Revision History (v3.2): Modification from v3.1

1. Support 2 broadcast channels

I. Hardware Requirement (Tested platform)
GL-AR750s router (WiFi chipset: QCA9563)

https://wikidevi.com/wiki/GL.iNet_GL-AR750S

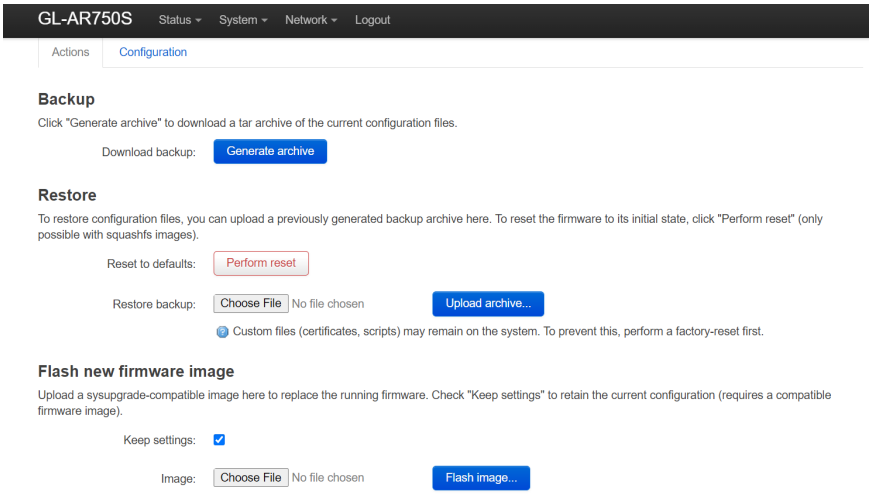
II. Software Requirement
A. Openwrt LEDE
openwrt-ar71xx-nand-gl-ar750s-squashfs-sysupgrade.tar
(Use this to upgrade the existing openwrt on the router)
openwrt-ar71xx-nand-gl-ar750s-ubi-factory.img
(Use this to install openwrt for the first time)

B. Installation files of Wi-Fi iBeacon
BeaconFi_1.0-1_mips_24kc.ipk
kmod-ath9k_4.9.120+2017-11-01-9_mips_24kc.ipk

C. Install BLE scanner in the smartphone (available in App Store of either Android or IOS)

III. Deployment Procedure
A. Flash GL-AR750s with provided Openwrt image.

Log into the admin page of the router and upgrade the firmware with openwrt-ar71xx-nand-gl-ar750s-squashfs-sysupgrade.tar



Note: The default OS in GL-AR750s has a different appearance. But there is a similar page for flashing image.

Note: if the default OS in the router is not openwrt, try to install openwrt-ar71xx-nand-gl-ar750s-ubi-factory.img instead.

After flashing the image, wait until the root reboots. Then, open a cmd in PC (window or linux) and do the follows in the cmd line.

B. Copy the ipk to the /tmp directory in the router

```
scp BeaconFi_1.0-1_mips_24kc.ipk  kmod-ath9k_4.9.184+4.19.32-1-2_mips_24kc.ipk
root@IP_ADDR_OF_ROUTER:/tmp
```

IP_ADDR_OF_ROUTER is typically 192.168.8.1

C. Log into the router and Install ipk

```
ssh root@IP_ADDR_OF_ROUTER
opkg install /tmp/BeaconFi_1.0-1_mips_24kc.ipk
opkg remove kmod-ath9k
opkg install /tmp/kmod-ath9k_4.9.120+2017-11-01-9_mips_24kc.ipk
```

D. Configure the basic rate in /etc/config/wireless to be 11MHz

Add the following line to the configuration of 2G radio.

```
list basic_rate '11000'
```

```
config wifi-device 'radio1'
        option type 'mac80211'
        option channel '11'
        option hwmode '11g'
        option path 'platform/qca956x_wmac'
        option txpower '20'
        option noscan '1'
        option band '2G'
        option disabled '0'
        list basic_rate '11000'
        option country 'CN'
        option legacy_rates '1'
        option htmode 'HT40'
```

E. Reboot the router

```
root
```

After the steps above, there will two files deployed:

1) An executive called “BeaconFi” under /usr/bin: this is the C program that takes iBeacon configurations, e.g., uuid, major, minor and dynamically generates Wi-Fi payload or Wi-Fi probe request script.
2) A text configuration file called “beaconfi_config” under /etc: it is the default iBeacon configurations that BeaconFi will take to generate Wi-Fi payload.

```
advAddr=0xea,0x54,0x2d,0x0c,0x16,0x77
uuid=0x6b,0x76,0xe2,0x8a,0x6f,0xa2,0x48,0xc9,0x85,0x02,0xc1,0xda,0xa3,0x88,0xab,0x2c
major=0x02,0x05
minor=0x02,0x05
ifname=wlan1
#wifi_mac=0xe4,0x95,0x6e,0x48,0x78,0xe7
#capabilities=0x11ee
#max_mcs=7
beacon_interval_us=500000
```

An example of beaconfi_config

F. Generate probe request injection script with BeaconFi

BeaconFi -s

This produces the shell script called “probe” under /tmp. You may cat /tmp/probe to double check if the script is correct.

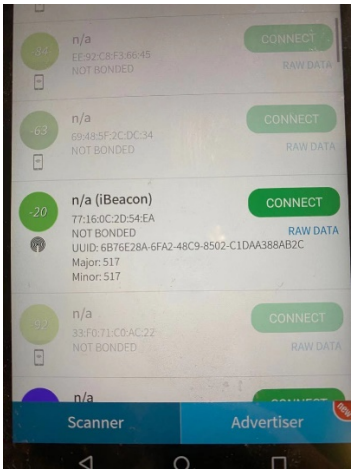
```
#!/bin/sh
while [ 1 ]
do
    iw dev wlan0 scan -u freq 2427 ies DD:a7:4c:6a:e1:ab:41:4d:df:35:d4:37:73:fe:cd:ac:73:6b:7e:4a:b0:09:85:c1
    usleep 500000
done
```

An example of “probe”

G. Running probe script and transmit the WiFi ibeacon

cd /tmp

sh probe



Misc.

Our openwrt image does not contain luci web admin. To install luci web admin, connected the router to the internet through ethernet port. Then ssh into the router and

Opkg update

Opkg install luci