Flash Instructions for Xiaomi Routers

Introduction

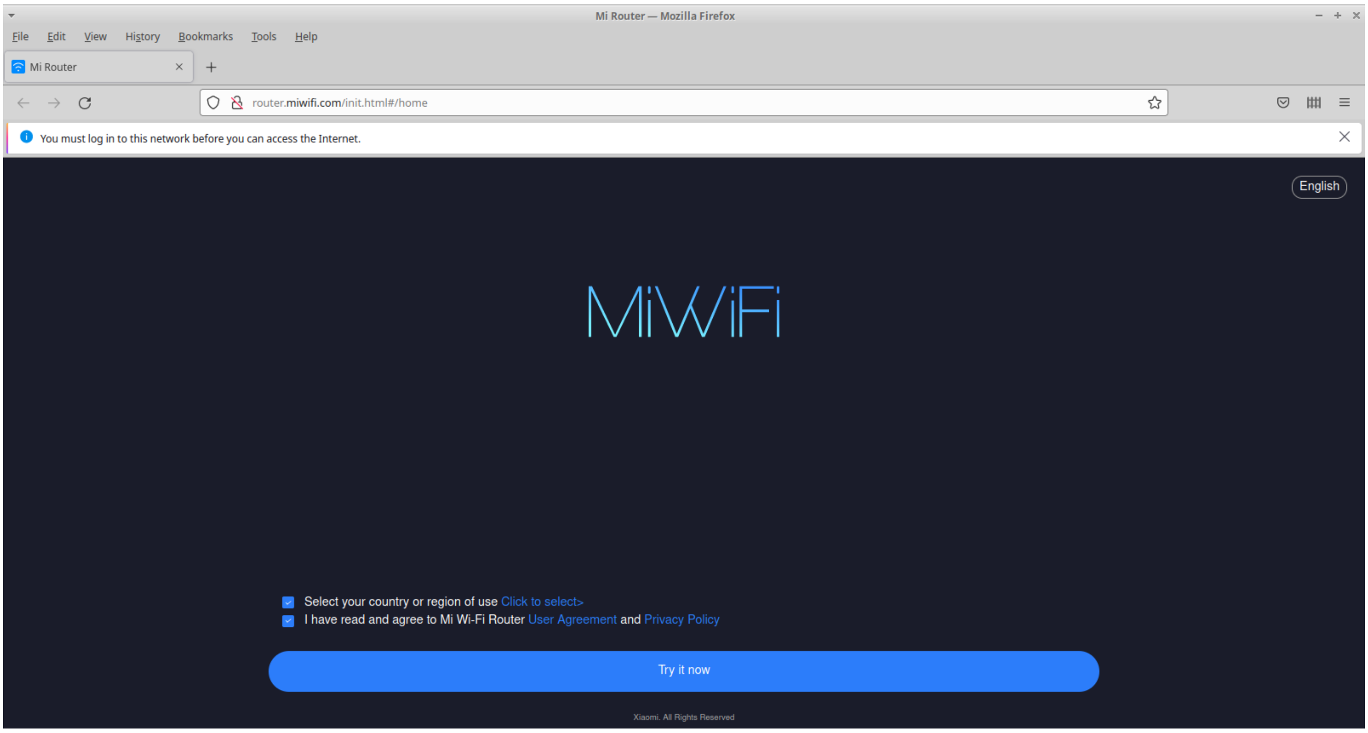
- In the past it used to be quite a mission to get OpenWrt flashed onto Xiaomi Routers.
- Things however changed drastically recently with the availability of **OpenWRTInvasion**.
- The following instructions can be applied to the **4A Gigabit Edition**, **4A 100M Edition** and **4C** models.
- Since there are still many older instructions floating around on the Internet it can be confusing initially to find a working set of instructions.
- The instructions on the OpenWrt Wiki for the **4C** are the best and to the point.
- https://openwrt.org/toh/xiaomi/xiaomi_mi_router_4c
- The instructions on this page will be based on them.

Overview

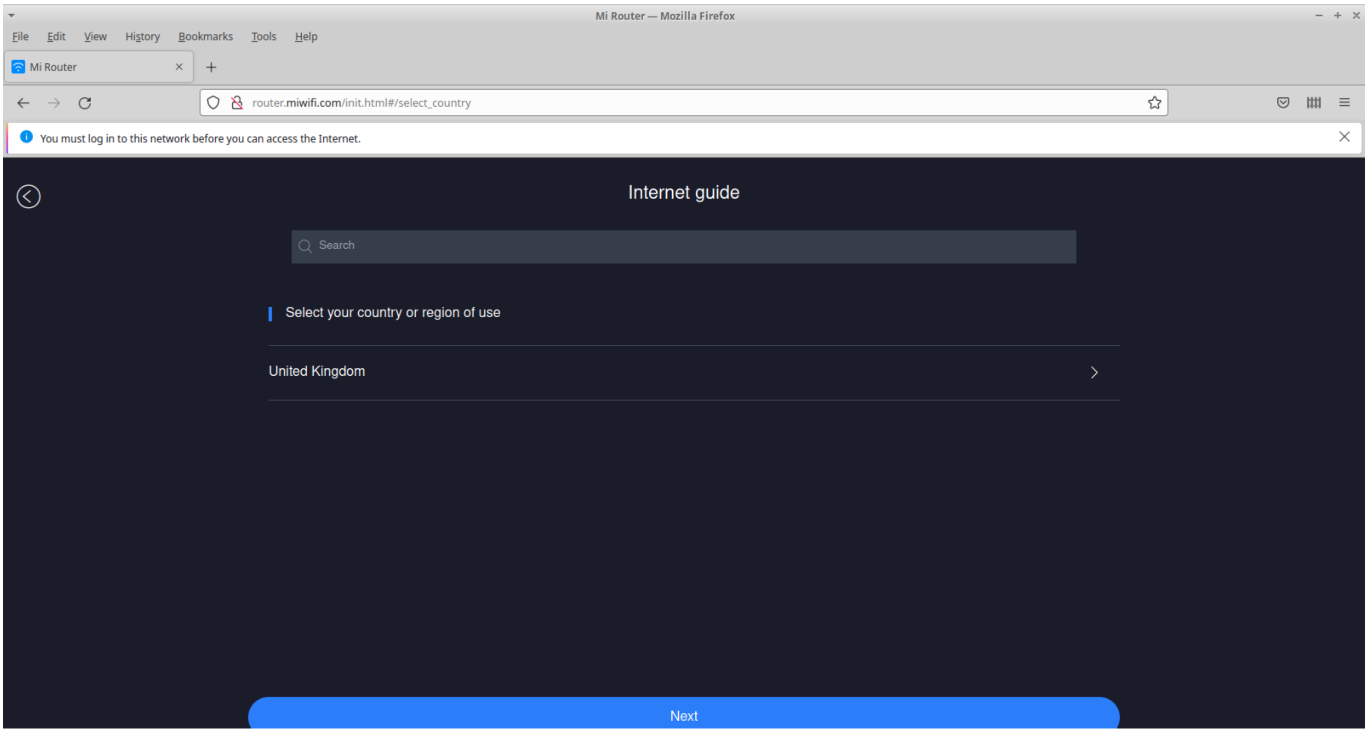
- Its always good to understand actually what is happening when you do something so that when things do go wrong you will have a better ability to do troubleshooting.
- With the latest version of OpenWRTInvasion you need to
  - Connect the Xiaomi router to the Internet (Using the WAN port)
  - Connect your computer (ours is running Ubuntu 20.04) to the LAN.
  - The Xiaomi router by default has the following subnet **192.168.31.x** on the LAN.
  - The Xiaomi router will listen on **192.168.31.1**.
- The OpenWRTInvasion **invade** into the standard Xiaomi router and install a few utilities from the Internet onto the router self.
- This is why the router **needs to** have Internet access.
- For this invasion to happen you need to get a special key (called the **stok** value) from the Xiaomi router.
- Once the invasion is complete you will be able to ssh or telnet into the Xiaomi router,
- Then you can download and flash OpenWRT onto the router using the **mtd** command.
- If things go wrong there is an easy way to install the original Xiaomi firmware again onto the device and start from scratch.
- This makes the devices very robust.

Finding the stok code on the router

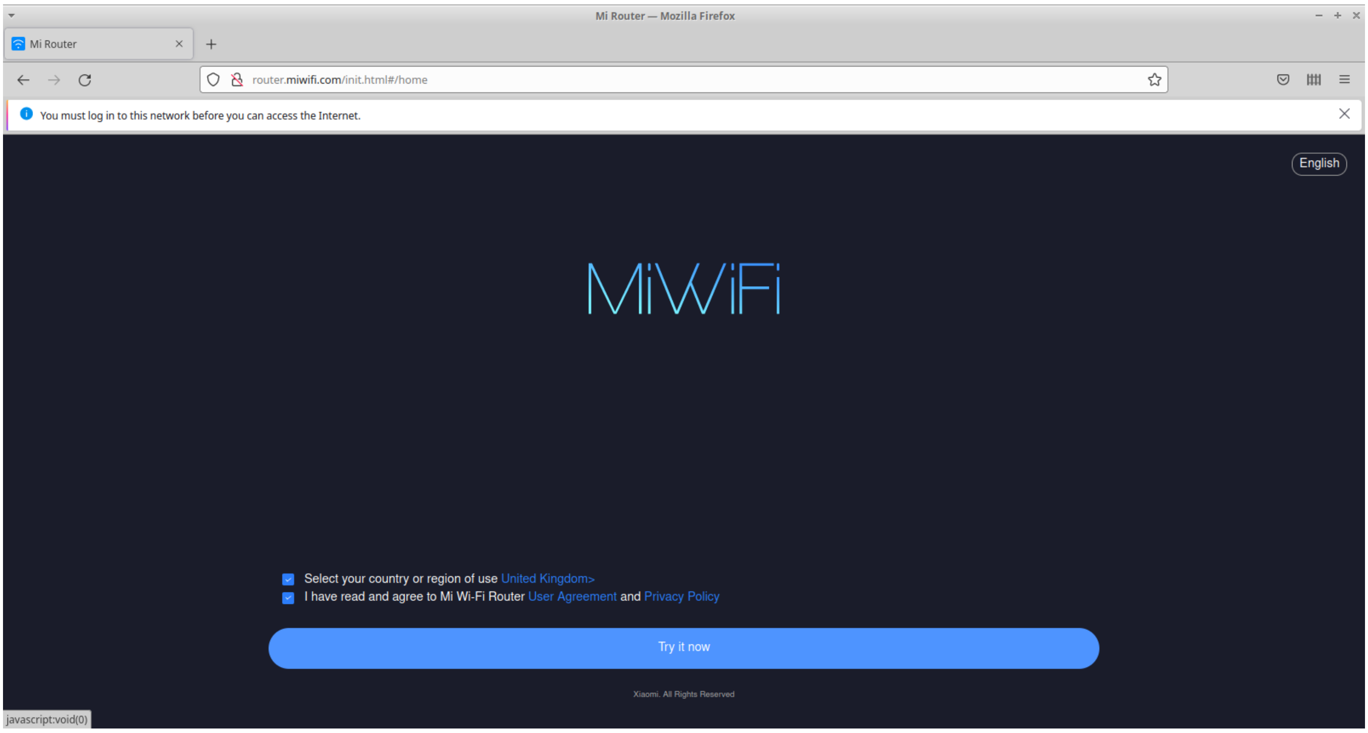
- This section will show a couple of screenshots from the Xiaomi 4C router to get to the **stok** code needed when using **OpenWRTInvasion**.
- These routers are easy to source in most countries. I got one from a local online store in South Africa for ~15USD delivered to my door.
- I connected the WAN port to my TLE router and connected my laptop to the LAN side of the 4C.


Mi Router — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Mi Router
router.miwifi.com/init.html#/home
You must log in to this network before you can access the Internet.
English
MiWiFi
☑ Select your country or region of use Click to select>
☑ I have read and agree to Mi Wi-Fi Router User Agreement and Privacy Policy
Try it now
Xiaomi. All Rights Reserved

- The very first screen you are met with can be a bit confusing, since your natural reaction is to hit the **Try it now** button.
- You however have to first select the country. So click the **Click to select** link to select the country first.


Mi Router — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Mi Router
router.miwifi.com/init.html#/select_country
You must log in to this network before you can access the Internet.
Internet guide
Search
Select your country or region of use
United Kingdom
Next

- Not all countries are listed in the select, so I choose **United Kingdom**

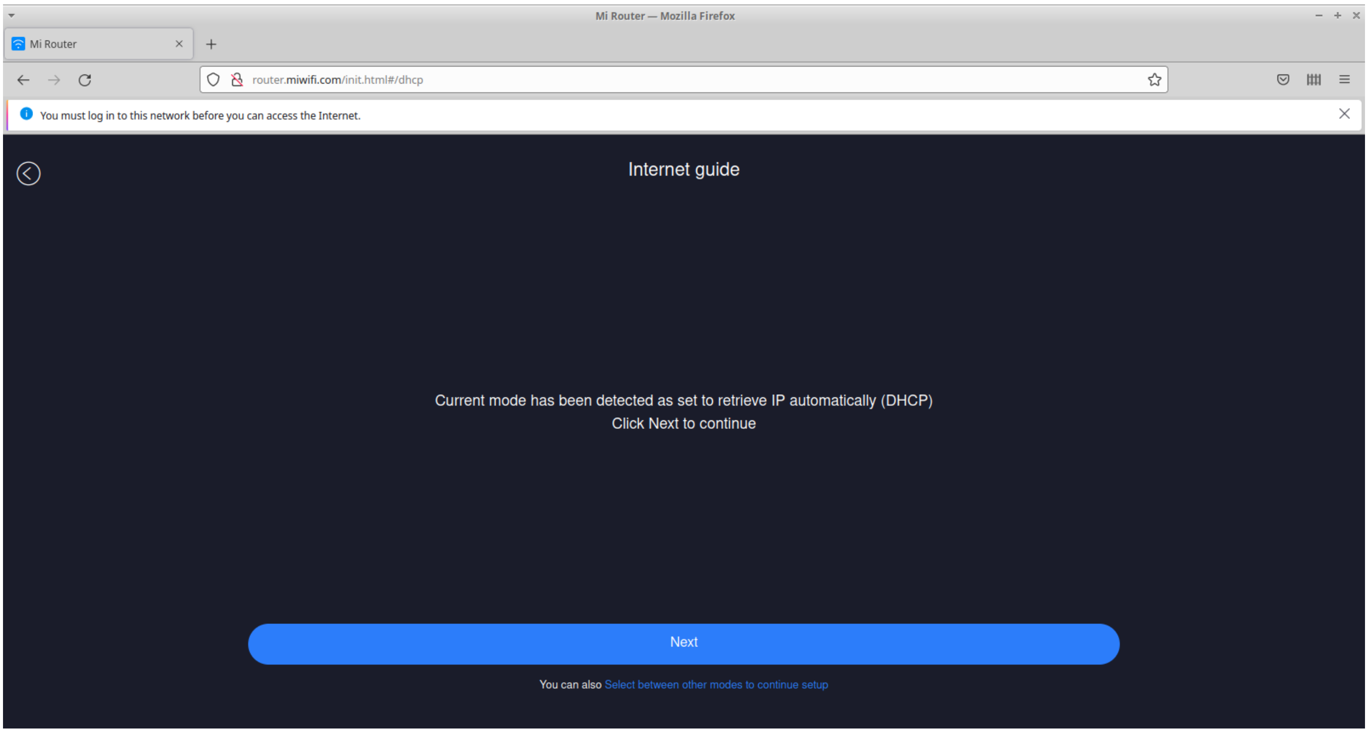

Mi Router — Mozilla Firefox
Mi Router
router.miwifi.com/init.html#/home
English
MiWiFi
Try it now
Xiaomi. All Rights Reserved
javascript:void(0)

You must log in to this network before you can access the Internet.

☑ Select your country or region of use United Kingdom>

☑ I have read and agree to Mi Wi-Fi Router User Agreement and Privacy Policy

- Once it is selected you can hit the **Try it now** button again.

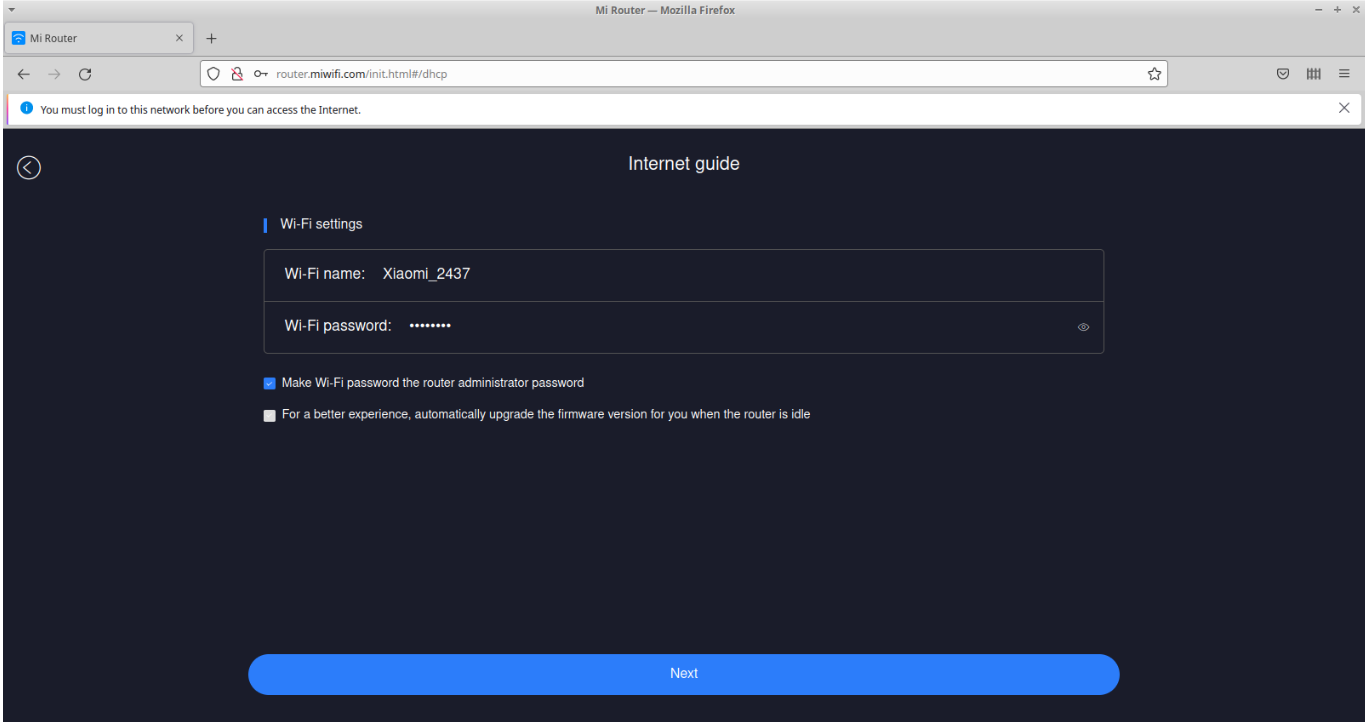

Mi Router — Mozilla Firefox
Mi Router
router.miwifi.com/init.html#/dhcp
Internet guide
Next

You must log in to this network before you can access the Internet.

Current mode has been detected as set to retrieve IP automatically (DHCP)
Click Next to continue

You can also Select between other modes to continue setup

- On the **Internet guide** screen you can leave the default and click it through



Mi Router — Mozilla Firefox
Mi Router
router.miwifi.com/init.html#/dhcp

You must log in to this network before you can access the Internet.

Internet guide

Wi-Fi settings

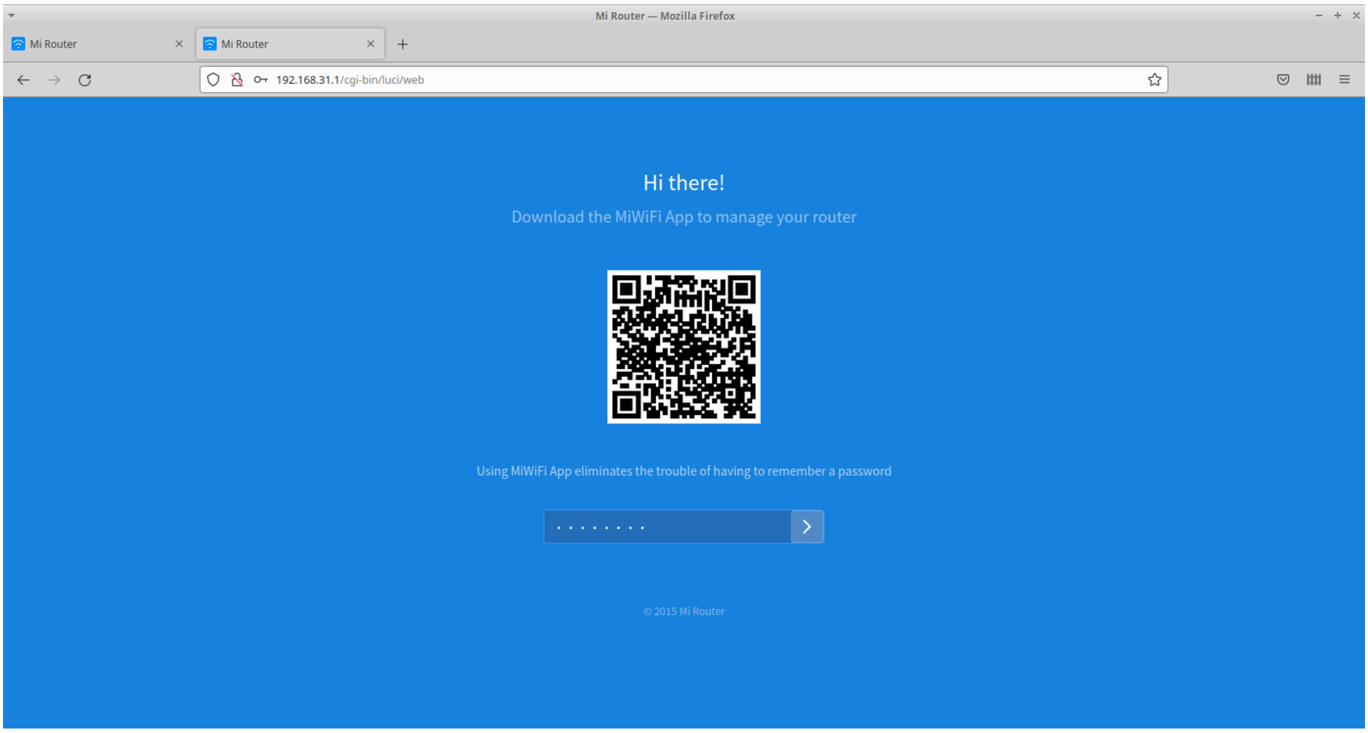
Wi-Fi name: Xiaomi_2437

Wi-Fi password: ••••••••

☑ Make Wi-Fi password the router administrator password

□ For a better experience, automatically upgrade the firmware version for you when the router is idle

- Provide a password for the router and Wireless and click next.

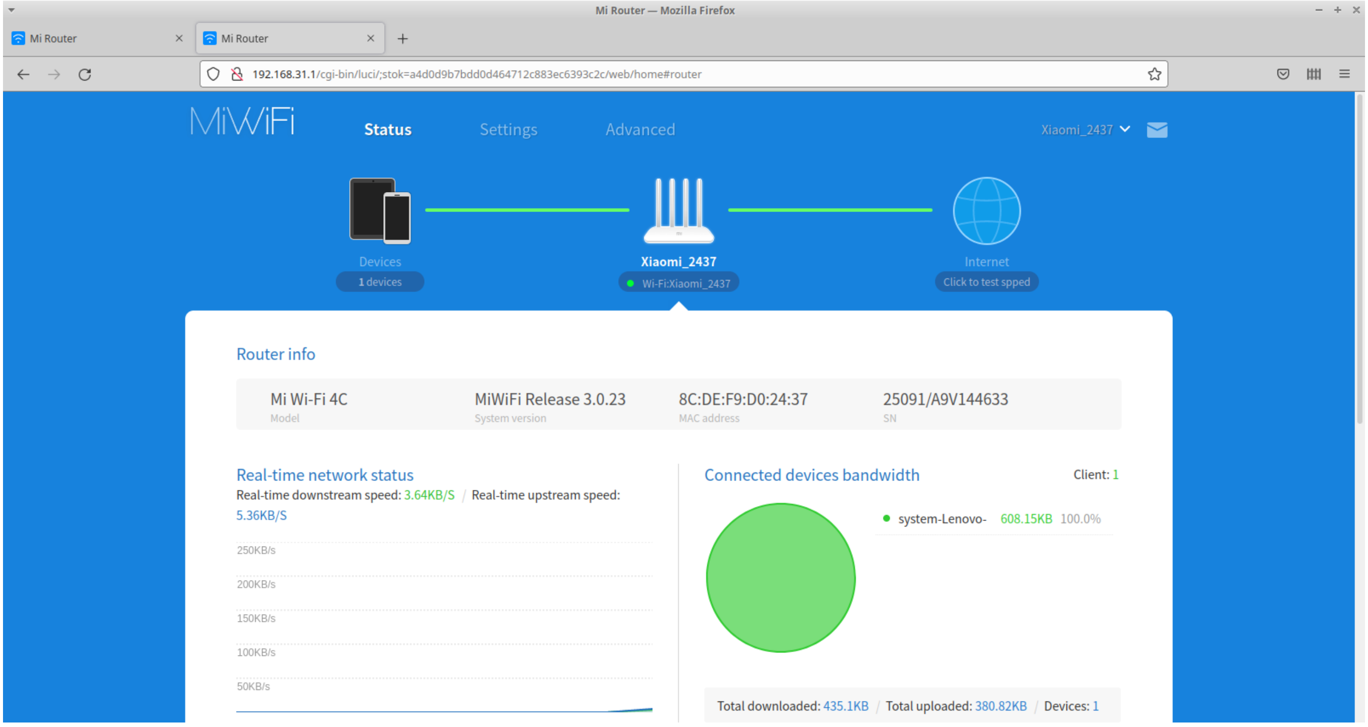


Hi there!

Download the MiWiFi App to manage your router

Using MiWiFi App eliminates the trouble of having to remember a password

- Setup is now complete and you can log in using the password you just provided.



Mi Router — Mozilla Firefox

192.168.31.1/cgi-bin/luci/;stok=a4d0d9b7bdd0d464712c883ec6393c2c/web/home#router

Router info

Model	System version	MAC address	SN
Mi Wi-Fi 4C	MiWiFi Release 3.0.23	8C:DE:F9:D0:24:37	25091/A9V144633

Real-time network status

Real-time downstream speed: 3.64KB/S / Real-time upstream speed: 5.36KB/S

Connected devices bandwidth Client: 1

system-Lenovo- 608.15KB 100.0%

Total downloaded: 435.1KB / Total uploaded: 380.82KB / Devices: 1

- Here we are logged in.
- As you can see in the URL Address bar there is a query string with an item called **stok** which you will use with **OpenWRTInvasion**
- Note that this value changes with each session so if you rebooted the router or logged out and then log in again the value will be different.
- Only the most recent value will work with **OpenWRTInvasion**

Invading the Router

- We assume you have an installation of Ubuntu 20.04.
- Make sure python3-pip and git is installed

```
sudo apt-get install python3-pip git
```

- Create a working directory where you can checkout OpenWRTInvasion

```
mkdir xiaomi_flash
cd xiaomi_flash/
git clone https://github.com/acecilia/OpenWRTInvasion.git
```

- Install the requirements and run it. You will need Admin rights to run the program else it will not work.

```
cd OpenWRTInvasion/
#Important to run as superuser
sudo pip3 install -r requirements.txt # Install requirements
sudo python3 remote_command_execution_vulnerability.py
```

- This will start the program and ask two questions for it to complete the invasion
  - **Router IP address**. The default as stated and specified will be 192.168.31.1.
  - **Stok value**. This is the value shown after you went through the initial setup wizard of the

router.
    - Mine was http://192.168.31.1/cgi-bin/luci/;stok=c047480902024ca71370a39eace78b36/web/home#router.
    - Note that this value is generated on the fly and changes next time the router boots again.

```
Router IP address [press enter for using the default 192.168.31.1]:
stok: c047480902024ca71370a39eace78b36
****************
router_ip_address: 192.168.31.1
stok: c047480902024ca71370a39eace78b36
****************
start uploading config file...
start exec command...
done! Now you can connect to the router using several options: (user: root, password: root)
* telnet 192.168.31.1
* ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cbc -o UserKnownHostsFile=/dev/null root@192.168.31.1
* ftp: using a program like cyberduck
```

- The invasion is now complete and you should be able to access the router.
- Note it takes ~2-3 minutes for the invasion to complete.

Flashing the new firmware

- As you can see from the snippet above there are a couple ways of reaching the invaded router.
- Please note that the router is fairly robust making it almost impossible hard brick the router.
- *Don't be to nervous when flashing the router as you always restore it again.*
- We will
    - SCP the firmware image onto the router
    - SSH into the router
    - Write the firmware to the OS1 flash partition using the **mtd** program.
- Copy the firmware file to the router.

!! Please change the name of the firmware file to match yours !!

```
scp -oKexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cbc -o UserKnownHostsFile=/dev/null openwrt-ramips-mt7621-xiaomi_mi-router-4a-gigabit-squashfs-sysupgrade.bin  root@192.168.31.1:/tmp
```

- SSH into the device

!! Here also change the name of the firmware file to match yours !!

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cbc -o UserKnownHostsFile=/dev/null root@192.168.31.1

BusyBox v1.19.4 (2019-06-28 10:13:42 UTC) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
 -----------------------------------------------------
       Welcome to XiaoQiang!
 -----------------------------------------------------
  $$$$$$\  $$$$$$$\  $$$$$$$$$\     $$\      $$\        $$$$$$\  $$\   $$\
 $$  __$$\ $$  __$$\ $$  _____|     $$ |     $$ |      $$  __$$\ $$ | $$  |
 $$ /  $$ |$$ |  $$ |$$ |           $$ |     $$ |      $$ /  $$ |$$ |$$  /
 $$$$$$$$ |$$$$$$$  |$$$$$\         $$ |     $$ |      $$ |  $$ |$$$$$  /
 $$  __$$ |$$  __$$< $$  __|        $$ |     $$ |      $$ |  $$ |$$  $$<
 $$ |  $$ |$$ |  $$ |$$ |           $$ |     $$ |      $$ |  $$ |$$ |\$$\
 $$ |  $$ |$$ |  $$ |$$$$$$$$$\      $$$$$$$$$  |       $$$$$$  |$$ | \$$\
 \__|  \__|\__|  \__|\________|      \_________/        \______/ \__|  \__|


root@XiaoQiang:~# cd /tmp
root@XiaoQiang:/tmp# mv openwrt-ramips-mt7621-xiaomi_mi-router-4a-gigabit-squashfs-sysupgrade.bin openwrt.bin
root@XiaoQiang:/tmp# mtd -e OS1 -r write openwrt.bin OS1
Unlocking OS1 ...
Erasing OS1 ...
```

- If all goes well the device will reboot.
- Keep an eye on the orange LED if it flashes you're in business since it is related to OpenWRT.
- While it flashes it means OpenWRT is busy creating its working filesystem on the flash chip.
- Remember that devices with 128M flash will take longer to settle down eventually.
- Once everything settles down you should have two blue LEDs.
- Now you can try out your new firmware.
- If things however did now work according to plan the next section is for you.

De-Bricking The Xiaomi Router

- There is an awesome write-up with some YouTube videos on how to de-brick and restore the router's original firmware.
- https://hoddysguides.com/xiaomi-debrick-tools-all/
- One point if interest is if you run a Linux environment you can simply install **Wine** and run the **pxesrv.exe** program as root.

```
sudo wine pxesrv.exe
```

From:
https://radiusdesk.com/docuwiki/ - **RADIUSdesk**

Permanent link:
https://radiusdesk.com/docuwiki/2021/xiaomi_flash

Last update: **2021/11/03 15:43**