NEW RADIO COMMUNICATION FOR NEW ERA

NRC7394 Evaluation Kit User Guide

(Host Mode)

Ultra-low power & Long-range Wi-Fi

Ver 1.0
Apr. 5, 2023

Newracom, Inc.

NRC7394 Evaluation Kit User Guide (Host Mode)
Ultra-low power & Long-range Wi-Fi

Office

NEWRACOM, Inc.
505 Technology Drive, Irvine, CA 92618 USA
http://www.NEWRACOM.com

Contents

1 Overview 7
1.1 HW list 8
1.1.1 NRC7394 module 8
1.1.2 NRC7394 EVB 8
1.1.3 Host board 8
1.2 Kit list 10
2 NRC7394 EVK manipulation 11
2.1 Direct manipulation 11
2.2 Remote manipulation 11
2.3 IP setting for Ethernet 12
3 NRC7394 EVK AP/STA operation 14
3.1 Start Script 14
3.2 AP mode operation 16
3.3 AP mode operation with Self-configuration 19
3.4 STA mode operation 21
3.5 Configure static IP address 23
4 NRC7394 EVK performance evaluation 24
4.1 Performance test 24
4.2 Enable/Disable A-MPDU 25
4.3 Enable/Disable NDP Probe Request 26
4.4 Enable/Disable power save 27
4.5 Enable/Disable board data 28
4.6 Enable/Disable BSS MAX IDLE element 29
5 Internet connection 30
6 Change configuration 31
7 NRC7394 EVK software 39
8 NRC7394 EVK Sniffer operation 41
9 Revision history 42
Appendix A. Upgrade hostapd & wpa_supplicant for supporting WPA3 43
A.1 Overview 43
A.2 Upgrade hostapd 44

A.3 Upgrade wpa_supplicant..... 44

List of Tables

Table 6.1 Available frequency band and corresponding channel bandwidth (US) 33
Table 6.2 Available frequency band and corresponding channel bandwidth (TW) 34
Table 6.3 Available frequency band and corresponding channel bandwidth (CN) 35
Table 6.4 Available frequency band and corresponding channel bandwidth (KR-USN) 35
Table 6.5 Available frequency band and corresponding channel bandwidth (KR-MIC) 35
Table 6.6 Available frequency band and corresponding channel bandwidth (JP) 35
Table 6.7 Available frequency band and corresponding channel bandwidth (EU) 36
Table 6.8 Available frequency band and corresponding channel bandwidth (NZ) 36
Table 6.9 Available frequency band and corresponding channel bandwidth (AU) 37
Table 6.10 US Channels of hw_mode=g in a configure file 38
Table 7.1 Files in AP 39
Table 7.2 Files in STA 40

List of Figures

Figure 1.1 NRC7394 evaluation board (Top view) 7
Figure 1.2 Host mode configuration 7
Figure 1.3 NRC7394 EVB Power Structure 8
Figure 1.4 Block diagram of NRC7394 evaluation board 9
Figure 1.5 NRC7394 hardware set 10
Figure 2.1 Mobaxterm display 11
Figure 2.2 VNC viewer display 12
Figure 2.3 Configuration of IP setting for Ethernet DHCP client 12
Figure 3.1 Usage of start.py script 14
Figure 3.2 Results of running AP (1/2) 17
Figure 3.3 Results of running AP (2/2) 18
Figure 3.4 Parmeter for Self-Configuration 19
Figure 3.5 Results of Self-Configuration on AP 19
Figure 3.6 Results of Self-Configuration with invalid target FW 20
Figure 3.7 Results of running STA (1/2) 22
Figure 3.8 Results of running STA (2/2) 23
Figure 3.9 Configure static IP address for STA 23
Figure 3.10 Configure static IP address for AP 23
Figure 4.1 Run iperf3 server 24
Figure 4.2 Run iperf3 client 24
Figure 4.3 Enable/disable A-MPDU 25
Figure 4.4 Enable/disable NDP Probe Request 26
Figure 4.5 Enable/disable power save 27
Figure 4.6 Enable/disable board data 28
Figure 4.7 Enable/disable BSS MAX IDLE 29
Figure 5.1 Result of ping 30
Figure 5.2 Internal connection 30
Figure 6.1 Contents of ap_halow_open.conf file (US/JP/TW) 31
Figure 6.2 Contents of ap_halow_open.conf file (KR/EU/CN) 32
Figure 6.3 hw_mode of ap_halow_open.conf file (US) 38

1 Overview

This document introduces NEWRACOM's NRC7394 Evaluation kit (EVK). The evaluation kit (EVK) is used to evaluate the performance of the NRC7394 module containing NEWRACOM's IEEE 802.11ah Wi-Fi System on Chip (SoC).

Configure mode switch J4 to 2-3 (XIP write) for host mode as shown in Figure 1.2.

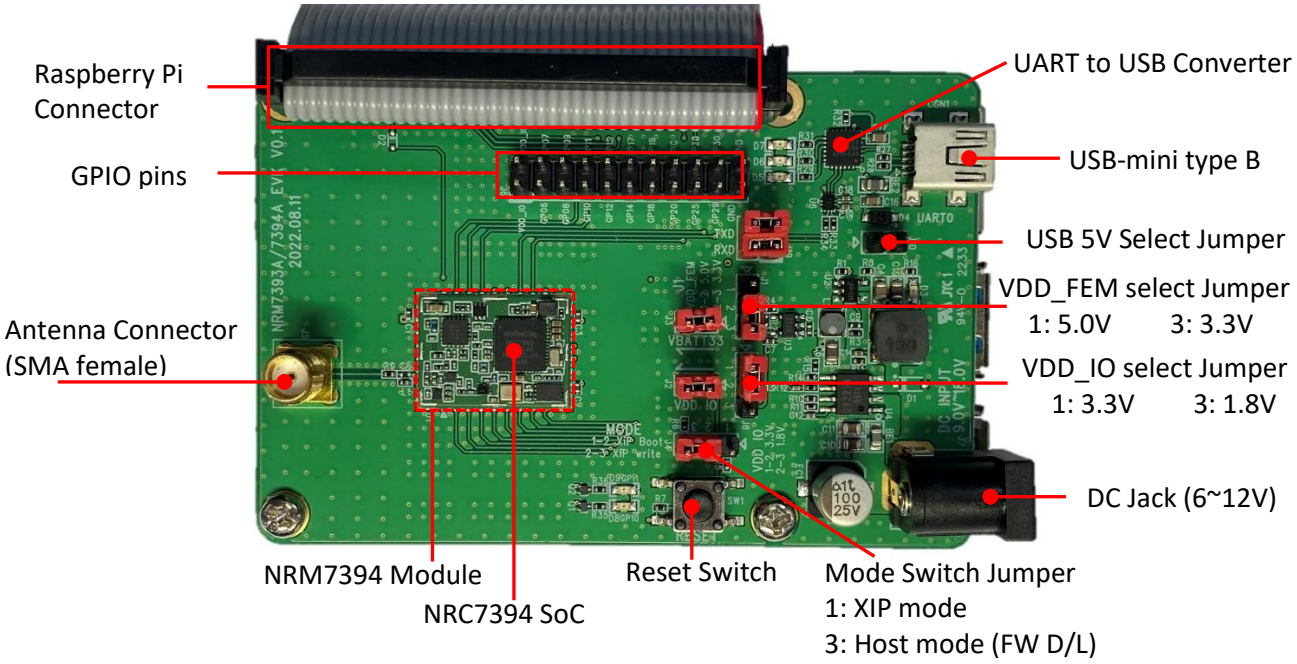


Figure 1.1 NRC7394 evaluation board (Top view)

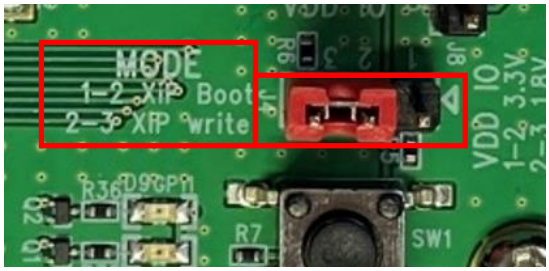


Figure 1.2 Host mode configuration

1.1 HW list

As shown in Figure 1.4, NRC7394 EVK consists of three components.

1.1.1 NRC7394 module

NRC7394 module contains IEEE 802.11ah Wi-Fi SoC solution. It also includes a RF front end module (FEM) to increase transmission power up to +27 dBm. Onboard serial flash memory can be used for over-the-air (OTA) software development and with 32KB cache in the NRC7394 supports the execution in place (XIP) feature.

1.1.2 NRC7394 EVB

NRC7394 EVB mainly offers communication interfaces to sensors or an external host.

DC power adaptor requires voltage range of 6~18V, and more than 1.5A current.

The EVB board has a function of step down the DC input power to each voltage source of the module, and also can supply 5V DC of Raspberry Pi4. Each voltage source of the module has a header type test point for easy current measurement. Refer to the Figure 1.3 for the EVB's power structure.

The board has a built-in USB to serial converter and is connected to UART0, so users can check status logs through the onboard USB mini connector.

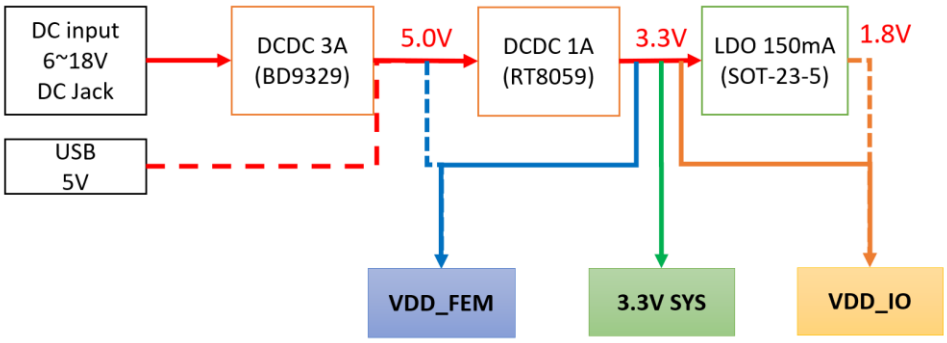


Figure 1.3 NRC7394 EVB Power Structure

1.1.3 Host board

NRC7394 EVB can be used either in standalone or slave to host processor via serial peripheral interface (SPI) or universal asynchronous receive transmitter (UART). Raspberry PI 4 can be one of the hosts used for normal operation, evaluation, and testing. When used in standalone, Raspberry PI4 board is not needed because NRC7394 operates without an additional host processor.

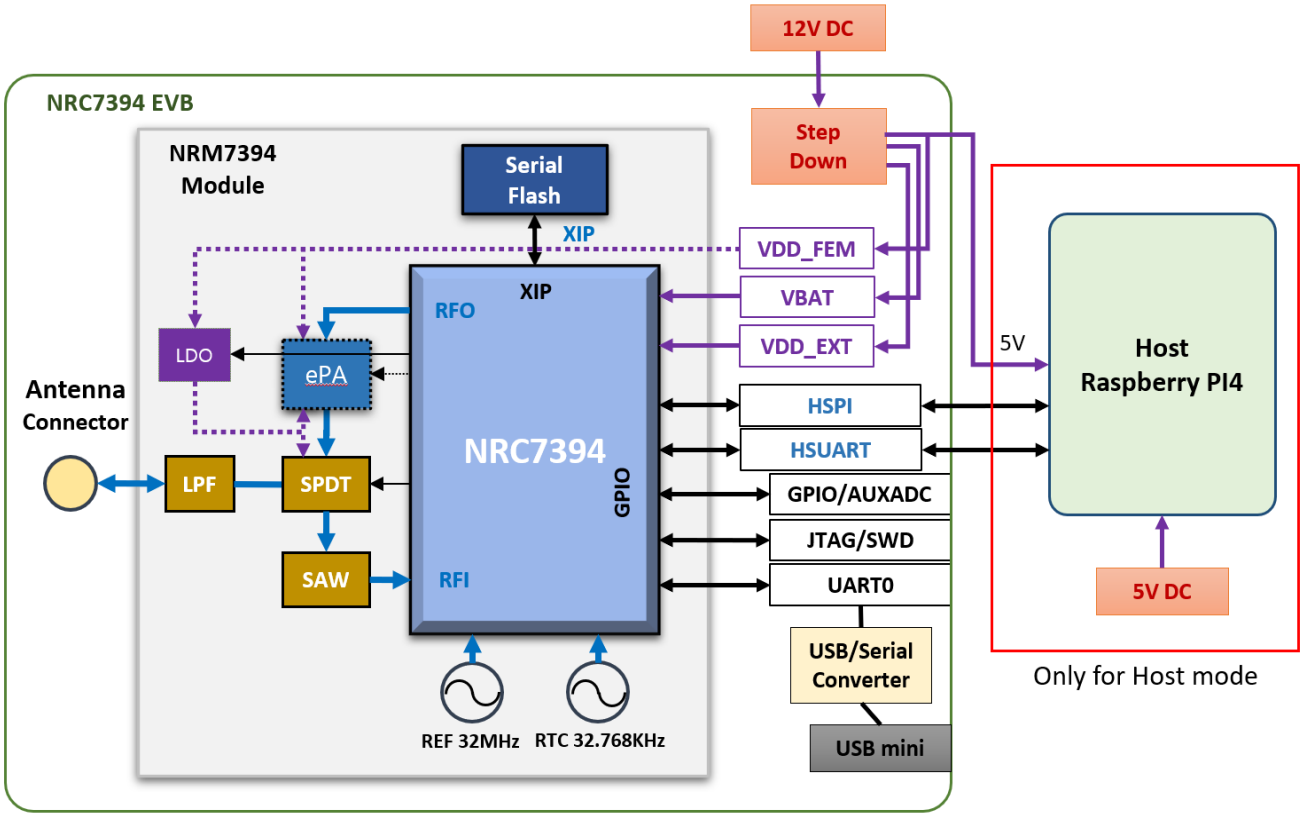


Figure 1.4 Block diagram of NRC7394 evaluation board

1.2 Kit list

NRC7394 EVK includes:

- NRC7394 EVB (NRM7394 module mounted)
- Raspberry PI4 board
- SD card with Linux OS, NRC7394 firmware, Wi-Fi driver, and scripts
- DC 12V (1.5A) power Adaptor
- Antenna (Country frequency)
- USB2.0 mini-B cable

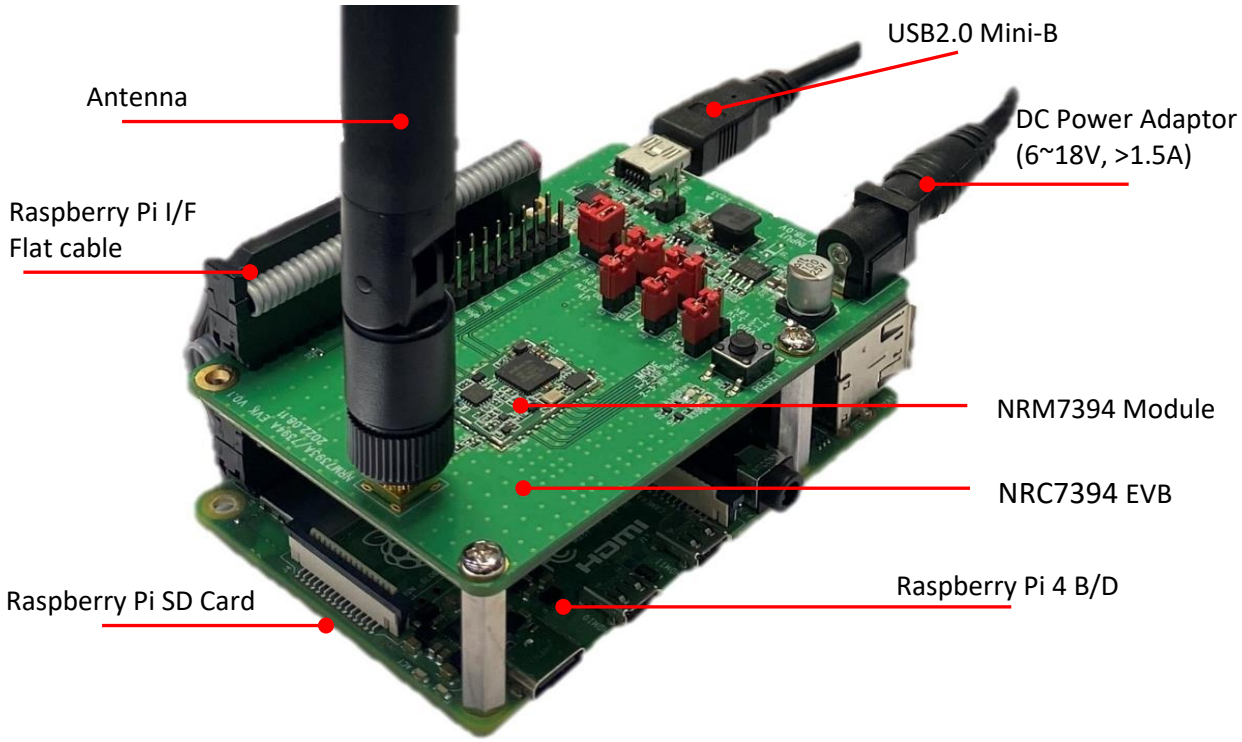


Figure 1.5 NRC7394 hardware set

***NOTE:**

The interface cable is removable to support the USB interface with the FTDI FT232H USB-SPI bridge cable. For more information, refer to the **AN-7292-008-FT232H_USB_SPI.pdf** file.

2 NRC7394 EVK manipulation

This chapter describes how to manipulate NRC7394 EVK directly or remotely. To directly control NRC7394 EVK, I/O devices such as: keyboard, mouse, monitor, and HDMI cable are needed. Otherwise, users can use terminal programs such as: Tera Term, Mobaxterm, VNC, etc. to control NRC7394 EVK remotely.

2.1 Direct manipulation

Using I/O devices is the simplest way to control NRC7394 EVK. It includes Raspberry PI3 which supports various I/O, especially useful is the HDMI connection. User can simply display Raspberry Pi (RPi) to a monitor by HDMI cable. Other USB-type keyboard and mouse can be utilized as input devices. However, if these I/O devices are not available, users have to additional options to manipulate NRC7394 EVK.

2.2 Remote manipulation

Raspberry PI4 has an Ethernet port, so users can remotely connect to RPi with terminal programs. There are two ways to obtain an IP address on RPi Ethernet, one way is static IP and the other is dynamic IP (DHCP). The initial (default) setting is set to obtain an IP address from the external DHCP server. Furthermore, the RPi can be operated as a DHCP server by changing the configuration. When enabled, the DHCP server will assign a static IP address (192.168.100.1) to RPi Ethernet and run the DHCP server. The PC will then obtain an IP address from RPi after connecting by Ethernet cable to the RPi. After the PC receives the IP address from RPi, then users can remotely access RPi (192.168.100.1) with terminal programs. Figure 2.1 and Figure 2.2 show Mobaxterm and VNC displays of PC receiving the IP address (192.168.100.10) after connecting to RPi.

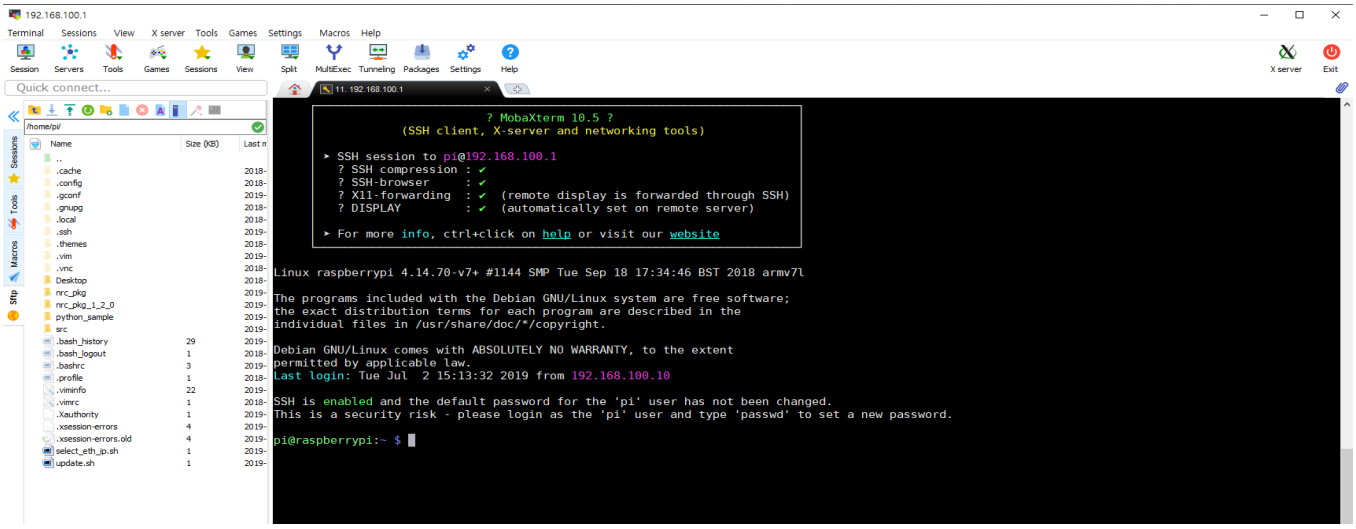


Figure 2.1 Mobaxterm display

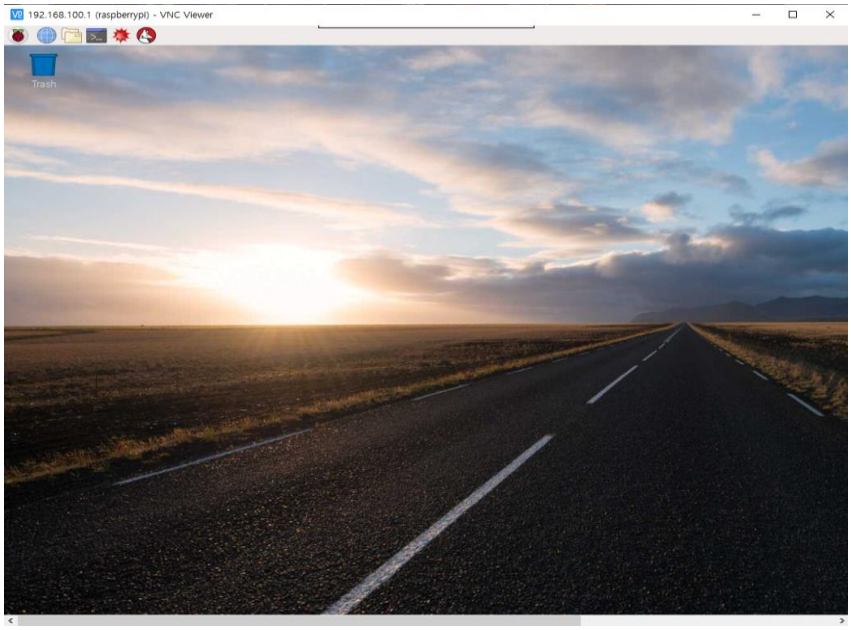


Figure 2.2 VNC viewer display

2.3 IP setting for Ethernet

By default, the RPi's Ethernet port is assigned an IP address through a DHCP server. To set up as an intra network, the Ethernet port can be used as a DHCP client by connecting the Ethernet cable from a switch, hub, or router to the RPi. The DHCP server on an intra network is assigned an Ethernet IP address and remotely accesses the RPi with the same IP address.

Script file (~/nrc_pkg/script/conf/etc/CONFIG_IP)

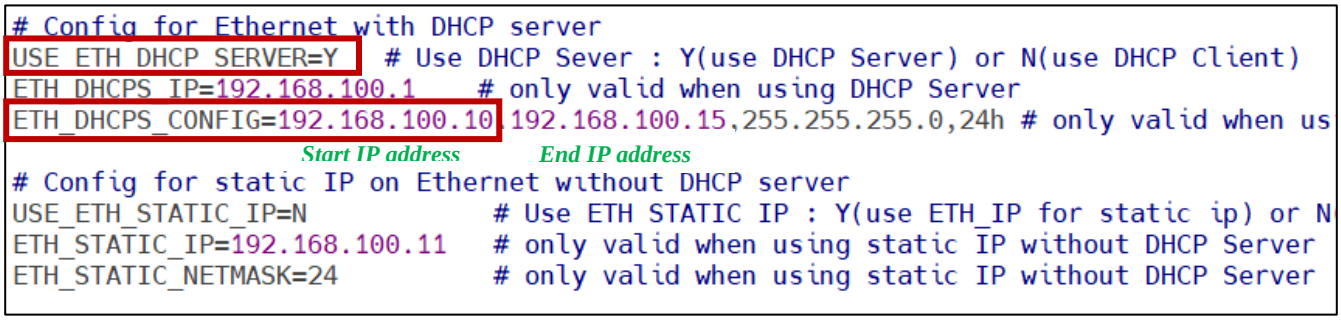
```
# Config for Ethernet with DHCP server
USE_ETH_DHCP_SERVER=N    # Use DHCP Sever : Y(use DHCP Server) or N(use DHCP Client)
ETH_DHCPS_IP=192.168.100.1    # only valid when using DHCP Server
ETH_DHCPS_CONFIG=192.168.100.10,192.168.100.15,255.255.255.0,24h # only valid when usi

# Config for static IP on Ethernet without DHCP server
USE_ETH_STATIC_IP=N           # Use ETH STATIC IP : Y(use ETH_IP for static ip) or N(
ETH_STATIC_IP=192.168.100.11  # only valid when using static IP without DHCP Server
ETH_STATIC_NETMASK=24         # only valid when using static IP without DHCP Server
```

Figure 2.3 Configuration of IP setting for Ethernet DHCP client

If the RPi Ethernet port works as a DHCP server, change it to “USE_ETH_DHCP_SERVER=Y” and run the script and reboot the RPi. After the reboot, the Ethernet IP is set to 192.168.100.1. One device connected with an Ethernet cable will be assigned an IP of 192.168.100.10. If more than one DHCP client devices are required, change the 'End IP address' parameter of 'ETH_DHCPS_CONFIG' from '192.168.100.10' to the required range such as

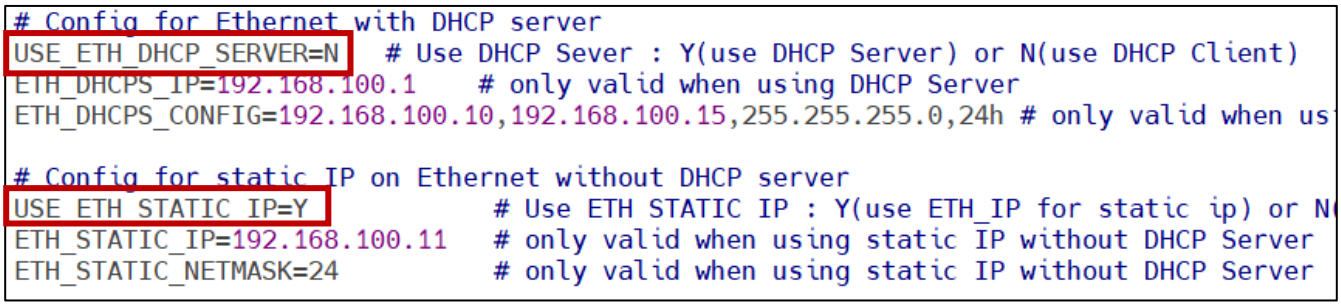
”ETH_DHCPS_CONFIG=192.168.100.10,192.168.100.15,255.255.255.0,24h”




```
# Config for Ethernet with DHCP server
USE_ETH_DHCP_SERVER=Y   # Use DHCP Sever : Y(use DHCP Server) or N(use DHCP Client)
ETH_DHCPS_IP=192.168.100.1     # only valid when using DHCP Server
ETH_DHCPS_CONFIG=192.168.100.10,192.168.100.15,255.255.255.0,24h # only valid when us
# Config for static IP on Ethernet without DHCP server
USE_ETH_STATIC_IP=N            # Use ETH STATIC IP : Y(use ETH_IP for static ip) or N
ETH_STATIC_IP=192.168.100.11   # only valid when using static IP without DHCP Server
ETH_STATIC_NETMASK=24          # only valid when using static IP without DHCP Server
```

Figure 2.4 Configuration of IP setting for Ethernet DHCP server

If the RPi's Ethernet Port is to work with Static IP instead of a DHCP Server, change it to “USE_ETH_DHCP_SERVER=N” and “USE_ETH_STATIC_IP=Y” and run the script and reboot the RPi. After reboot, the RPi's Ethernet IP is set to 192.168.100.11 and the device connected to the Ethernet cable is set to Static IP.



```
# Config for Ethernet with DHCP server
USE_ETH_DHCP_SERVER=N   # Use DHCP Sever : Y(use DHCP Server) or N(use DHCP Client)
ETH_DHCPS_IP=192.168.100.1     # only valid when using DHCP Server
ETH_DHCPS_CONFIG=192.168.100.10,192.168.100.15,255.255.255.0,24h # only valid when us

# Config for static IP on Ethernet without DHCP server
USE_ETH_STATIC_IP=Y            # Use ETH STATIC IP : Y(use ETH_IP for static ip) or N
ETH_STATIC_IP=192.168.100.11   # only valid when using static IP without DHCP Server
ETH_STATIC_NETMASK=24          # only valid when using static IP without DHCP Server
```

Figure 2.5 Configuration of IP setting for Ethernet Static IP

3 NRC7394 EVK AP/STA operation

This chapter explains how to start the IEEE 802.11ah AP operation and enable STA to connect to AP.

3.1 Start Script

The “start.py” in ~/nrc_pkg/script folder is the unified script used to initiate AP, STA, Sniffer, MP, MAP, RELAY and STA with Ucode. For each operation, the different arguments are needed.

Three arguments which are *sta_type*, *security_mode*, *country* is necessary for an AP or STA operation.

However, for Sniffer operation, two additional arguments, *channel*, and *sniffer mode*, are needed.

Please refer to other user guide documents for the usage of MP, MAP for Mesh and RELAY.

```
pi@raspberrypi:~/nrc_pkg/script $ ./start.py
Done.
Done.
Usage:
        start.py [sta_type] [security_mode] [country] [channel] [sniffer_mode]
        start.py [sta_type] [security_mode] [country] [mesh_mode] [mesh_peering] [mesh_ip]
Argument:
        sta_type      [0:STA   |  1:AP  |  2:SNIFFER  | 3:RELAY |  4:MESH]
        security_mode [0:Open  |  1:WPA2-PSK  |  2:WPA3-OWE  |  3:WPA3-SAE | 4:WPS-PBC]
        country       [US:USA  |  JP:Japan  |  TW:Taiwan  | KR:Korea | EU:EURO | CN:China |
                       AU:Austrailia  |  NZ:New Zealand] \
        ------------------------------------------------------------
        channel       [S1G Channel Number]   * Only for Sniffer
        sniffer_mode  [0:Local | 1:Remote]   * Only for Sniffer
        mesh_mode     [0:MPP | 1:MP | 2:MAP] * Only for Mesh
        mesh_peering  [Peer MAC address]     * Only for Mesh
        mesh_ip       [Static IP address]    * Only for Mesh
Example:
        OPEN mode STA for Korea                : ./start.py 0 0 KR
        Security mode AP for US                : ./start.py 1 1 US
        Local Sniffer mode on CH 40 for Japan  : ./start.py 2 0 JP 40 0
        SAE mode Mesh AP for US                : ./start.py 4 3 US 2
        Mesh Point with static ip              : ./start.py 4 3 US 1 192.168.222.1
        Mesh Point with manual peering         : ./start.py 4 3 US 1 8c:0f:fa:00:29:46
        Mesh Point with manual peering & ip    : ./start.py 4 3 US 1 8c:0f:fa:00:29:46 192.168.222.1
Note:
        sniffer_mode should be set as '1' when running sniffer on remote terminal
        MPP, MP mode support only Open, WPA3-SAE security mode
```

Figure 3.1 Usage of start.py script

NOTE

Executing “start.py” script overwrites some lane in the dhcpcd.conf (~/nrc_pkg/etc/dhcpcd/) and the dnsmasq.conf (~/nrc_pkg/etc/dnsmasq) files as shown below. To keep the user’s configuration, users should leave that lane blanked.

dhcpcd.conf file	**dnsmasq.conf**
Line 59, 62 //IP address for wlan0 Line 65, 68 //IP address for wlan1 Line 71, 72 //IP address for eth0	Line 2 //DHCPS configuration for eth0 Line 3, 4 //DHCPS configuration for wlan0 or wlan1

3.2 AP mode operation

1) Open terminal with SSH

After boot-up of AP board, connect via SSH to the AP by using the terminal emulator like MobaXterm. The ID and PW are as follows:

- ID : pi
- PW : raspberry

2) Run script

To run AP, a user should give “1” as *sta_type* and select one of the security mode and country code.

parameter setting

- *sta_type* : **1 (AP)**
- *security_mode* : available modes are 0(open), 1(WPA2-PSK), 2(WPA3-OWE) and 3(WPA3-SAE)
- *country* : available country codes are US, JP, TW, KR, EU, CN, AU, NZ
  Ex) open mode AP to be used in Korea : ./start.py 1 0 KR

3) Check results

Once AP runs by start script, there are several procedures that are executed: 1) clear apps 2) copy firmware 3) load module 4) set configurations 5) start the hostapd 6) set NAT 7) start DNSMASQ, and performed in sequential order. If all procedures are successful, the user can find the wlan0 interface with the IP address created as shown in Figure 3.3.

```
pi@raspberrypi:~/nrc_pkg/script $ ./start.py 1 0 KR
Done.
Done.
------------------------------
Model            : 7292
STA Type         : AP
Country          : KR
Security Mode    : OPEN
CAL. USE         : ON
AMPDU            : ON
Download FW      : uni_s1g.bin
TX Power         : 17
BSS MAX IDLE     : 180
------------------------------
NRC AP setting for HaLow...
[*] Set Max CPU Clock on RPi
1200000
1200000
1200000
1200000
Done
[0] Clear
wpa_supplicant: no process found
wireshark-gtk: no process found
rm: cannot remove '/home/pi/nrc_pkg/script/conf/temp_self_config.conf': No such file or dir
ectory
[1] Copy
total 648
drwxr-xr-x 2 pi   pi     4096 Oct 15 11:39 .
drwxr-xr-x 4 pi   pi     4096 Oct 15 11:35 ..
-rwxrwxrwx 1 pi   pi      271 Oct 15 11:35 copy
-rwxr-xr-x 1 pi   pi      562 Oct 15 11:35 nrc7292_bd.dat
-rwxr-xr-x 1 pi   pi   321980 Oct 15 11:35 nrc7292_cspi.bin
-rwxr-xr-x 1 root root 321980 Oct 15 12:04 uni_s1g.bin
-rw-r--r-- 1 root root 321980 Oct 15 12:04 /lib/firmware/uni_s1g.bin
====================================
 AP INTERFACE     : wlan0
 AP STATIC IP     : 192.168.200.1
 NET MASK NUM     : 24
====================================
Config for AP is done!
IP and DHCP config done
[2] Set Module Parameters
[3] Loading module
sudo insmod /home/pi/nrc_pkg/sw/driver/nrc.ko  hifspeed=20000000 spi_bus_num=0 spi_cs_num=0
 spi_gpio_irq=5 spi_gpio_poll=-1 fw_name=uni_s1g.bin power_save=0 bss_max_idle=180 ndp_preq
=1 auto_ba=1 listen_interval=1000
[4] Set tx power
Tx power : 17                   Calibration_use : ON
OK
Board Data use                   : off
OK
[5] Set guard interval
guard interval : long
OK
```

Figure 3.2 Results of running AP (1/2)

```
[6] Set cal_use
Calibration_use : on                    Country   : KR
OK
[*] Start DHCPCD and DNSMASQ
[*] Self configuration off
[6] Start hostapd on wlan0
Configuration file: /home/pi/nrc_pkg/script/conf/KR/ap_halow_open.conf
wlan0: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlan0 with hwaddr 8c:0f:fa:00:33:73 and ssid "halow_demo"
wlan0: interface state COUNTRY_UPDATE->ENABLED
wlan0: AP-ENABLED
[7] Start NAT
[8] ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.27  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::3260:a163:3814:e3ef  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:5a:ee:24  txqueuelen 1000  (Ethernet)
        RX packets 24218  bytes 15393968 (14.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28862  bytes 3784531 (3.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 71  bytes 10658 (10.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 71  bytes 10658 (10.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.1  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::6078:4d87:cac6:e0f  prefixlen 64  scopeid 0x20<link>
        ether 8c:0f:fa:00:33:73  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3780 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

HaLow AP ready
------------------------------------------------------------------
Done.
```

Figure 3.3 Results of running AP (2/2)

3.3 AP mode operation with Self-configuration

We provide 'Self-configuration' feature on AP, which is optional but aims to start AP with optimal channel after CCA scan before starting hostapd. (c.f. without the feature, AP just use static CH in conf. file of hostapd)

AP executes CCA scan on every CH, finds the best channel, and finally starts with the channel once the feature is enabled in the 'start.py'. There are 3 parameters related to the feature and Figure 3.4 shows them.

- self_config: enable/disable feature (default: disabled)
- perfer_bw: set the specific bandwidth you want to find (1MHz, 2MHz, 4MHz or any (all BW))
- dwell_time: time (in ms unit) to wait on each channel for CCA Scan (default: 100ms)

```
#------------------------------------------------------------------------------#
# Self configuration (AP Only)
#  AP scans the clearest CH and then starts with it
self_config       = 0        # 0 (disable)  or 1 (enable)
prefer_bw         = 0        # 0: no preferred bandwidth, 1: 1M, 2: 2M, 4: 4M
dwell_time        = 100      # max dwell is 1000 (ms), min: 10ms, default: 100ms
#------------------------------------------------------------------------------#
```

Figure 3.4 Parameter for Self-Configuration

CCA scan results (high percentage means CH is busy) on each channel is shown and best CH is selected accordingly. For this example, best CH is 39 (1MHz 928.5MHz) because CCA percentage is the lowest (0%) among all the channels. If you set prefer_bw = 0, 1M BW CH has higher priority than 2 and 4M BW CH with the same percentage. Basically, the best CH is automatically selected by CCA results, so it takes much more time according to the number of CH and dwell time on each CH.

```
[*] Self configuration start!
country: KR, prefer_bw: 0, dwell_time: 100
Start CCA scan.... It will take up to 2 sec to complete
        Frequency       CCA     bandwidth
--      925.5 MHz       8.2%    1M
--      926.5 MHz       2.9%    1M
--      927.5 MHz       0.3%    1M
--      928.5 MHz       0.0%    1M
--      929.5 MHz       0.0%    1M
--      930.5 MHz       0.2%    1M
--      927.0 MHz       1.6%    2M
--      929.0 MHz       0.0%    2M
[Optimal freq.] 928.5 MHz (CCA:0.0%, BW:1M)
[*]ch_num:39
OK
```

Figure 3.5 Results of Self-Configuration on AP

Please note that you should use target FW that supports Self-Configuration. If not, you will face the error log like below and hostapd will be started with static CH in conf. file.

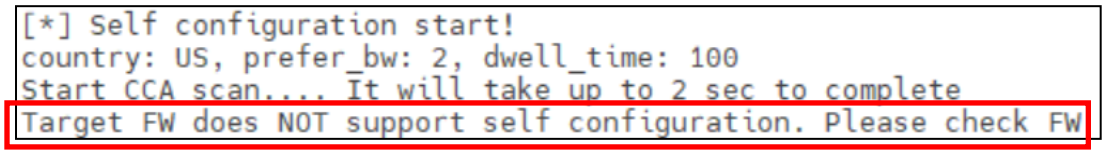


Figure 3.6 Results of Self-Configuration with invalid target FW

3.4 STA mode operation

1) Open terminal with SSH

After boot-up of STA board, connect via SSH to the STA by using the terminal emulator like MobaXterm. The ID and PW are as follows:

- ID : pi
- PW : raspberry

2) Run script

Running STA is similar to the procedure as AP's except for giving "0" as *sta_type*.

parameter setting

- *sta_type* : **0 (STA)**
- *security_mode* : available modes are 0(open), 1(WPA2-PSK), 2(WPA3-OWE) and 3(WPA3-SAE)
- *country* : available country codes are US, JP, TW, KR, EU, CN, AU, NZ

Ex) security mode STA to be used in Japan : ./start.py 0 1 JP

3) Check results

Once STA runs by start script, there are several procedures that is performed, 1) clear apps 2) copy firmware 3) load module 4) Set configurations 5) start wpa supplicant 6) start scan AP 7) connect to AP 8) start DHCP client are performed sequentially. If all the procedures are successful, STA finally gets an IP address.

```
pi@raspberrypi:~/nrc_pkg/script $ ./start.py 0 0 KR
Done.
Done.
------------------------------
Model            : 7292
STA Type         : STA
Country          : KR
Security Mode    : OPEN
CAL. USE         : ON
AMPDU            : ON
CQM              : ON
Download FW      : uni_s1g.bin
TX Power         : 17
Power Save Type  : Always On
Listen Interval  : 1000
------------------------------
NRC STA setting for HaLow...
[*] Set Max CPU Clock on RPi
1200000
1200000
1200000
1200000
Done
[0] Clear
hostapd: no process found
wireshark-gtk: no process found
rm: cannot remove '/home/pi/nrc_pkg/script/conf/temp_self_config.conf': No such file or
directory
[1] Copy
total 648
drwxr-xr-x 2 pi   pi     4096 Oct 15 11:40 .
drwxr-xr-x 4 pi   pi     4096 Oct 15 11:40 ..
-rwxrwxrwx 1 pi   pi      271 Oct 15 11:40 copy
-rwxr-xr-x 1 pi   pi      562 Oct 15 11:40 nrc7292_bd.dat
-rwxr-xr-x 1 pi   pi   321980 Oct 15 11:40 nrc7292_cspi.bin
-rwxr-xr-x 1 root root 321980 Oct 15 12:03 uni_s1g.bin
-rw-r--r-- 1 root root 321980 Oct 15 12:03 /lib/firmware/uni_s1g.bin
==================================
 STA INTERFACE    : wlan0
 USE DHCP Client
==================================
Config for STA is done!
IP and DHCP config done
[2] Set Module Parameters
[3] Loading module
sudo insmod /home/pi/nrc_pkg/sw/driver/nrc.ko  hifspeed=20000000 spi_bus_num=0 spi_cs_nu
m=0 spi_gpio_irq=5 spi_gpio_poll=-1 fw_name=uni_s1g.bin power_save=0 ndp_preq=1 auto_ba=
1 listen_interval=1000
[4] Set tx power
Tx power : 17                   Calibration_use : ON
OK
Board Data use                   : off
OK
[5] Set guard interval
guard interval : long
OK
```

Figure 3.7 Results of running STA (1/2)

```
[6] Set cal_use
Calibration_use : on                    Country   : KR
OK
[*] Start DHCPCD and DNSMASQ
wpa_supplicant: no process found
[6] Start wpa_supplicant on wlan0
Successfully initialized wpa_supplicant
[7] Connect and DHCP
Waiting for IP
wlan0: SME: Trying to authenticate with 8c:0f:fa:00:33:73 (SSID='halow_demo' freq=5220 M
Hz)
wlan0: Trying to associate with 8c:0f:fa:00:33:73 (SSID='halow_demo' freq=5220 MHz)
wlan0: Associated with 8c:0f:fa:00:33:73
wlan0: CTRL-EVENT-CONNECTED - Connection to 8c:0f:fa:00:33:73 completed [id=0 id_str=]
wlan0: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0
Waiting for IP
Waiting for IP
        inet 192.168.200.31  netmask 255.255.255.0  broadcast 192.168.200.255
IP assigned. HaLow STA ready
------------------------------------------------------------------
Done.
```

Figure 3.8 Results of running STA (2/2)

3.5 Configure static IP address

The DHCP client on a STA can obtain an IP address after successful connection to the AP. Or the users can assign a static IP address to the STA by using the script file provided with software package. Figure 3.9 presents the script (~/nrc_pkg/script/conf/etc/CONFIG_IP) and indicates the fields to set.

```
# Config for HaLow STA's IP and Defautl GW
USE_HALOW_STA_STATIC_IP=N     # Use STATIC IP :  Y(use Static IP) or N(use Dynamic IP(DHCP))
HALOW_STA_IP=192.168.200.11   # only valid when using static IP
HALOW_STA_NETMASK=24          # only valid when using static IP
HALOW_STA_DEFAULT_GW=192.168.200.1 # only valid when using static IP
```

Figure 3.9 Configure static IP address for STA

In addition, users can configure static IP addresses in the same way as the STA configuration. Figure 3.6 shows the fields to configure.

```
# Config for HaLow AP's IP and DHCPS configuration
HALOW_AP_IP=192.168.200.1
HALOW_AP_NETMASK=24
HALOW_AP_DHCPS_CONFIG=192.168.200.10,192.168.200.50,255.255.255.0,24h
```

Figure 3.10 Configure static IP address for AP

4 NRC7394 EVK performance evaluation

4.1 Performance test

Users can evaluate throughput performance by using the iperf3 tool.

1) Run iperf3 server at AP side

```
pi@raspberrypi:~/nrc_pkg/script $ iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 192.168.200.37, port 48108
[  5] local 192.168.200.1 port 5201 connected to 192.168.200.37 port 33605
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec   320 KBytes  2.62 Mbits/sec  6.193 ms  0/40 (0%)
[  5]   1.00-2.00   sec   352 KBytes  2.88 Mbits/sec  9.022 ms  0/44 (0%)
[  5]   2.00-3.00   sec   352 KBytes  2.88 Mbits/sec  10.556 ms  0/44 (0%)
[  5]   3.00-4.00   sec   368 KBytes  3.01 Mbits/sec  7.511 ms  0/46 (0%)
[  5]   4.00-5.00   sec   376 KBytes  3.08 Mbits/sec  7.605 ms  0/47 (0%)
[  5]   5.00-6.00   sec   368 KBytes  3.01 Mbits/sec  8.038 ms  0/46 (0%)
[  5]   6.00-7.00   sec   368 KBytes  3.01 Mbits/sec  7.942 ms  0/46 (0%)
[  5]   7.00-8.00   sec   400 KBytes  3.28 Mbits/sec  6.621 ms  0/50 (0%)
[  5]   8.00-9.00   sec   384 KBytes  3.15 Mbits/sec  8.250 ms  0/48 (0%)
[  5]   9.00-10.00  sec   360 KBytes  2.95 Mbits/sec  9.083 ms  0/45 (0%)
[  5]  10.00-10.24  sec  96.0 KBytes  3.22 Mbits/sec  9.234 ms  0/12 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  5]   0.00-10.24  sec  0.00 Bytes  0.00 bits/sec  9.234 ms  0/468 (0%)
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Figure 4.1 Run iperf3 server

2) Run iperf3 client at STA side (users can use other iperf3 options as well)

```
pi@raspberrypi:~/nrc_pkg/script $ iperf3 -c 192.168.200.1 -u -b 10m -t 10
Connecting to host 192.168.200.1, port 5201
[  4] local 192.168.200.37 port 33605 connected to 192.168.200.1 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   416 KBytes  3.41 Mbits/sec  52
[  4]   1.00-2.00   sec   360 KBytes  2.95 Mbits/sec  45
[  4]   2.00-3.00   sec   344 KBytes  2.82 Mbits/sec  43
[  4]   3.00-4.00   sec   368 KBytes  3.01 Mbits/sec  46
[  4]   4.00-5.00   sec   376 KBytes  3.08 Mbits/sec  47
[  4]   5.00-6.00   sec   368 KBytes  3.01 Mbits/sec  46
[  4]   6.00-7.00   sec   368 KBytes  3.01 Mbits/sec  46
[  4]   7.00-8.00   sec   392 KBytes  3.21 Mbits/sec  49
[  4]   8.00-9.00   sec   392 KBytes  3.21 Mbits/sec  49
[  4]   9.00-10.00  sec   360 KBytes  2.95 Mbits/sec  45
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec  3.66 MBytes  3.07 Mbits/sec  9.234 ms  0/468 (0%)
[  4] Sent 468 datagrams

iperf Done.
```

Figure 4.2 Run iperf3 client

4.2 Enable/Disable A-MPDU

Aggregate MAC protocol data unit (A-MPDU) is a MAC frame with multiple MAC sub-frames and single PHY header. By using A-MPDU, users can improve throughput because overhead is decreased in PHY header and inter-frame space (IFS).

Users can enable/disable A-MPDU by changing the *ampdu_enable* value in the 'start.py' script as shown in Figure 4.3. Setting "0" disables A-MPDU, setting "1" enables A-MPDU.

When AMPDU is enabled, maximum numbers of aggregation (i.e. maximum numbers of MPDU per AMPDU) is decided by NDP block ACK type. In case of using 2M NDP Block ACK, maximum 16 MPDUs can be aggregated and maximum 8 MPDUs while using 1M NDP Block ACK. Which one is used can be chosen by a parameter “ndp_ack_1m” in start.py (default: 2M NDP Block ACK on 2M or 4M Bandwidth CH, 1M NDP Block ACK on 1M Bandwidth CH) Please note that only 1M NDP Block ACK can be used on 1MHz Bandwidth channel regardless of the setting of ndp_ack_1m.

Please note that ndp_ack_1m should be set on AP and STA should follow AP’s setting.

```
################################################################################
# RF Conf.
# Board Data includes TX Power per MCS and CH
txpwr_val         = 17       # TX Power
txpwr_max_default = 24       # Board Data Max TX Power
bd_download       = 0        # 0(Board Data Download off) or 1(Board Data Download
bd_name           = 'nrc7292_bd.dat'
#-------------------------------------------------------------------------------#
# Calibration usage option
#  If this value is changed, the device should be restarted for applying the value
cal_use            = 1       # 0(disable) or 1(enable)
################################################################################
# PHY Conf.
guard_int         = 'long'   # Guard Interval ('long'(LGI) or 'short'(SGI))
################################################################################
# MAC Conf.
# AMPDU (Aggregated MPDU)
#  Enable AMPDU for full channel utilization and throughput enhancement
ampdu_enable      = 1        # 0 (disable) or 1 (enable)
#-------------------------------------------------------------------------------#
# 1M NDP (Block) ACK (AP Only)
#  Enable 1M NDP ACK on 2/4MHz BW for robustness (default: 2M NDP ACK on 2/4MH BW)
#  STA should follow, if enabled on AP
#  Note: if enabled, max # of mpdu in ampdu is restricted to 8 (default: max 16)
ndp_ack_1m        = 0        # 0 (disable) or 1 (enable)
```

Figure 4.3 Enable/disable A-MPDU

4.3 Enable/Disable NDP Probe Request

A probe request frame may be transmitted by the STA at the 802.11 baseline to collect information required for connection operation.
The PHY header uses a robust coding scheme to improve the transmission reliability of NDP probe requests, and the NDP probing procedure is used to reduce energy consumption during the scan procedure.
Users can enable/disable NDP Probe Request by changing the ndp_preq value of the 'start.py' script as shown in Figure 4.4. If "1" is set to ndp_preq, NDP Probe Request is activated. If it is set to "0", Legacy Probe Request is used. To activate the NDP Probe Request, "scan_ssid=1" must be included in the wpa_supplicant configure file.

```
##############################################################################
# PHY Conf.
guard_int          = 'long'    # Guard Interval ('long'(LGI) or 'short'(SGI))
##############################################################################
# MAC Conf.
# AMPDU (Aggregated MPDU)
#  Enable AMPDU for full channel utilization and throughput enhancement
ampdu_enable       = 1         # 0 (disable) or 1 (enable)
#-----------------------------------------------------------------------------#
# 1M NDP (Block) ACK (AP Only)
#  Enable 1M NDP ACK on 2/4MHz BW for robustness (default: 2M NDP ACK on 2/4MH BW)
#  STA should follow, if enabled on AP
#  Note: if enabled, max # of mpdu in ampdu is restricted to 8 (default: max 16)
ndp_ack_1m         = 0         # 0 (disable) or 1 (enable)
#-----------------------------------------------------------------------------#
# NDP Probe Request
#  For STA, "scan_ssid=1" in wpa_supplicant's conf should be set to use
ndp_preq           = 1         # 0 (Legacy Probe Req) 1 (NDP Probe Req)
#-----------------------------------------------------------------------------#
# CQM (Channel Quality Manager) (STA Only)
#  STA can disconnect according to Channel Quality (Beacon Loss or Poor Signal)
#  Note: if disabled, STA keeps connection regardless of Channel Quality
cqm_enable         = 1         # 0 (disable) or 1 (enable)
#-----------------------------------------------------------------------------#
# RELAY (Do NOT use! it will be deprecated)
relay_type         = 1         # 0 (wlan0: STA, wlan1: AP) 1 (wlan0: AP, wlan1: STA)
#-----------------------------------------------------------------------------#
```

Figure 4.4 Enable/disable NDP Probe Request

4.4 Enable/Disable power save

As shown in Figure 4.5, the user can enable/disable the power saving option by changing the power_save value in the 'start.py' script, and 4 options can be selected, and the default is 0 (disable).

Setting to "0" disables the power saving function, and a value of "1" enables modem sleep, which is a turn off only RF while PS. Values "2" and "3" enable deep sleep, which turns off almost all power, and can save more power than modem sleep.

A value of "2" activates deep sleep mode (TIM) and periodically checks the beacon during power save, A value of "3" activates the deep sleep mode (nonTIM), and it is not awakened by the AP's beacon, but is awakened by the station's Tx or an external interrupt.

```
#------------------------------------------------------------------------------#
# CQM (Channel Quality Manager) (STA Only)
#  STA can disconnect according to Channel Quality (Beacon Loss or Poor Signal)
#  Note: if disabled, STA keeps connection regardless of Channel Quality
cqm_enable        = 1        # 0 (disable) or 1 (enable)
#------------------------------------------------------------------------------#
# RELAY (Do NOT use! it will be deprecated)
relay_type        = 1        # 0 (wlan0: STA, wlan1: AP) 1 (wlan0: AP, wlan1: STA)
#------------------------------------------------------------------------------#
# Power Save (STA Only)
#  4-types PS: (0)Always on (1)Modem_Sleep (2)Deep_Sleep(TIM) (3)Deep_Sleep(nonTIM
#  Modem Sleep : turn off only RF while PS (Fast wake-up but less power save)
#   Deep Sleep : turn off almost all power (Slow wake-up but much more power save)
#     TIM Mode : check beacons during PS to receive BU from AP
#  nonTIM Mode : Not check beacons during PS (just wake up by TX or EXT INT)
power_save        = 0        # STA (power save type 0~3)
ps_timeout        = '3s'     # STA (timeout before going to sleep) (min:1000ms)
sleep_duration    = '3s'     # STA (sleep duration only for nonTIM deepsleep) (min:
listen_interval   = 1000     # STA (listen interval in BI unit) (max:65535)
#------------------------------------------------------------------------------#
# BSS MAX IDLE PERIOD (aka. keep alive) (AP Only)
#  STA should follow (i.e STA should send any frame before period),if enabled on AP
#  Period is in unit of 1000TU(1024ms, 1TU=1024us)
#  Note: if disabled, AP removes STAs' info only with explicit disconnection like d
bss_max_idle_enable = 1      # 0 (disable) or 1 (enable)
bss_max_idle        = 180    # time interval (e.g. 60: 614400ms) (1 ~ 65535)
#------------------------------------------------------------------------------#
```

Figure 4.5 Enable/disable power save

4.5 Enable/Disable board data

A user can enable/disable the option to download board data by changing the bd_download value in the 'start.py' script.

Setting BD Data is an enhanced Tx Power scheme, and Tx Power is set differently according to the rate table of board data. “0” disables downloading board data with the firmware and value “1” enables downloading board data with the firmware. Currently only works in Country US, default value is 0.

```
##################################################################################
# DEBUG Conf.
# NRC Driver log
driver_debug      = 0         # NRC Driver debug option : 0(off) or 1(on)
#---------------------------------------------------------------------------------#
# WPA Supplicant Log (STA Only)
supplicant_debug  = 0         # WPA Supplicant debug option : 0(off) or 1(on)
#---------------------------------------------------------------------------------#
# HOSTAPD Log (AP Only)
hostapd_debug     = 0         # Hostapd debug option    : 0(off) or 1(on)
##################################################################################
# CSPI Conf. (Default)
spi_clock         = 20000000  # SPI Master Clock Frequency
spi_bus_num       = 0         # SPI Master Bus Number
spi_cs_num        = 0         # SPI Master Chipselect Number
spi_gpio_irq      = 5         # CSPI_EIRQ GPIO Number, BBB is 60 recommanded.
spi_gpio_poll     = -1        # CSPI_EIRQ GPIO Polling Interval (if negative, irq m
#---------------------------------------------------------------------------------#
# FT232H USB-SPI Conf. (FT232H CSPI Conf)
ft232h_usb_spi    = 0         # FTDI FT232H USB-SPI bridge : 0(off) or 1(on)
##################################################################################
# RF Conf.
# Board Data includes TX Power per MCS and CH
txpwr_val         = 17        # TX Power
txpwr_max_default = 24        # Board Data Max TX Power
bd_download       = 0         # 0(Board Data Download off) or 1(Board Data Download
bd_name           = 'nrc7292_bd.dat'
#---------------------------------------------------------------------------------#
# Calibration usage option
#  If this value is changed, the device should be restarted for applying the value
cal_use            = 1        # 0(disable) or 1(enable)
##################################################################################
# PHY Conf.
guard_int         = 'long'    # Guard Interval ('long'(LGI) or 'short'(SGI))
##################################################################################
```

Figure 4.6 Enable/disable board data

4.6 Enable/Disable BSS MAX IDLE element

A user can enable/disable the option to download bss_max_idle with value by changing the bss_max_idle_enable in the 'start.py' script.

The bss_max_idle is used to check whether the STA is deactivated, and if the keep alive packet or any data is not received from the STA within the bss_max_idle value, the AP determines that the STA is no longer connected. If the AP is determined that the STA cannot be reached, the STA information is cleared through disassoc frame / deauthentication frame. The default is 180 seconds and can be set up to 65535. The default 'bss_max_idle_enable' is 1

:q

```
#------------------------------------------------------------------------------#
# BSS MAX IDLE PERIOD (aka. keep alive) (AP Only)
#  STA should follow (i.e STA should send any frame before period),if enabled on AP
#  Period is in unit of 1000TU(1024ms, 1TU=1024us)
#  Note: if disabled, AP removes STAs' info only with explicit disconnection like d
bss_max_idle_enable = 1      # 0 (disable) or 1 (enable)
bss_max_idle        = 180    # time interval (e.g. 60: 614400ms) (1 ~ 65535)
#------------------------------------------------------------------------------#
# Mesh Options (Mesh Only)
#  SW encryption by MAC80211 for Mesh Point
sw_enc              = 0     # 0 (disable), 1 (enable)
#  Manual Peering & Static IP
peer                = 0     # 0 (disable) or Peer MAC Address
static_ip           = 0     # 0 (disable) or Static IP Address
#------------------------------------------------------------------------------#
# Self configuration (AP Only)
#  AP scans the clearest CH and then starts with it
self_config       = 0        # 0 (disable)  or 1 (enable)
prefer_bw         = 0        # 0: no preferred bandwidth, 1: 1M, 2: 2M, 4: 4M
dwell_time        = 100      # max dwell is 1000 (ms), min: 10ms, default: 100ms
################################################################################
```

Figure 4.7 Enable/disable BSS MAX IDLE

5 Internet connection

If NAT configuration is complete with the start script in chapter 0 and AP is connected to the Internet through its Ethernet interface, then the STA connected to the AP can access the Internet via AP. After boot-up, AP can obtain IP address from DHCP server.

On successful Wi-Fi connection, users can verify the reachability to the internet by using a ping program.

```
pi@raspberrypi:~/nrc_pkg/script $ ping google.com -c 3
PING google.com (172.217.24.206) 56(84) bytes of data.
64 bytes from hkg12s13-in-f14.1e100.net (172.217.24.206): icmp_seq=1 ttl=50 time=37.9 ms
64 bytes from hkg12s13-in-f14.1e100.net (172.217.24.206): icmp_seq=2 ttl=50 time=37.3 ms
64 bytes from hkg12s13-in-f14.1e100.net (172.217.24.206): icmp_seq=3 ttl=50 time=38.7 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 37.380/38.016/38.716/0.547 ms
```

Figure 5.1 Result of ping

Once the internet connection is confirmed by STA, users can surf the web and play YouTube.

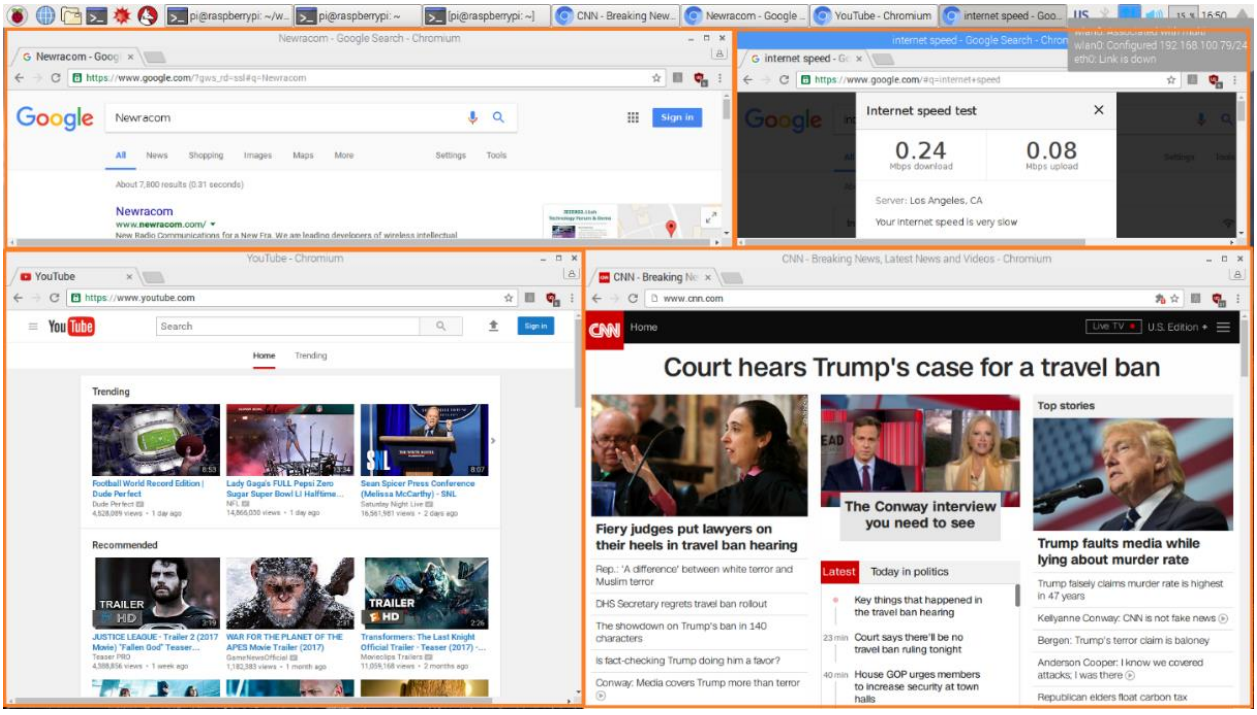


Figure 5.2 Internal connection

6 Change configuration

NRC7394 supports 1/2/4 MHz channel bandwidth (only 1 MHz for JP and 1/2 MHz for EU). The default channel bandwidth and frequency are different for every country (e.g. 2 MHz BW at 909 MHz for US, 1MHz BW at 917 MHz for JP, 2 MHz BW at 843.5 MHz for TW. Users can change the frequency band and channel bandwidth by editing only the frequency band index of the configuration file of AP named COUNTRY/*ap_halow_open.conf* (Users must attempt to change the channel on the AP).

```
ctrl_interface=/var/run/hostapd
country_code=US
interface=wlan0
#ssid=halow_demo
ssid=halow
hw_mode=a

#1MHz
#909.5MHz
#channel=37
#915.5MHz
#channel=43
#922.5MHz
#channel=150

#2MHz
#909MHz
#channel=153
#915MHz
#channel=156
#921MHz
#channel=159
#925MHz
channel=161

#4MHz
#910MHz
#channel=162
#914MHz
#channel=163
#922MHz
#channel=165

ieee80211h=1
ieee80211d=1
ieee80211n=1
#wmm_enabled=1
macaddr_acl=0
driver=nl80211
beacon_int=100
#disable_sgi=0
#ap_max_inactivity=3
ap_max_inactivity=16780
# USF=0, UI=2 : 3
# USF=1, UI=2 : 16780
# USF=0, UI=10: 11
# USF=1, UI=10: 16788
#listen_interval=2
```

```
ctrl_interface=/var/run/hostapd
country_code=JP
interface=wlan0
ssid=halow_demo
hw_mode=a

#1MHz
#917MHz
channel=36
#918MHz
#channel=37
#919MHz
#channel=38
#920MHz
#channel=39
#921MHz
#channel=40
#922MHz
#channel=41
#923MHz
#channel=42
#924MHz
#channel=43
#925MHz
#channel=44
#926MHz
#channel=45
#927MHz
#channel=46

ieee80211h=1
ieee80211d=1
ieee80211n=1
#wmm_enabled=1
macaddr_acl=0
driver=nl80211
beacon_int=100
#disable_sgi=0
#ap_max_inactivity=3
ap_max_inactivity=16780
# USF=0, UI=2 : 3
# USF=1, UI=2 : 16780
# USF=0, UI=10: 11
# USF=1, UI=10: 16788
#listen_interval=2
```

```
ctrl_interface=/var/run/hostapd
country_code=TW
interface=wlan0
ssid=halow_demo
hw_mode=a

#1MHz
#839MHz
#channel=36
#843MHz
#channel=40
#850MHz
#channel=47

#2MHz
#839.5MHz
#channel=149
#843.5MHz
channel=151
#845.5MHz
#channel=152
#849.5MHz
#channel=154

#4MHz
#840.5MHz
#channel=155
#844.5Hz
#channel=156
#848.5MHz
#channel=157

ieee80211h=1
ieee80211d=1
ieee80211n=1
#wmm_enabled=1
macaddr_acl=0
driver=nl80211
beacon_int=100
#disable_sgi=0
#ap_max_inactivity=3
ap_max_inactivity=16780
# USF=0, UI=2 : 3
# USF=1, UI=2 : 16780
# USF=0, UI=10: 11
# USF=1, UI=10: 16788
#listen_interval=2
```

Figure 6.1 Contents of ap_halow_open.conf file (US/JP/TW)

```
ctrl_interface=/var/run/hostapd
country_code=KR
interface=wlan0
ssid=halow_demo
hw_mode=a

#tx_queue_data2_aifs=3
#tx_queue_data2_cwmin=15
#tx_queue_data2_cwmax=63
#tx_queue_data2_burst=30

#1MHz
#918MHz
#channel=36
#919MHz
#channel=37
#920MHz
#channel=38
#921MHz
#channel=39
#922MHz
#channel=40
#923MHz
#channel=41
#################
#942.8MHz
#channel=46
#943.8MHz
#channel=47
#944.8MHz
#channel=48
#945.8MHz
#channel=149

#2MHz
#918.5MHz
#channel=42
#920.5MHz
#channel=43
#922.5MHz
channel=44
#################
#943.3MHz
#channel=150
#945.3MHz
#channel=151

#4MHz
#921.5MHz
#channel=45
#################
#944.3MHz
#channel=152
```

```
ctrl_interface=/var/run/hostapd
country_code=DE
interface=wlan0
ssid=halow_demo
hw_mode=a

#1MHz
#863.5MHz
#channel=36
#864.5MHz
#channel=37
#865.5MHz
#channel=38
#866.5MHz
#channel=39
#867.5MHz
#channel=40

#2MHz
#864MHz
channel=41
#866MHz
#channel=42
```

```
ctrl_interface=/var/run/hostapd
country_code=CN
interface=wlan0
ssid=halow_demo
hw_mode=a

#1MHz
#755.5MHz
#channel=36
#759.5MHz
#channel=40
#763.5MHz
#channel=44
#767.5MHz
#channel=48
#770.5MHz
#channel=151
#779.5MHz
#channel=152
#780.5MHz
#channel=153
#781.5MHz
#channel=154
#782.5MHz
#channel=155
#783.5MHz
#channel=156
#784.5MHz
#channel=157
#785.5MHz
#channel=158
#786.5MHz
#channel=159

#2MHz
#780MHz
channel=160
#782MHz
#channel=161
#784MHz
#channel=162
#786MHz
#channel=163

#4MHz
#781MHz
#channel=164
#785MHz
#channel=165
```

Figure 6.2 Contents of ap_halow_open.conf file (KR/EU/CN)

Table 6.1 Available frequency band and corresponding channel bandwidth (US)

Available frequency band index	Bandwidth (MHz)	Sub-1GHz frequency
1	1	902.5
3	1	903.5
5	1	904.5
7	1	905.5
9	1	906.5
11	1	907.5
36	1	908.5
37	1	909.5
38	1	910.5
39	1	911.5
40	1	912.5
41	1	913.5
42	1	914.5
43	1	915.5
44	1	916.5
45	1	917.5
46	1	918.5
47	1	919.5
48	1	920.5
149	1	921.5
150	1	922.5
151	1	923.5
152	1	924.5
100	1	925.5
104	1	926.5
108	1	927.5
2	2	903
6	2	905
10	2	907
153	2	909
154	2	911
155	2	913
156	2	915
157	2	917
158	2	919
159	2	921
160	2	923

161 (Default)	**2**	**925**
112	2	927
8	4	906
162	4	910
163	4	914
164	4	918
165	4	922
116	4	926

Table 6.2 Available frequency band and corresponding channel bandwidth (TW)

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
36	1	839
37	1	840
38	1	841
39	1	842
40	1	843
41	1	844
42	1	845
43	1	846
44	1	847
45	1	848
46	1	849
47	1	850
48	1	851
149	2	839.5
150	2	841.5
151(Default)	**2**	**843.5**
152	2	845.5
153	2	847.5
154	2	849.5
155	4	840.5
156	4	844.5
157	4	848.5

Table 6.3 Available frequency band and corresponding channel bandwidth (CN)

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
36	1	749.5
37	1	750.5
38	1	751.5
39	1	752.5
40 (Default)	**1**	**753.5**
41	1	754.5
42	1	755.5
43	1	756.5
149	2	750
151	2	752
153	2	754
155	2	756
150	4	751
154	4	755

Table 6.4 Available frequency band and corresponding channel bandwidth (KR-USN)

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
44 (Default)	**1**	**921.5**
45	1	922.5

Table 6.5 Available frequency band and corresponding channel bandwidth (KR-MIC)

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
37	1	926.5
38	1	927.5
39 (Default)	**1**	**928.5**
40	1	929.5
42	2	927.0
43	2	929.0

Table 6.6 Available frequency band and corresponding channel bandwidth (JP)

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
40 (Default)	**1**	**921.0**
42	1	923.0
43	1	924.0
44	1	925.0

45	1	926.0
46	1	927.0
36	2	923.5
37	2	924.5
38	2	925.5
39	2	926.5
47	4	924.5
48	4	925.5

Table 6.7 Available frequency band and corresponding channel bandwidth (EU)

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
36 (Default)	1	863.5
37	1	864.5
38	1	865.5
39	1	866.5
40	1	867.5

Table 6.8 Available frequency band and corresponding channel bandwidth (NZ)

Available frequency band index	Bandwidth (MHz)	Sub-1GHz frequency
36 (Default)	**1**	**915.5**
37	1	916.5
38	1	917.5
39	1	918.5
40	1	919.5
41	1	920.5
42	1	921.5
43	1	922.5
44	1	923.5
45	1	924.5
46	1	925.5
47	1	926.5
48	1	927.5
153	2	916.0
154	2	918.0
155	2	920.0
156	2	922.0
157	2	925.0
158	2	927.0
162	4	917.0

163	4	921.0
164	4	926.0

Table 6.9 Available frequency band and corresponding channel bandwidth (AU)

Available frequency band index	Bandwidth (MHz)	Sub-1GHz frequency
36 (Default)	**1**	**915.5**
37	1	916.5
38	1	917.5
39	1	918.5
40	1	919.5
41	1	920.5
42	1	921.5
43	1	922.5
44	1	923.5
45	1	924.5
46	1	925.5
47	1	926.5
48	1	927.5
153	2	916.0
154	2	918.0
155	2	921.0
156	2	923.0
157	2	925.0
158	2	927.0
162	4	917.0
163	4	922.0
164	4	926.0

Note that when changing the AP channel, when using Sub 1 GHz of the Available frequency band index (1~13), the AP configuration file such as ap_halow_open.conf must be modified. The 'hw_mode=a' in the 7th line of the configure file for AP must be changed to 'hw_mode=g', and it is only applicable to US Channel.

```
ctrl_interface=/var/run/hostapd
country_code=US
interface=wlan0
ssid=halow_demo
#ssid=halow_relay_1
hw_mode=g

#1MHz
############
#Below channel Must be set hw_mode=g in line 7
############
#902.5MHz
channel=1
#903.5MHz
#channel=3
#904.5MHz
#channel=5
#905.5MHz
#channel=7
#906.5MHz
#channel=9
#907.5MHz
#channel=11
#############
```

Figure 6.3 hw_mode of ap_halow_open.conf file (US)

Table 6.10 US Channels of hw_mode=g in a configure file

Available frequency band index	Bandwidth (MHz)	Sub 1 GHz frequency (MHz)
1	1	902.5
3	1	903.5
5	1	904.5
7	1	905.5
9	1	906.5
11	1	907.5
2	2	903
6	2	905
10	2	907
8	2	906

7 NRC7394 EVK software

Table 7.1 and Table 7.2 show AP and STA's file directory on the Raspberry PI 4 host. NRC7394 EVK contains some scripts to start AP/STA operation, a configuration file for operation, Linux Wi-Fi module driver, and NRC7394 firmware.

Table 7.1 Files in AP

File or Folder	Path	Description
ap_halow_open.conf	NRC_PKG/script/conf/COUNTRY	AP configuration file (open mode)
ap_halow_wpa2.conf	NRC_PKG/script/conf/COUNTRY	AP configuration file (WPA2-PSK)
ap_halow_owe.conf	NRC_PKG/script/conf/COUNTRY	AP configuration file (WPA3-OWE)
ap_halow_sae.conf	NRC_PKG/script/conf/COUNTRY	AP configuration file (WPA3-SAE)
start.py	NRC_PKG/script	start script
stop.py	NRC_PKG/script	stop script
CONFIG_IP	NRC_PKG/script/conf/etc	IP and DHCP configuration
ip_config.sh	NRC_PKG/script/conf/etc	IP and DHCP configuration script
clock_config.sh	NRC_PKG/script/conf/etc	RPi Max Clock configuration script
nrc.ko	NRC_PKG/sw/driver	NRC7394 Host Wi-Fi driver
uni_s1g.bin	NRC_PKG/sw/firmware	NRC7394 firmware

※ NRC_PKG = /home/pi/nrc_pkg/

Table 7.2 Files in STA

File or Folder	Path	Description
sta_halow_open.conf	NRC_PKG/script/conf/COUNTRY	STA configuration file (open mode)
sta_halow_wpa2.conf	NRC_PKG/script/conf/COUNTRY	STA configuration file (WPA2-PSK)
sta_halow_owe.conf	NRC_PKG/script/conf/COUNTRY	STA configuration file (WPA3-OWE)
sta_halow_sae.conf	NRC_PKG/script/conf/COUNTRY	STA configuration file (WPA3-SAE)
start.py	NRC_PKG/script	start script
stop.py	NRC_PKG/script	stop script
CONFIG_IP	NRC_PKG/script/conf/etc	IP and DHCP configuration
ip_config.sh	NRC_PKG/script/conf/etc	IP and DHCP configuration script
clock_config.sh	NRC_PKG/script/conf/etc	RPi Max Clock configuration script
nrc.ko	NRC_PKG/sw/driver	NRC7394 Host Wi-Fi driver
uni_s1g.bin	NRC_PKG/sw/firmware	NRC7394 firmware

※ NRC_PKG = /home/pi/nrc_pkg/

8 NRC7394 EVK Sniffer operation

NRC7394 EVK can be used to capture 11ah frames in the air like other Wi-Fi sniffer devices in the market. For the installation of software package and operation for sniffer, please refer to “NRC7394 EVK User Guide (NewraPeek™)”.

9 Revision history

Revision No	Date	Comments
Ver 1.0	4/5/2023	Initial version

Appendix A.
Upgrade hostapd & wpa_supplicant for supporting WPA3

A.1 Overview

WPA3 is the next generation of Wi-Fi security and provides state-of-the-art security protocols to the market. So, all WPA3 networks:

- Use the latest security methods
- Disallow outdated legacy protocols
- Require use of Protected Management Frame (PMF)

WPA3-Personal brings better protections by providing robust password-based authentication. This capability is enabled by Simultaneous Authentication of Equals (SAE), which replaces Pre-Shared Key (PSK) in WPA2-Personal.

WPA3-Enterprise has two modes. Basic mode is based on WPA2-Enterprise and PMF. An optional mode using 192-bit security protocols is also defined in WPA3-Enterprise, but this is not adequate for the IoT application. So, it is not supported in NRC7394 EVK.

However, NRC7394 EVK supports Wi-Fi Enhanced Open mode, which is based on Opportunistic Wireless Encryption (OWE) and replaces open mode.

In summary, NRC7394 EVK supports following WPA3 security modes.

- Wi-Fi Enhanced Open (OWE mode)
- WFA3-Personal (WPA3-SAE mode)

By the way, it is necessary recommendation to upgrade hostapd and wpa_supplicant to version 2.10 for the full support of WPA3 protocols. Please follow the steps listed below to upgrade version.

A.2 Upgrade hostapd

A.2.1 Download hostapd v2.10 and install required libraries

Please follow the procedure below.

```
$ wget http://w1.fi/releases/hostapd-2.10.tar.gz
$ tar zxf hostapd-2.10.tar.gz
$ sudo apt-get update
$ sudo apt-get install libnl-3-dev libnl-genl-3-dev libssl-dev
```

A.2.2 Build and install hostapd v2.10

Please follow the procedure below.

```
$ cd hostapd-2.10/hostapd
$ cp defconfig .config
$ vi .config
Enable followings:
CONFIG_IEEE80211N=y
CONFIG_OWE=y
CONFIG_WPS=y
Insert following:
CONFIG_SAE=y
CONFIG_TESTING_OPTIONS=y
$ vi ../src/ap/wpa_auth.c
Comment line 72:
69 //static const u32 eapol_key_timeout_subseq = 1000; /* ms */
Add line 73:
70 static const u32 eapol_key_timeout_subseq = 2000; /* ms */
$ make
$ sudo make install
```

Note. eapol_key_timeout_subseq = 2000 should be added to support WPA3-OWE (This is only to support NRC7292 devices.)

A.3 Upgrade wpa_supplicant

A.3.1 Download wpa_supplicant v2.10 and install required libraries

Please follow the procedure below.

```
$ wget http://w1.fi/releases/wpa_supplicant-2.10.tar.gz
$ tar zxf wpa_supplicant-2.10.tar.gz
$ sudo apt-get update
$ sudo apt-get install libnl-3-dev libnl-genl-3-dev libssl-dev
$ sudo apt-get install libdbus-1-dev libdbus-glib-1-dev
```

A.3.2 Build and install wpa_supplicant v2.10

Please follow the procedure below.

```
$ cd wpa_supplicant-2.10/wpa_supplicant
$ cp defconfig .config
$ vi .config
```

Enable followings:

```
CONFIG_IEEE80211N=y
CONFIG_OWE=y
CONFIG_SAE=y
CONFIG_MESH=y
CONFIG_WPS=Y
CONFIG_TESTING_OPTIONS=y
```

Disable followings:

```
#CONFIG_DRIVER_WIRED=y
#CONFIG_DRIVER_MACSEC_LINUX=y
#CONFIG_CTRL_IFACE_DBUS_NEW=y
#CONFIG_WNM=y
```

```
$ make
$ sudo make install
```