives such as Asus ARM powered routers using Broadcom SoC capable of running stock or RMerlin AsusWrt. Eg. RT-AC86u.

## OpenVPN Server for BT Home Hub 5A

---

Q. The HH5a sits behind the ISP router. I can ping both the OpenVPN server and the ISP facing router LAN IP addresses, but I can't ping a Windows PC?

A. The Windows firewall on the PC is likely to be blocking icmp ping requests. Verify you can ping another device such as a printer on the same subnet as the Windows PC.

Q. I can connect to the OpenVPN server when my remote device is on the LAN, but when I try to connect from a remote location or using 4G/5G, it fails.

A. Check the IP address/hostname and the port number specified in the `client.ovpn` for errors. Also check port forwarding rule is correctly configured if the HH5a is behind an ISP router.

Q. Will the OpenVPN server operate on a Carrier Grade NAT (CGNAT) internet service?

A. No, to the best of my knowledge. CGNAT shares the same IP address with multiple customers. Contact the ISP to see if they offer a non-CGNAT solution.

Q. I am trying to follow the latest wiki instructions to install OpenVPN server onto OpenWrt 19.07, and it does not work. The OpenVPN client reports tls-crypt parsing error when trying to open the ovpn file.

A. Please refer to an older article to resolve the issue.

<https://OpenWrt.org/docs/guide-user/services/vpn/openvpn/server?rev=1632708683>

Q. Key generation is horrendously slow on HH5a, can I generate the keys on a faster PC and use them in OpenWrt?

A. Yes, see this thread for more information.

<https://forum.openwrt.org/t/openvpn-server-generate-dh-parameters-on-pc-then-import-them-to-openwrt/150103>

## 2.8 OpenWrt settings

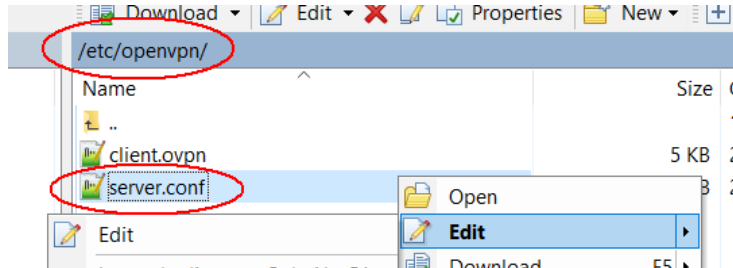
From OpenWrt 21.02 installation.

### OpenVPN

# OpenVPN Server for BT Home Hub 5A

See [section 2.4](#) with regards to the `client.ovpn` settings file.

The openvpn server settings are found within `/etc/openvpn/server.conf`



Contents of `/etc/openvpn/server.conf`

```
/etc/openvpn/server.conf - 192.168.111.1 - Editor - WinSCP
user nobody
group nogroup
dev tun
port 1194
proto udp
server 192.168.8.0 255.255.255.0
topology subnet
client-to-client
keepalive 10 60
persist-tun
persist-key
push "dhcp-option DNS 192.168.8.1"
push "dhcp-option DOMAIN lan"
push "redirect-gateway def1"
push "persist-tun"
push "persist-key"
<dh>
-----BEGIN DH PARAMETERS-----
```

There is also the `/etc/config/openvpn` config file. As far as I'm aware, this is not used at all. TBC.

## Firewall

### Traffic Rule

Allow-OpenVPN

Incoming *IPv4* and *IPv6*, protocol *UDP*

From wan

*Accept* input



To this device, port 1194

## LAN zone setting

### Firewall - Zone Settings

General Settings

Advanced Settings

Conntrack Settings

Extra iptables arguments

The options below control the forwarding policies between this zone (lan) and other zones. **lan**. *Source zones* match forwarded traffic from other zones **targeted at lan**. The forwarding *not* imply a permission to forward from wan to lan as well.

Covered devices	<input checked="" type="checkbox"/> tun+
Covered subnets	<input type="checkbox"/> Bridge: "br-lan" (lan) <input type="checkbox"/> Ethernet Switch: "eth0" <input type="checkbox"/> Switch VLAN: "eth0.1" <input type="checkbox"/> Switch VLAN: "eth0.2" (wan) <input type="checkbox"/> Ethernet Adapter: "tun0" <input type="checkbox"/> Wireless Network: Master "OpenWrt" (lan) <input type="checkbox"/> Wireless Network: Master "OpenWrt" (lan) <input checked="" type="checkbox"/> Absent Interface: "tun+" <input type="checkbox"/> -- custom --
Restrict to address family	
Restrict Masquerading to given source subnets	
Restrict Masquerading to given	

# OpenVPN Server for BT Home Hub 5A

Changes to /etc/config/firewall config file

```
/etc/config/firewall - 192.168.111.1 - Editor - WinSCP

config zone 'lan'
    option name 'lan'
    option input 'ACCEPT'
    option output 'ACCEPT'
    option forward 'ACCEPT'
    list network 'lan'
    list device 'tun+'

config rule 'ovpn'
    option name 'Allow-OpenVPN'
    option src 'wan'
    option dest_port '1194'
    option proto 'udp'
    option target 'ACCEPT'
```

## System Log

```
Wed Dec 22 16:52:16 2021 daemon.warn openvpn(server)[1974]: --cipher is not set. Previous OpenVPN version defaulted to BF-CBC as fallback when cipher negotiation failed
Wed Dec 22 16:52:16 2021 daemon.notice openvpn(server)[1974]: OpenVPN 2.5.3 mips-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [MH/PKTINFO] [AEAD]
Wed Dec 22 16:52:16 2021 daemon.notice openvpn(server)[1974]: library versions: OpenSSL 1.1.1f 24 Aug 2021, LZO 2.10
Wed Dec 22 16:52:16 2021 daemon.warn openvpn(server)[1974]: NOTE: your local LAN uses the extremely common subnet address 192.168.0.x or 192.168.1.x. Be aware that
Wed Dec 22 16:52:16 2021 daemon.warn openvpn(server)[1974]: NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Wed Dec 22 16:52:17 2021 user.notice firewall: Reloading firewall due to ifup of lan (br-lan)
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: TUN/TAP device tun0 opened
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: net_iface_mtu_set: mtu 1500 for tun0
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: net_iface_up: set tun0 up
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: net_addr_v4_add: 192.168.8.1/24 dev tun0
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: /usr/libexec/openvpn-hotplug up server tun0 1500 1621 192.168.8.1 255.255.255.0 init
Wed Dec 22 16:52:17 2021 daemon.err odhcpd[1542]: Failed to send to ff02::1%lan@br-lan (Address not available)
Wed Dec 22 16:52:17 2021 daemon.warn openvpn(server)[1974]: Could not determine IPv4/IPv6 protocol. Using AF_INET
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: UDPv4 link local (bound): [AF_INET][undef]:1194
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: UDPv4 link remote: [AF_UNSPEC]
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: GID set to nogroup
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: UID set to nobody
Wed Dec 22 16:52:17 2021 daemon.notice openvpn(server)[1974]: Initialization Sequence Completed
```



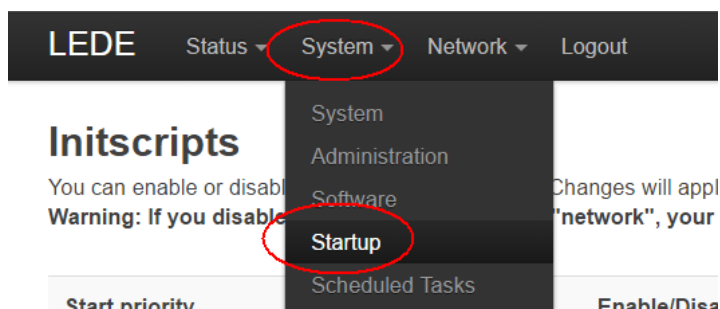
## 3. Bug fixes for Home Hub 5A

### 3.1 How to disable 'dsl\_control' (DSL port)

It appears when the DSL port is not being used, a bug in the VDSL app causes unexpected high load, and can eventually cause the HH5a to crash and reboot without warning. This usually occurs within an hour of starting the HH5A. This issue may also affect other modem routers with Lantiq SoC.

In the meantime, it is recommended to disable 'dsl\_control' if the DSL port won't be used.

Start LUCI and navigate to `System -> Startup` menu



Scroll down until you find 'dsl\_control'. Then click on 'Enabled' and 'Stop' buttons.

96	led	Enabled	Start	Restart	Stop
97	dsl_control	Enabled	Start	Restart	Stop
98	sysntpd	Enabled	Start	Restart	Stop

Ensure that Disabled is displayed as shown below.

core	Enabled	Start
led	Enabled	Start
dsl_control	Disabled	Start
eventd	Enabled	Start

Optionally, shut down and restart the HH5a.

The DSL port is now disabled.

## 3.2 Random WAN port MAC address fix

If the HH5a is configured to use the red Ethernet WAN port, you may observe when using DHCP-client, the WAN port acquires a different IP address every time the hub is power-cycled. This is because the WAN port's MAC address has not been defined properly during boot up. A side effect is if the hub is attached to your LAN, it could use up the pool of DHCP IP addresses if the hub is rebooted very frequently. Fortunately, the WAN port's MAC address does not change during DHCP IP address renewal.

### OpenWrt - up to 19.07

To resolve the issue, start LUCI and navigate to `Network -> Interfaces` menu.

Network	Status	Actions
<b>LAN</b> br-lan	Uptime: 0h 1m 47s <b>MAC-Address: 8C:10:D4:0C:2C:EC</b> RX: 64.77 KB (602 Pkts.) TX: 169.11 KB (576 Pkts.) IPv4: 192.168.1.1/24 IPv6: fdad:4053:2891::1/60	Connect  Stop  Edit
<b>WAN</b> eth1.2	Uptime: 0h 0m 0s <b>MAC-Address: 96:6F:97:AD:8B:9A</b> RX: 0 B (0 Pkts.) TX: 13.05 KB (43 Pkts.)	Connect  Stop  Edit

Notice the MAC addresses for the LAN and WAN interfaces are very different in above example.

Click on 'Edit' and go the 'Advanced Settings' tab.

### Interfaces - WAN

On this page you can configure the network interface  
network interfaces separated by spaces. You can al

#### Common Configuration

[General Setup](#) [Phy](#)

# OpenVPN Server for BT Home Hub 5A

Scroll down the page until you find the 'Override MAC Address' field.



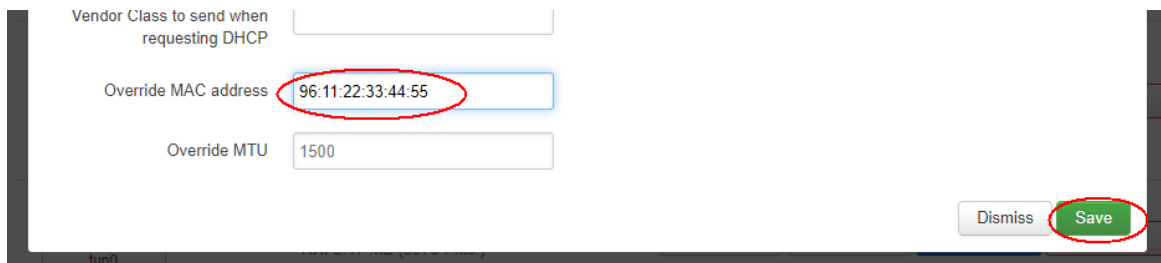
Vendor Class to send when requesting DHCP

Override MAC address 96:6F:97:AD:8B:9A

Override MTU 1500

In the above example, the MAC address beginning '96:6F' changes every time the hub is power cycled.

Enter a new MAC address. Ensure any address you choose is NOT used elsewhere. You can choose to use the MAC address already shown in the above box such as the address beginning '96:6F' if you wish. Ensure the 2<sup>nd</sup> digit is always an even number, such as '6' in example below.



Vendor Class to send when requesting DHCP

Override MAC address 96:11:22:33:44:55

Override MTU 1500

Dismiss Save

Press the 'Save' button

Press the 'Save & Apply' button at the bottom of the page.

## OpenWrt – all versions

The above method is no longer available starting from OpenWrt 21.02, as part of eventual migration to DSA.

Fortunately, you can also fix the problem by editing the 'wan\_dev' section of the /etc/config/network configuration file.

For LEDE 17, search for 'ptm0' as shown below.

For OpenWrt 18, 19 & 21, search for 'ds10'

For dhcp-client mode

## OpenVPN Server for BT Home Hub 5A

---

```
config interface 'wan'
    option ifname 'eth0.2'
    option proto 'dhcp'
    option ipv6 'auto'

config device 'wan_dev'
    option name 'ptm0'          # requires to be changed to 'eth0.2'
    option macaddr 'xx:xx:xx:xx:xx:yy'
```

For LEDE 17, OpenWrt 18 and 19, the existing 'wan\_dev' should be amended to read:

```
config device 'wan_dev'
    option name 'eth0.2'
    option macaddr '78:65:59:ae:fc:51'
```

For OpenWrt 21.02, the option name should be changed from dsl0 to eth0.2:

```
config device
    option name 'eth0.2'
    option macaddr '78:65:59:ae:fc:51'
```

Enter a new MAC address. Ensure any address you choose is NOT in active use elsewhere.

**Important:** Ensure the 2<sup>nd</sup> digit is always an even number, such as '8' in above example images.





Note that if you choose to edit the 'option name' to match what is shown in the 'wan' section, the 'Override MAC address' option in LuCI will no longer work in versions of OpenWrt up to 19.07.

For OpenWrt 21.02, navigate to **LuCI -> Network -> Interfaces -> Devices** tab. You can make further changes by clicking on 'Configure' button in future.

# OpenVPN Server for BT Home Hub 5A

Interfaces **Devices** Global network options DSL ATM Bridges

### Devices


Device	Type	MAC Address	MTU	
 br-lan	Bridge device	78:65:59:AE:FC:50	1500	<a href="#">Config</a>
 eth0.1	Network device	78:65:59:AE:FC:50	1500	<a href="#">Config</a>
 <b>eth0.2</b>	Network device	<b>78:65:59:AE:FC:51</b>	1500	<a href="#">Config</a>
 eth0	Network device	26:8C:E4:4B:97:A2	1500	<a href="#">Config</a>

[Add device configuration...](#)

### Network device: eth0.2

[General device options](#) [Advanced device options](#)

Device type Network device

Existing device  eth0.2

MTU

MAC address

TX queue length

Enable IPv6 ☒

IPv6 MTU

DAD transmits

## OpenWrt - 21.02 only






If you don't wish to use SSH and VI, this alternative method also appears to work but may leave your **/etc/config/network** file looking a bit more complicated

Navigate to **LuCI -> Network -> Interfaces -> Devices** tab

Locate the `'eth0.2'` entry and click **Configure** button.

# OpenVPN Server for BT Home Hub 5A

## Devices

Device	Type	MAC Address	MTU	
 br-lan	Bridge device	78:65:59:AE:FC:50	1500	<a href="#">Configure...</a>
 eth0.1	Network device	78:65:59:AE:FC:50	1500	<a href="#">Configure...</a>
 dsl0	Network device	78:65:59:AE:FC:51	-	<a href="#">Configure...</a>
 eth0	Network device	F2:70:0D:28:94:52	1500	<a href="#">Configure...</a>
 eth0.2	VLAN (802.1q)	F2:70:0D:28:94:52	1500	<a href="#">Configure...</a>

Edit the MAC address field as shown below:

Ensure any address you choose is NOT in active use elsewhere.

**Important:** Ensure the 2<sup>nd</sup> digit is always an even number, such as '8' in the following example image.

## VLAN (802.1q): eth0.2

[General device options](#)

[Advanced device options](#)

Device type

Base device  eth0

VLAN ID

Device name

MTU

MAC address

Press the 'Save' button.

# OpenVPN Server for BT Home Hub 5A

Interfaces





Devices

Global network options

DSL

ATM Bridges

Devices

Device	Type	MAC Address	MTU
 br-lan	Bridge device	78:65:59:AE:FC:50	1500
 eth0.1	Network device	78:65:59:AE:FC:50	1500
 dsl0	Network device	78:65:59:AE:FC:51	-
 eth0.2	VLAN (802.1q)	78:65:59:AE:FC:57	1500

Press the 'Save & Apply' button.

Now reboot the HH5a for the changes to take effect.

The /etc/config/network file will contain a new section:

```
config device
    option name 'eth0.2'
    option type '8021q'
    option ifname 'eth0'
    option vid '2'
    option macaddr '78:65:59:AE:FC:57'
```

